Data Protection Legal Reforms in Africa

Candidate: Patricia Boshe

Supervisor: Prof. Dr. Dirk Heckmann

A Thesis Submitted to the Chair of Public Law, Security Law and Internet Law at Passau University for the Degree of Doctor of Juris

July 2017

Table of Contents

Abbreviations and Acronyms

ACHPR	African Charter on Human and Peoples' Rights
AIDS	Acquired immune deficiency syndrome
APEC	Asia-Pacific Economic Cooperation
Art	Article
AU	African Union
BPO	Business Process Outsourcing
CAT	Court of Appeal of Tanzania
CDHRI	Cairo Declaration on Human Rights in Islam
CETS	Council of Europe Treaty Series
CFI	Court of First Instance (EU)
CFR	Charter of Fundamental Rights (Europe)
CoE	Council of Europe
CRID	*Centre de Recherches Informatique et Droit* (University of Namur, Belgium)
CRS	Congressional Research Service
DAAD	Deutscher Akademischer Austausch Dienst
e.g.	*exampli gratia* (for example)
EAC	East African Community
EC	European Community
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECOWAS	Economic Community for West African States
ECtHR	European Court of Human Rights
ed(s)	editor
EEA	European Economic Area
EPIC	Electronic Privacy Information Centre
et al.	*et alii/alia* (and others)
etc	*et cetera* (extra)
ETS	European Treaty Series
EU	European Union
HCT	High Court of Tanzania
HIV	Human immunodeficiency virus
i.e.	*id est.* (that is to say)

Ibid	ibidem (in the same place)
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICT	Information Communication Technology
IMF	International Monetary Fund
Infra	later cited
ITES	Information Technology Enabled Service
MCT	Media Council of Tanzania
NEPAD	New Partnership for Africa's Development
No	Number
NRCCL	Norwegian Research Centre for Computers and Law
O.J	Official Journal of the European Communities/European Union
OAU	Organisation of African Unity
OECD	Organisation for Economic Co-operation and Development
OIC	Organisation of Islamic Cooperation
p/pp	page(s)
para	paragraph
PMG	Parliamentary Monitoring Group (South Africa)
R	Recommendation
RSA	Republic of South Africa
s	section
SA	South Africa
SADC	Southern African development Community
SAP	Structural Adjustment Programme
SH/SHA	Safe Harbor Agreement
Supra	previously cited
T.L.R	Tanzania Law Report
TCRA	Tanzania Communications Regulatory Authority
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UKHL	United Kingdom House of Lords
UN	United Nations
URT	United Republic of Tanzania
US/USA	United States of America

USSR	Union of Soviet Socialist Republics
v	versus
Vol.	Volume
WB	World Bank
WIPO	World Intellectual Property Organisation
WITS	University of Witwatersrand
WLR	Weekly Law Report (UK)
WTO	World Trade Organisation

Statutory Declaration

I **Patricia Boshe** hereby confirm my thesis entitled '**Data Protection Legal Reforms in Africa**' is the result of my own work. I did not receive any help or support from individual or commercial consultants. All sources and/ or material used are listed and specified in the thesis accordingly.

Furthermore, I declare that, the requirements of paragraph § 6 1. No. 4 of the PhD regulations of 2007, as amended on 17th February 2014 has been fulfilled. That, this thesis has not been submitted as part of another examination process, or used for an award in any University in the Federal Republic of Germany or any other State, neither in identical or similar form.

I also confirm that, I do not hold any doctoral degree from a university in the Federal Republic of Germany or submitted a dissertation for the purpose of acquiring doctoral degree.

---------- ----------

Place, date Signature

Eidesstattliche Erklärung

Ich **Patricia Boshe**, erkläre hiermit an Eides statt, die Dissertation ***'Data Protection Legal Reforms in Africa'*** eigenständig, h.d insbesondere selbständig und ohne Hilfe eines Kommeziellen Promotionsberaters, angefertigt und keine anderen als die von mir angegeben Quellenen und hilfsmittel verwendet zu haben.

Ich erkläre Außerdem, dass die Voraussetzungen des § 6 Abs. 1 Nr. 4 der Promotionsordnung von 2007 in der Fassung vom 17. Februar 2014 erfüllt sind. Ich erkläre dass die Dissertation weder in gleicher noch in ähnlicher Form bereits in einem anderen Prüfungsverfahren vorgelegen hat.

---------- ----------

Ort, Datum Unterschrift

Acknowledgements

I am especially grateful to my supervisor Herrn Prof. Dr. Dirk Heckmann for navigating me through the rightful path in the preparation of this thesis. Prof. Heckmann allocated his time in his busy schedule to discuss and help organize my thoughts into a workable blueprint and supervise me throughout the final thesis.

I am indebted to the Deutscher Akademischer Austausch Dienst (DAAD) who funded my studies and my stay in Germany for the whole period of writing this thesis. In the same vein, I am thankful to the Open University of Tanzania who financially supported my field work. I also wish to thank Dr. Alex Boniface Makulilo who offered tremendous advice, professional and topical advice on the subject matter of this thesis in light of African context and for reading and reviewing my initial and current document. Similarly, I extend my sincere gratitude to Hon. Judge Dr. Benhajj Shaaban Masoud for reading, reviewing and advice on my initial project proposal and the final work and for words of encouragement whenever we communicated. Similar support and encouragement was provided by Dr. Yitiha Simbeye from the Open University of Tanzania. I am really humbled.

In a special way, I appreciate and honor the support offered by my late husband, Andrew William Gimbika, from the beginning of this journey in 2013 until the time he met his untimely death in 2014. While I pray for his soul to continue resting in eternal peace, I wish to say, as difficult as it was to pick myself up and continue with this project, I managed out of remembrance of his constant reminder of the importance of this endeavor. Our son, Ethan Andrew Gimbika whose presence gave me hope and courage to continue this journey, and whose smile gave me the strength to stand again and reach the finish line; this is for both of you!

Last but not least, I appreciate the support offered by my family during the very difficult time of my life; when I lost my beloved husband. It was not easy to get back into my feet; but with the encouragement and support from my family, I was able to pick myself up and continue, not only with my life but also with studies. In a special way, I would like to mention my mother, Theonestina Kaiza-Boshe, my father, John Izaack Boshe, my sisters and Cousin Pendo Boshe, Judith Boshe and Edina Kaiza, my brothers, Fredrick and Peter Boshe and my brother in law Nguvu Kamando. Thank you for instilling hope in me!

I, however, bear all the responsibility for any errors and shortcomings of this work.

Abstract

This work illustrates reform approaches in Africa using an international legal comparative approach. The research uses Tanzania and Senegal as the primary case studies and France, the United Kingdom and Germany as secondary case studies to illustrate how Europe reformed data protection regimes through the transposition of the EU Data Protection Directive of 1995.

Chapter one introduces the work; explaining the forces towards data protection regulations and their basis. Chapter two provides for a 'back-to-back' comparison in three countries (France, Germany and United Kingdom) against the 1995 Data Protection Directive. The idea behind this chapter is to draw a picture on how the legal culture and the pre-existing notions of the right to privacy inform on data protection legal reforms and determines the nature, contents, context and interpretation of adopted regime for data protection. Eventually, all these aspects affect the nature and extent of protection offered regardless of the substance of the law adopted.

Chapter three gives a narrative explanation of nature and perceptions of the right to privacy in Africa and how this may affect data protection reforms in Africa. In the same disposition, African customary legal systems and practices are explained providing a reader with a picture of the overall nature of African systems that makes up an African legal culture. The overview of African privacy perception and legal system is necessary for assessing the workability of any data protection regime to be adopted in Africa which in effect answers the first research question. The chapter draws its rationale from chapter two. In understanding African perceptions of privacy and the African legal culture, one can be able to predict the content and context of the reforms and maybe how the judiciary might interpret the laws based on local perceptions and supporting systems.

An overview of the African data protection architecture or rather human right architecture is provided in chapter four; ideally to provide a reader with a picture of the enforcement systems in Africa as a continent. This is followed by chapter five discussing the two major legal systems in Africa; the civil law and the common law system. The chapter also illustrates the position of African landscape in relation to legal harmonization/unification. This aspect is considered necessary because data protection regimes are more focused on legal harmonization and hence the question of how well or to what extent Africa as a continent can bring about harmonization in law became inevitable. Eventually, the chapter offers a comparative mirror analysis of the

primary case studies, i.e. Senegal and Tanzania. The analysis is made on the reform approach taken, motivation behind the reforms and on the regime erected (this is done through textual analysis of the law and the draft bill respectively).

Chapter six concludes the work by answering research questions based on findings and scrutiny from each chapter. It is concluded that there is a very slim chance for the African States to cling on the cultural defence against the adoption of the Western frameworks for data protection. It is also concluded that, lest Africa becomes an active participant in the global process that informs on data protection challenges and regulations, it faces a danger of becoming a puppet of foreign data protection regulation, which may or may not fit African legal culture. The chapter also illustrates how Africa as a continent and the African States individually have taken up data protection reforms blindly. The motivations for the reforms are vaguely stated and unclear. In the majority of legal instruments, the reforms are not taken as a move towards securing and protecting individual rights rather a purely political move influenced by economic motivations. The reforms are to a large extent, a mere impression to align with global data protection regimes and hence lack the political will to enforce the laws.

Zusammenfassung

Die Arbeit beleuchtet Reformansätze in Afrika im Rahmen eines internationalen rechtsvergleichenden Ansatzes. In der Studie werden Tansania und Senegal als primäre Fallbeispiele und Frankreich, United Kingdom und Deutschland als sekundäre Fallbeispiele verwendet, um aufzuzeigen, wie in Europa die Datenschutzregelungen durch die Umsetzung der EU Data Protection Directive aus dem Jahre 1995 reformiert wurden.

Kapitel eins beinhaltet eine Einführung in die Arbeit; dabei wird der Druck zur Einführung von Datenschutzvorschriften und deren Grundlage erklärt. Kapitel zwei bietet einen direkten Vergleich dreier Länder (Frankreich, Deutschland und United Kingdom) mit der EU Data Protection Directive, 1995. Der diesem Kapitel zugrundeliegende Gedanke war, sich ein Bild davon zu machen, inwieweit die Rechtskultur und vorgefassten Meinungen zum Recht auf Schutz der Privatsphäre Auskunft geben über Datenschutzrechtsreformen und wie dadurch Charakter, Inhalt, Kontext und Auslegung des verabschiedeten Regelwerks zum Datenschutz bestimmt werden. Letztendlich haben all diese Aspekte Auswirkungen auf den Charakter und das Ausmaß des gewährten Schutzes, unabhängig vom Inhalt des verabschiedeten Gesetzes.

In Kapitel drei werden der Charakter und die Sichtweise des Rechts auf Schutz der Privatsphäre in Afrika beschreibend erläutert, und inwieweit dies Datenschutzreformen in Afrika beeinflussen könnte. Gleichzeitig werden in Afrika gebräuchliche Rechtssysteme and Praktiken erläutert, damit sich der Leser ein Bild machen kann vom allumfassenden Charakter der afrikanischen Systeme, welche die afrikanische Rechtskultur ausmachen. Diese Übersicht über die afrikanische Sichtweise zum Thema Schutz der Privatsphäre und zum afrikanischen Rechtssystem ist notwendig, um beurteilen zu können, inwieweit ein Datenschutzregelwerk, welches in Afrika gesetzlich verabschiedet werden soll, überhaupt praktikabel ist, was im Endeffekt die erste wissenschaftliche Fragestellung beantwortet. Die logische Grundlage des Kapitels stützt sich auf Kapitel zwei. Indem man die afrikanische Sichtweise von Privatsphäre und die afrikanische Rechtskultur versteht, kann man sowohl zu Inhalt und Kontext der Reformen Prognosen abgeben als unter Umständen auch dazu, wie das Justizwesen diese Gesetze basierend auf der lokalen Wahrnehmung und den unterstützenden Systemen interpretieren wird.

Eine Übersicht über die afrikanische Datenschutzstruktur oder besser gesagt über die Menschenrechtsstruktur wird in Kapitel vier gegeben; idealerweise sollte damit dem Leser ein

Bild von den Systemen zur Rechtsdurchsetzung in Afrika als Kontinent vermittelt werden. Hierauf folgt Kapitel fünf, in welchem die beiden größten Rechtssysteme in Afrika erörtert werden, das Zivilrechtssystem und das Gewohnheitsrechtssystem. In diesem Kapitel wird auch die Position der afrikanischen Landschaft im Hinblick auf rechtliche Harmonisierung/Vereinheitlichung dargestellt. Dieser Aspekt wird als notwendig erachtet, da der Fokus von Datenschutzregelwerken eher auf einer rechtlichen Harmonisierung liegt und daher auf der Frage, wie gut oder in welchem Ausmaß Afrika als Kontinent eine rechtliche Harmonisierung umsetzen kann die unvermeidbar geworden ist. Schlussendlich bietet dieses Kapitel auch noch eine vergleichende Spiegelsichtanalyse der Primärfallstudien, d.h. Senegal und Tansania. Die Analyse erfolgte hinsichtlich des gewählten Reformansatzes, der Beweggründe auf welchen die Reformen basierten und des errichteten Systems (dies geschieht durch eine Textanalyse des Gesetzes beziehungsweise des Gesetzentwurfs).

In Kapitel sechs wird die Arbeit mit der Beantwortung der wissenschaftlichen Fragestellung basierend auf den Erkenntnissen und einer genauen Untersuchung aller vorangehenden Kapitel abgeschlossen. Die Schlussfolgerung ist, dass nur eine sehr geringe Chance für die afrikanischen Staaten besteht, dass diese sich kulturell verteidigen werden können gegen eine Übernahme des westlichen Rechtsrahmens für Datenschutz. Ferner wird zu der Auffassung gelangt, dass – sofern Afrika nicht aktiv an dem globalen Prozess teilnimmt, welcher Informationen zu den Herausforderungen des Datenschutzes und zu Datenschutzbestimmungen liefert der Kontinent in Gefahr läuft, zu einer Marionette ausländischer Datenschutzvorschriften zu werden, ganz gleich ob diese zur afrikanischen Rechtskultur passen oder nicht. Das Kapitel zeigt auch auf, wie Afrika als Kontinent und die afrikanischen Staaten jeweils für sich genommen Datenschutzreformen blindlings übernommen haben. Die Beweggründe für die Reformen sind nicht genau benannt und nicht klar. Bei der Mehrheit der Rechtsvorschriften wurden die Reformen nicht durchgeführt um die Rechte Einzelner zu schützen und abzusichern, sondern als rein politischer Schachzug basierend auf wirtschaftlichen Beweggründen. Die Reformen sind größtenteils lediglich ein bloßer Eindruck sich an globale Datenschutzregelwerke anzupassen und es fehlt daher am politischen Willen, diese Gesetze auch durchzusetzen.

Table of Statutes and Conventions

African Union

African Charter on Human and Peoples' Rights 1981

African Charter on the Rights and Welfare of the Child 1990

African Union Cybersecurity Convention 2014

APEC

APEC Privacy Framework 2004

Australia

Australian Privacy Amendment (Private Sector) Act 2000

Cape Verde

Cape Verdean Constitution 2010

Lei nº 133/V/2001, de 22 de Janeiro Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares 2001

Council of Europe

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981
Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine 1997

European Convention on Human Rights and Fundamental Freedoms 1950

World Health Organisation Declaration on the Promotion of Patients' Rights in Europe 1994

EAC

Draft Bill of Rights for the East African Community 2009

Legal Framework for Cyberlaws 2008 (Phase I)

Legal Framework for Cyberlaws 2011 (Phase II)

Treaty for Establishment of the East African Community 1999

ECOWAS

ECOWAS Treaty 1975

Supplementary Act A/SA.1/01/07 on the Harmonization of Policies and the Regulatory Framework for the Information and Communication Technology (ICT) Sector 2007

Supplementary Act A/SA.1/01/10 on Personal data Protection within ECOWAS 2010

European Union

Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001

Charter of Fundamental Rights of the European Union 2000

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006

Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

General Data Protection Regulation 2016

Protocol No.11 (ETS No. 155) to the European Convention on Human Rights 1998

R *(2010)13 with regard to automatic processing of personal data in the context of profiling 2010*

R *(81) 1 on regulations for automated medical data banks 1981*

R *(83) 10 on the protection of personal data used for scientific research and statistics 1983*

R *(2002) 9 on the protection of personal data collected and processed for insurance purposes 2002*

R *(85) 20 on the protection of personal data used for the purposes of direct marketing 1985*

R *(86) 1 on the protection of personal data for social security purposes 1986*

R *(87) 15 regulating the use of personal data in the police sector 1987*

R *(89) 2 on the protection of personal data used for employment purposes 1989*

R *(90) 19 on the protection of personal data used for payment and other operations 1990*

R *(91) 10 on the communication to third parties of personal data held by public bodies 1991*

R *(95) 4 on the protection of personal data in the area of telecommunication services 1995*

R (97) 18 on the protection of personal data collected and processed for statistical purposes 1997

R (97) 5 on the protection of medical data 1997

R (99) 5 for the protection of privacy on the Internet 1999

Regulation (EC) 45/2001 with regard to the processing of personal data by the institutions and bodies on the Community 2001

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws 2009

Treaty Establishing a Constitution for Europe 2004

Treaty of Lisbon 2007

Kenya

Constitution of Kenya 1963

Constitution of Kenya 2010

Data Protection Bill 2014

League of Arab States

Arab Charter of Human Rights 2004

Morocco

Loi n° 09-08 Relative à la Protection des Personnes Physiques à l'égard du Traitement des Données à Caractère Personnel 2009

New Zealand

Privacy Act 1993

Nigeria

Constitution of Nigeria 1999

OECD

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

OIC

Cairo Declaration on Human Rights in Islam 1990

Charter of the Organisation of the Islamic Conference 2008

Rwanda

Loi n° 44/2001 DU 30/11/2001 Organisant les Telecommunications

SADC

Data Protection Model-Law 2012

Declaration and Treaty of SADC 1992

Senegal

Décret n° 2011-0929 du 29 juin 2011 portant nomination des membres de la Commission de protection des données à caractère personnel

Senegal, Loi n° 2008-12 sur la Protection des Données à Caractère Personnel 2008

Seychelles

Data Protection Act 2003

South Africa

Constitution of South Africa 1996

Constitution of the Republic of South Africa 1993

Customs and Excise Act 1964

Electronic Communications and Transactions Act 2002

Protection of Personal Information Act 2013

Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002

Revenue Laws Amendment Act 2008

Tanzania

Broadcasting Services Act Cap.306 R.E 2002

Constitution of Tanganyika 1961

Constitution of Tanganyika 1962

Constitution of the United Republic of Tanzania 1977

Constitution of Zanzibar 1984

Constitutional Review Act 2011

Data Protection Bill 2014

Electronic and Postal Communications Act 2010

Fair Competition Act, Cap. 285 R.E 2002

HIV and AIDS (Prevention and Control) Act 2008

Human DNA Regulation Act 2009

Interim Constitution of Tanzania 1965

Prevention of Terrorism Act 2002

Regulations and Identification of Persons Act 1986

Tanzania Communications Act Cap. 302 R.E 2002

Tanzania Communications Regulatory Authority Act Cap.172 R.E 2002

Tanzania Intelligence and Security Act 1996

Tunisia

Loi n° 2004-63 Portant sur la Protection des Données à Caractère Personnel 2004

United Kingdom

Data Protection Act 1984

Data Protection Act 1998

Human Rights Act 1998

United Nations

Guidelines for the Regulation of Computerized Personal Data Files 1990

HIV/AIDS and the World of Work, ILO Code of Practice, Geneva 2001

International Covenant on Civil and Political Rights 1966

Protection of Workers' Personal Data, ILO Code of Practice, Geneva 1997

Statute of the International Court of Justice (ICJ) 1945

United Nations Convention on the Rights of the Child 1989

Universal Declaration of Human Rights 1948

United States of America

American Convention on Human Rights 1969

Cable Communications Policy Act 1984

Children's Online Privacy Act 1999

Computer Matching and Privacy Protection Act 1988

Driver's Privacy Protection Act 1994

Electronic Communications Privacy Act 1986

Fair Credit Reporting Act 1970

Family Educational Rights and Privacy Act 1974

Grammm-Leach-Billy Act 1999

Health Insurance Portability and Accountability Act 1996

Privacy Act 1974

Privacy Protection Act 1980

Right to Financial Privacy Act 1978

Safe Harbor Agreement 2000

Telecommunications Act 1996

Video Privacy Protection Act 1988

Zimbabwe

Zimbabwean Access to Information and Protection of Privacy Act Chapter 10:27

Zimbabwean Interception of Communications Act 2007

Table of Cases

Council of Europe

Campbell v United Kingdom (1993) 15 EHRR 137

Gaskin v United Kingdom, ECtHR, Strasburg, Application No. 10454/83[1989]

Malone v United Kingdom (1984) 7 EHRR 14

Pierre Herbecq and the Association Ligue des droits de l'homme v Belgium, Decision of 14 January 1998 on the applicability of the applications No. 32200/96 and 32201/96(Joined) Decisions and Reports, 1999

European Union

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) v Administración del Estado, ECJ Case C-468/10 and C-469/10

Bavarian Lager Co. Ltd v Commission, CFI Case, T-194/04

Bodil Lindqvist v Åklagarkammaren i Jönköping, ECJ Case C-101/01

Direktsia Obzhalvane i upravlenie na izpalnenieto Varna v Auto Nikolovi, ECJ Case, C-203/10

European Commission v Federal Republic of Germany, ECJ Case, C-518/07

European Parliament v Council of the European Union and Commission of the European Communities, ECJ Joined Cases, C-317/04 and 318/04

Kalliopi Nikolaou v Commission, CFI Case, T-259/03

France

Germany

South Africa

Bernstein v Bester NO, 1996(2) SA (A); (2) SA 751 (CC)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, 2004(1) SA 406(CC)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, 2004(1) SA 406(CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd, 1993 (2) SA 451(A)

I & J Ltd v Trawler & Line Fishing Union and Others (2003) 24 ILJ 565(LC)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty); In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO, 2001 1 SA 545 (CC)

Jansen van Vuuren v Kruger, 1993(4) SA 842(A)

Jansen van Vuuren v Kruger, 1993(4) SA 342

Joy Mining Machinery v NUMSA and Others (2002) 4 BLL 372 (LC)

National Media Ltd v Jooste [1996] 3 SA 262(A)

NM and Others v Smith and Others, 2007(5) SA 250

O'Keeffe v Argus Printing and Publishing Co Ltd, 1954 (3) SA 244(C)

PFG Building Glass (Pty) Ltd v Chemical Engineering Pulp Paper Wood and Allied Workers Union and Others (2003) 24 ILJ 974(LC)

Protea Technology Limited and Another v Wainer and Others [1997] 3 All SA 594

S v Kidson, 1999(1) SACR 338(W)

Waste Products Utilisation (Pty) Ltd v Wilkes and Another, 2003(2) SA 515(W)

Tanzania

Attorney-General v Lesinoi Ndeinai & Joseph Selayo Laizer and Two Others [1980] T.L.R 214

Bernado Ephraim v Holaria Pastory and Gervazi Kaizilege, (PC) Civil Appeal No. 70 of 1989, HCT, Mwanza (Unreported)

Christopher Mtikila v Attorney General, Miscellaneous Cause No.10 of 2005, HCT, Dar es Salaam (Unreported)

Chumchua s/o Marwa v Officer i/c of Musoma Prison and the Attorney General, Miscellaneous Criminal Cause No. 2 of 1988, HCT, Mwanza (Unreported)

Director of Public Prosecutions v Daudi Pete [1993] TLR 22

Hatimali Adamji v East African Posts and Telecommunications Corporation [1973] T.L.R. 6

Jackson Ole Nemeteni and 19 Others v the Attorney General, Misc. Civil Cause No. 117 of 2004, HCT, Dar es Salaam (Unreported)

Julius Ishengoma Francis Ndyanabo v Attorney General, Civil Appeal No. 64 of 2001, CAT, Dar s Salaam (Unreported)

Kukutia Ole Pumbun and Another v Attorney General and Another [1993] TLR 159

Legal and Human Rights Centre and Others v Attorney General, Miscellaneous Civil Cause No. 77 of 2005, HCT, Dar es Salaam (Unreported)

Mkami Kasege & Ismail Msengi v Risasi, Conciliation Case No. 1 of 2005, 1997-2007, MCT 111

Re Innocent Mbilinyi, Deceased [1969] H.C.D 283

Sia Dominic Nyange v Mwananchi Communications Ltd, Civil Case No. 155 of 2005, the Resident Magistrate's Court of Dar es Salaam, Kisutu (Unreported)

United Kingdom

Common Services Agency v Scottish Information Commissioner [2008] UKHL 47

David Paul Johnson v the Medical Defence Union [2007] EWCA Civ 262

Michael John Durant v Financial Service Authority [2003] EWCA Civ 1746

Wainwright v Home Office [2003] UKHL 53; [2003]3WLR 1137

William Smith v Lloyd TBS Bank plc [2005] EWHC 246(Ch)

United States of America

Griswold v Connecticut, 381 U.S. 479 [1965]

1. Introduction

1.1 Background

For decades, the Constitutional right to privacy has played a vital role in privacy protection in many African countries. However, only two countries, namely Kenya and South Africa managed to judicially interpret and define the scope of the right to privacy.[1] Meanwhile, the adoption and use of ICTs including cloud computing are increasing by the day. In 1999, only 10% of the African population had access to ICTs[2] (at least a connected mobile phone), ten years after, in 2009 it was 38.0%, and in 2016 it was 80.8% per 100 inhabitants.[3] Furthermore, between 2014 and 2015 when the international internet capacity in Europe, US and Canada had slowed at 33% compounded annually, international internet capacity connected to Africa grew by 41% to 51% compound annually between the year 2011 and 2015. (TeleGeography) In fact, in 2012, there were 650 million mobile subscriptions in Africa, exceeding the statistics in the US or the European Union, making Africa the second fastest growing region in the world after South Asia.[4] This is said to be just the beginning of the growth curve in ICT usage.[5] In contrast with the Western world, in Africa, mobile devices are mostly used to access different services than fixed broadband. Mobile connectivity is in Africa, preferred due to low- cost handsets and business models that lower the cost access such as pre-paid air time.[6]

ICT connectivity and usage continue to grow in the absence of proper regulation in place to regulate user pattern, safeguard individual privacy and protect personal data. In 2001 Cape Verde became the first African State to adopt a comprehensive framework for data protection, yet, to date there is no established supervisory authority for the enforcement of the law. The African Union adopted the Convention on Cyber Security and Data Protection (The Malabo Convention) in June 2014. Malabo Convention is a closed Convention and requires ratification and accession of at least fifteen (15) Member States to come into force. So far, as of 26th April 2017, only eight (8) out of 54 Member States has signed,[7] none of the AU Member States have ratified the Convention.

Regardless of the Malabo Convention's unpopularity, States had and continued to reform their legal system by establishing data protection regimes. 18 out of 54 States have adopted data protection legal frameworks while 19 States have either Bills or draft Bills pending before their

[1] See e.g.; Makulilo, A.B., 'Myth and reality of harmonisation of data privacy policies in Africa', Computer Law & Security Review, 2015, Vol.31, No.1, pp.78-89, at pp.80-81.
[2] Donovan, K. P and Martin, A. K., 'The Rise of African SIM Registration: the Emerging Dynamics of Regulatory Change', First Monday, 2014, Vol. 19, No. 2-3, DOI: http://dx.doi.org/10.5210/fm.v19i2.4351.
[3] http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx accessed on 20.04.2017
[4] Kearney, A. T., 'African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services'; Prepared for GSM Association, http://www.gsma.com/spectrum/wp-content/uploads/2011/12/Africa-Mobile-Observatory-2011.pdf accessed 07/06/2016.
[5] Yonazi, E et al(Eds)., 'The Transformational Use of Information and Communication Technologies in Africa', eTransform Africa, p. 33.
[6] Castells, M et al., Mobile communication and society: A global perspective. Cambridge, Mass.: MIT Press, 2007.
[7] Benin, Chad, Congo, Guinea Bissau, Mauritania, São Tomé and Principe, Sierra Leone and Zambia.

legislative bodies or are undergoing internal review respectively.[8] It is imperative to note that out of the 18 African countries with data protection laws, only a few of them have brought their laws into force and full enforcement.

Lack of data protection regulation means sensitive information such as criminal, health and sensitive financial data are shared across institutions and mobile operators with no comprehensive regulation on ground.[9] The growing social and economic dependence on ICT's and the ease cross-border communications, financial transactions, and sharing of data and information in Africa creates vulnerability on personal privacy and data security.

European Union has now adopted the General Data Protection Regulation (GDPR)[10] to replace the Data Protection Directive of 1995 (DPD).[11] The DPD has been a 'model law' for data protection legislation in Europe since its adoption in 1995. It contains rules regulating a specific type of data; from the way such data is collected, registered, stored, shared and used. The DPD was a result of the growth in information technologies and globalization process which threatened personal privacy. The DPD establishes a system to regulate personal data as a distinct legal regime from the general right to privacy.

The establishment of a separate legal regime to regulate data privacy was suggested as early as 1890 by Brandeis and Warren by serious proposals were made in the 1970s.[12] Reasons advanced for the inevitability of data protection regulation includes the emergence of networks that simplifies data sharing and allowing access to wider range of personal data;[13] enhancing organizational efforts, profitability, collection, collation, dissemination, use and reuse of personal data across organizational boundaries,[14] all of which increased vulnerability in data.

Perhaps, for purposes of general understanding, it is imperative to elaborate how personal data can lead to security and privacy issues. The collection and processing of personal data are not a problem by itself;[15] but it increases data vulnerability, threatens its security, potentially violate the right to privacy and damage data subject's confidence especially in online transactions. As explained by Bygrave and Clarke, this new pattern in usage and sharing of personal data increased fear on individual privacy and on personal data security exuberated with technological

[8] African countries with data protection laws are Cape Verde, Mauritius, Seychelles, Madagascar , Sao Thome and Principe, Republic of South Africa, Morocco, Tunisia, Senegal, Burkina Faso, Gabon, Zimbabwe, Ivory Coast, Ghana, Benin, Angola, Lesotho and Mali. African countries with either data protection Bills or draft Bills are Algeria, Chad, Democratic Republic of Congo (DRC), Ethiopia, Ghambia, Guinea Bisau, Kenya, Liberia, Malawi, Mauritania, Namibia, Niger, Nigeria, Rwanda, Sierra Leone, Swaziland, Tanzania, Togo and Uganda.

[9] For comprehensive discussion about this, see e.g; Makulilo, A. B., The Right to Privacy Relating to Credit Reporting: A Critical Review of the Emerging Africa's Credit Reference Market, Journal of Internet Law, 2016, Vol. 19, No. 9, pp. 3-17.

[10] Adopted by the EU Parliament on 14/06/2016.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[12] Birnhack M. D., 'The EU Data Protection Directive: An Engine of a Global Regime' Computer & Security review, 2008, Vol.24, No.6, pp. 508-520, at p. 511.

[13] Roos, A., 'Data protection' in van der Merwe, D., Information Communication Technology Law, LexisNexis, South Africa, 2008, p. 314.

[14] Bygrave, L.A., Data Privacy Law: An International Perspective, Oxford University Press, UK, 2014, p.9.

[15] See generally Lee, D. J et al., 'Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection', MIS Quarterly, 2011, Vol. 35, No.2, pp. 423-444.

and organization developments in processing personal data.[16] Individuals worry about loss of control over their data once subjected to automated systems, possible abuses by government institutions with established centralized data banks.[17] Roos elaboration of what Bygrave and Clarke terms as a 'new pattern' in the usage of personal data gives a clearer picture. She says;

> '….with the development of personal computers (the PC) linked by means of communication networks, including the Internet, it was no longer necessary for an institution to keep all its information on a particular machine, at a particular place or even in a particular country. Networks enabled more users to gain access to a wider range of personal information. In theory, all the information kept by different organisations (such as financial, medical, educational or employment records) can be shared by different computer users across networks. The notion of information that is stored in a file, therefore, became outdated. The emphasis moved from the threat posed by computers to the threat posed by the much wider concept of Information Communications Technology (or ICT). ICT technology makes it possible for vast amounts of personal information to be collected, stored indefinitely, processed in various ways and disseminated to an unlimited number of third parties'[18]

The risks go beyond the sharing or unauthorized access to personal data; it includes the possibility of processing of inaccurate, incomplete and/or irrelevant personal data. With automatic processing, the risks are inflated; as Merwe narrates, 'it is very difficult to check the contents of a storage system because information is stored in a form which is not immediately intelligible. The volume, range and nature of the data stored may be enormous. [It also] increases the possibility of intercepting, storing, matching, sharing, mining.'[19] With the use of internet, data subject leaves 'footprints' which can enable collection of further data on data subject. Also, tracking technologies can be very intrusive to individual privacy.[20] To secure individual privacy, autonomy and integrity as the basis for democratic, pluralistic society in the face of massive growth in data processing, specific data protection regulations became indispensable.[21]

Pre-existing rules or the blanket Constitutional privacy rights are therefore considered insufficient and unfitting to address the intricacies of privacy issues raised by these developments.[22] The law of tort, common law principles of the law of trust and contractual obligation are no longer well fitted to address such challenges with an adverse impact on personal privacy.[23] Warren and Brandeis elaborate;

---

[16] Bygrave(n14), p.10; Clarke, R., 'Information Technology and Datavaillance', Communications of ACM, 1988, Vol. 31, No. 5, pp.498-512, at pp.505-508

[17] Roos, A., 'Privacy in the Facebook Era: A South Africa Legal Perspective, South African Law Journal, 2012, Vol. 129, No. 2, pp. 375-402 at p. 377

[18] Ibid.

[19] Roos (n 13).

[20] Ibid, p. 315.

[21] Bygrave (n 14), p. 8.

[22] Warren, S.D and Brandeis, L.S., 'The Right to Privacy', Harvard Law Review, 1890, Vol. 4, No. 5, pp. 193-220.

[23] Ibid, pp. 198-199, 'the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action. It deals only with damage to reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows'.

> 'The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will.'[24]

Warren and Brandeis argument was that the law in the protection of personal privacy and data could be made 'by the analogue in the law of libel and slander, of cases which deals with a qualified privilege of comment and criticism on a matter of public and private general interest'.[25] Indeed, analysts such as Makulilo[26] suggest this to be the birth of the modern conception of data protection. Bygrave[27] supports this on account that privacy and data protection law is a result of pre-existing rules more obvious are the rules on right to privacy and protection of personality but also rules on defamation, as was suggested by Warren and Brandeis.

In 1945, the CoE decided to make the UNDHR right to privacy a distinct right. Consequently, nations established legal regimes to protect individual privacy. This, according to Scott Rempell was taken as means for the protection of private affairs of the citizens in the aftermath of the Second World War to restrict public officials on the degree of scrutiny previously afforded by the Nazi party leadership.[28]

In the wake of 1960's, the right to privacy became a major concern, with technological innovation and development making personal data easily collectable, stored and shared. International organizations and institution started to devise means to control the effect of technology on privacy by devising rules and regulations. And with the wisdom of scholars such as Alan Westin, privacy came to be formulated as a legal right which a person can claim. Westin redefined privacy as a 'right in which a person has the ability to control how much about oneself can be revealed to others'[29] the concept which Marc Rotenberg, the executive director of the Electronic Privacy Information considers it to be the cornerstone of the modern right to privacy. Eventually, the concept of privacy progressed into a form of positive informational rights tasking information handlers with certain responsibilities in situations implicating individuals' right to privacy.[30] This was the birth of data protection regulation as a separate legal regime; as previously stated. During this period, researches[31] in this field emerged as well.

---

[24] Ibid, pp. 214-215.
[25] Ibid.
[26] Makulilo, A.B., 'Protection of Personal Data in Sub-Sahara Africa', PhD thesis, Universität Bremen, 2012, p.1.
[27] Bygrave (n14).
[28] Rempell, S., 'Privacy, personal data and subject access rights in the European Data Directive and implementing UK statute: Durant v Financial services authority as a paradigm of data protection nuances and emerging dilemmas', Florida Journal of International Law, 2006, Vol. 18, pp. 807-840 at p. 814.
[29] Alan, F.W., Privacy and Freedoms, Atheneum, New York, 1967, p. 7.
[30] Rempell (n28).
[31] The first research on the topic was conducted in 1970 by the Norwegian Research Centre for Computers and Law aiming at issues of 'Computer and Law'. The result of this research was a seminar qualified by the Centre as 'day of birth,' http://www.jus.uio.no/ifp/english/about/organization/nrccl/ accessed on 02/05/2014

Apart from technological development, Banisar[32] considers this evolution as resistance against governmental abuses and prevention of such abuses that implicates citizens' privacy manifesting in personal information. Also is the strategy to ensure the swift and safe approach to embracing technological development while ensuring compatibility with international and regional standards. This regime for the protection of personal privacy in data emerged with the adoption of data protection laws which Bennett[33] refers to as 'group of policies designed to regulate the collection, storage, use and transmittal of personal information'.

The German State of Hesse was the first to enact Data Privacy Act (*Hessiches Datenshutzgesetz*) on 30 September 1970,[34] followed by other German States. In 1973 the world witnessed the first national wide data protection law enacted in Sweden, the Swedish Data Act (*Datalagen*). The Swedish Data Act provided what we currently recognize as a basic set of protection principles. Later on, other countries in the Western world enacted data protection laws. However, it is worth noting that, Germany was the first country to interpret and implement data protection principles in its strictest sense. This happened in 1983 in *Volkszählungsurteil* (Population Census Case) when the Germany Federal Court interpreted the Federal Data Protection Act of 1978 in restricting potential violation of statistical census. The Court in interpreting provisions of the Federal Data Protection Act and Article 1 and 2 of the German Constitution (*Grundgesetz*) on general human freedoms formulated fundamental and general requirements for data collection and processing. The formulation led to the emergence of the fundamental right to information self-determination (*Informationelle Selbstbestimmung*). According to the Court, this right can only be curtailed if legally permitted by the Constitution and the laws but in compliance with the principle of 'proportionality'.[35]

The other States in Europe followed the trend by enacting domestic legislation to protect personal data and privacy. These domestic legislations were adopted in an uncoordinated manner, resulting in laws with varied standards, some with stricter principles and enforcement mechanisms than others. As a consequence, there was uneven protection, which also affected realization of internal markets and growth of European computer industry.[36] This, as explained by Rampell, threatened member states' integration efforts,[37] hence called for a Europe-wide harmonized regime.

In 1980 OECD adopted Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.[38] The aim was to harmonize data protection practices and offer guidelines in data

---

[32] Banisar, D., 'Privacy and Data Protection Around the World', Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13th September 1999, pp.1-5, at p.1, available at http://www.pcpd.org.hk/english/infocentre/conference.html accessed 20/05/ 2014.

[33] Bennett, C.J., Regulating Privacy: Data Protection and Public Policy in Europe and United States, Cornell University Press, Ithaca/London 1992, p. 13.

[34] At Federal level, the first data protection law in Germany was adopted in 1977 and came into force on 1 January 1978.

[35] Judgment of the Federal Constitutional Court of 15 December 1983, Case No. : 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83.

[36] Bygrave (n 14), p. 55; See also, Schoeman, F.D., Privacy and Social Freedom, Cambridge University Press, USA, 1992, Chapter 7.

[37] Rempell (n 28).

[38] The OECD Guidelines contain eight data protection principles including collection limitation principle, purpose specification principle, use limitation principle, data quality principle, security safe guard principle, openness

protection legislation. As the name suggests, they are mere guidelines with no binding force; although highly recommended by CoE as a model when member countries develop domestic legislation.[39] According to Michael Kirby, the chairman of OECD Expert Group in a formulation of the Guidelines, these Guidelines were meant to address the challenges of evolving technology to privacy and data security and the need to harmonize trans-border data flow rules.[40] [41]

These efforts led to the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108 or Convention 108)by CoE in 1981. Convention 108, unlike the Guidelines, is binding on Member States but has a limited scope of application than the Guidelines. Convention 108 is based on resolutions and recommendations by the CoE made in late the 1960s and early 1970s; specifically Resolutions (73)22 and (74)29 on the Protection of the Privacy of Individual vis-à-vis Electronic Data Banks in private and public sectors respectively.[42] Commentators suggest that the Convention borrowed from pre-existing data privacy laws such as the Hessian Data Protection Act of 1970, Swedish Data Act of 197, Draft Legislation for Belgium in 1972 and the US Fair Credit Reporting Act of 1970.[43] The Convention mainly focused on the weaknesses in the protection of privacy on personal data in a computer evolution era.[44] Makulilo suggests, its adoption is not only an indication of member states lack of adequate laws in protection of personal privacy and data[45] but also a phenomenon Fleischer terms as a mission to rescue uncoordinated and uneven nature of EU Member States rules in data protection.[46] Perhaps this explains the fact that it has been ratified by 45 out of 47 CoE Member States.

---

principle, individual participation principle and accountability principle. It also contains a requirement for establishment of a supervisory authority to oversee and implement the principles.

[39] Recommendation of the Council concerning Guidelines governing the protection of Privacy and Trans-border Flow of data, (adopted 23 September 1980); (C(80)58/FINAL).

[40] Kirby, M., 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' International Privacy Law, 2011, Vol. 1, No. 1, pp. 6-14 at pp. 6-8.

[41] The explanation memorandum 25 to the Guidelines states the objectives as:

> a) Achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;
> b) Reducing differences between relevant domestic rules and practices of Member countries to a minimum;
> c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and
> d) Eliminating, as far as possible, reasons which might induce Member countries to restrict trans-border flows of personal data because of the possible risks associated with such flows.

[42] Council of Europe, Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector (Adopted by the Committee of Ministers on 20 September 1974); Council of Europe, Resolution (74) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector (Adopted by the Committee of Ministers on 26 September 1973).

[43] Bygrave (n 14), p. 33; Makulilo (n 26), p. 145.

[44] ETS 108 came as a necessary measure to reconcile fundamental values of the respect for privacy and the free flow of information between peoples. ETS108 contextualized right to privacy by defining personal data, automatic processing, storage of data, carrying out of logical and/ or arithmetical operations on data, their alteration, erasure, retrieval or dissemination. See Additional Protocol to the Convection for the protection of individuals with regard to Automatic Processing of Persona Data regarding supervisory authority and transborder data flow; November 8 2001. C.E.T.S. No. 181.

[45] Makulilo (n 46).

[46] Fleischer, P., 'The Need for Global Privacy Standards' UNESCO Conference, Ethics and Human Rights in Information Society, 13-14 September 2007, Strasbourg.

The Convection contains the same privacy and data protection principle as the OECD Guidelines, although the former deals only with data in computerized (automated) systems. Its Article 3 (2)(c) encourages an application of the same principles even to manually processed data and employing additional measures in safeguarding privacy in personal data (Article 11); while permits departure from its principles when a country meets criteria under Article 9 and 11 of the said Convection. Bygrave submits that the Convection was intended to act as a catalyst and a guide for national legislative initiatives not to short-circuit them. Hence he cautions against taking the Convention as a finished package with directly applicable rules.[47]

In 2001 CoE complemented Convention 108 with an adoption of the Additional Protocol to the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flow. The amendments were aimed at calling the Member States to put in place an independent data protection authority.[48] Perhaps it is worth noting that CoE, has, through the Convention 108, adopted several sector-specific Recommendations to address emerging risks and uniqueness of different sectors.[49] In its present status, the Convention binds Member States, although article 23 mandates the CoE Committee Ministers to invite non-member States to accede to upon request.

The need for a European harmonization of the data protection regime resulted in the 1990 draft data protection framework adopted in 1995 as a Directive.[50] The Directive (DPD) drew inspirations from the OECD Guidelines and Convention 108. Like Convention 108, the DPD is legally binding but unlike Convention 108, is enforced by the ECJ making it the first international instrument with the strongest data privacy enforcement mechanism. The DPD, as Greenleaf puts it, came to strengthen the previous codes; the OECD Guidelines and Convention 108.[51] This is also evidenced by the instrument itself which under Recital 11 admits to having

---

[47] Bygrave (n 14), p. 36.

[48] See Additional Protocol to the Convection for the protection of individuals with regard to Automatic Processing of Persona Data regarding supervisory authority and transborder data flow; November 8 2001. C.E.T.S. No. 181.

[49] Recommendation No. R (81) 1 on regulation for automated medical data banks (23 January 1981 and later replaced by Recommendation No. R (97) 5; Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983 which was later replaced by Recommendation No. R (97) 18 with regard to statistics; Recommendation No. R (85) 20 on the protection of personal data used for purposes of direct marketing (25 October 1985); Recommendation No. R (86) 1 on protection of personal data for social security purposes (23 January 1986); Recommendation No. R (87) 15 regulating the use of personal data in police sector (17 September 1987); Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989); Recommendation No. R (90) 19 on protection of personal data used for payment and other operations (13 Septenber1990); Recommendation No. R (95) 10 on communications to third parties of personal data held by public bodies (9 September 1991);Recommendation No. R (95) 4 on the protection of personal data in area of telecommunication services, with particular reference to telephone services (7 February 1995); Recommendation No. R (97) 5 on the protection of medical data (13 February 1997); Recommendation No. R (97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997); Recommendation NO. R (99) 5 on the protection of privacy on the internet (23 February 1999); Recommendation No. R (2002) 9 on protection of personal data collected and processed for insurance purposes (18 September 2002); Recommendation CM/Rec (2010) 13 of the Committee of Ministries to member states on the protection of individuals with regard to automatic processing of personal data in context of profiling (23 November 2010).

[50] The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, was based on the directives of the European parliament and of the council of European Union of 24 October 1995. The Directive sets out the first comprehensive framework for privacy protection in Europe.

[51] Greenleaf, G., 'The influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108', International Data Privacy Law, 2012, Volume 2, No. 2, pp. 68-92, at p. 68.

given substance to and amplified the privacy principles contained in the CoE Convention of 1981.

The DPD was adopted with two main objectives, to protect personal rights to privacy with respect to the processing of personal data, and to provide harmonization of rules relating to trans-border data flow.[52] It is therefore not surprising that the DPD has consistent privacy principles, but somewhat stronger than, those in the OECD and CoE agreements. The DPD added much stronger enforcement requirements, including the establishment of an independent DPA and a right to have disputes determined by the courts'.[53] DPD required its implementation by the Member States by 24 October 1998. It has also incorporated the 1992 Agreement on the Economic Area (EEA) hence binding all EEA Member States as well.

The distinctive feature of the DPD includes the restrictions on data exports to third countries without 'adequate protection' for personal data, an aspect which Bygrave believe to be a predominant concern of the DPD. The DPD has also introduced special rules to relax the restrictions in previous instruments, harmonise national rules and provide for what Makulilo calls 'special rules' for transfer of personal data to third countries.[54] These rules also serve to control data controllers from shifting their operation to countries with lenient data privacy standards.[55] This framework for trans-border data flow found under chapter IV (Articles 25 and 26) of the DPD.

Regardless of its intentions, the DPD has not been able to enforce uniformity in data protection laws within its Member States.[56] Its application is fragmented among the Member States, making its enforcement difficult across Members. The DPD is also considered ill-equipped to address challenges of the growing technology.[57] Consequently, the EU decided to replace the DPD with the General Data Protection Regulation to address the above-mentioned weaknesses. As pointed out by Viviane Reding, the DPD required reforms to address the challenges brought by development in modern technology, globalized data flows and access to personal data by law enforcement authorities, growth of modern devices, web-user generated contents, the outburst of social networking sites, cloud computing technologies all of which postdate the DPD.[58] The GDPR has been created as a more cohesive instrument to provide a balanced framework of law which applies the same data protection rules to all fields of EU activities.[59]

---

[52] Directive 95/46/EC; Article 1 (1) (2) and Recitals 8, 9, 10, 11.
[53] Greenleaf (n51).
[54] Makulilo (n 26), p 168.
[55] Der Datenschutz im grenzüberschreitende Datenverkehr: Eine rechtsvergleichende und kollisionsrechtliche Untersuchung,Baden-Baden: Nomos, p. 87 cited in Makulilo(n 26)p.54
[56] Polcˇa´k, R., 'Getting European data protection off the ground', International Data Privacy Law, 2014, Vol. 4, No. 4, pp. 282-289, at footnote 39; Koops, B., 'The trouble with European data protection law', International Data Privacy Law, 2014, Vol. 4, No. 4, pp. 250-261, at p. 260; LRDP KANTOR Ltd and Centre for Public Reform., Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Final Report, 20 January 2010, pp.27-42.
[57] See e.g., Reding, V., 'The Upcoming Data protection Reform for the European Union', International Data Privacy Law, 2011, Vol 1, No. 1, pp. 3-5, at p. 3.
[58] Reding (n 57); Reding, V., 'The European data protection framework for the twenty-first century', International Data Privacy Law, 2012, Vol. 2, No. 3, pp. 119-129; Rotenberg M and Jacobs D., 'Updating the Law of Information Privacy: The New Framework of The European Union', Harvard Journal of Law & Public Policy, 2013, Vol. 36, No. 2, pp. 605-652 at pp. 623-624; see also Makulilo(n 26), pp. 194-199.
[59] Rotenberg and Jacobs (n 58), pp. 630-631.

While these developments take place in the Western, that is, the recognition of right to privacy as a distinct legal regime around 1970's,[60] and regional harmonization in 1980's and the current development with the GDPR in 2016; in Africa, most States still relies on the constitutional right to privacy as a regime for data protection. A few that have adopted the comprehensive data protection regimes have yet to implement these laws. The laws are also said to have been adopted hastily in responding to restrictions to trans-border data flow under DPD.[61] In an inevitable effort to maintain international trade, information sharing and e-commerce; as a result, many of the reforms are a replication of the DPD in a 'cut and paste' basis.

Moreover, domestic reforms have triggered reactions at regional and sub-regional level. The Malabo Convention of June 2014[62] establishes, under its part II, standards for a legal framework for the protection of personal data. The Malabo Convention is promulgated to address security challenges brought by development in technology; and aims at the protection personal data, harmonization of cyber laws across Africa and promotion of electronic commerce.[63]

Sub-Regional frameworks on data protection started before the Malabo Convention. It started in 2010 within ECOWAS,[64] followed by EAC Legal Framework for Cyber Laws 2010, and SADC in 2012.[65] These Sub-Regional instruments were not only adopted as a response to the extra-territorial mechanism of the DPD but also copied the DPD, some mimicry (with exception to the EAC Frameworks). The assumption for this approach in reforms is perhaps their need to meet the adequate level of protection which is associated with transposition of the DPD.

This approach, as clarified by Birnhack suggests the initiatives signify global 'consensus' towards data protection with a slow but steady process of globalization of data protection standards in expectation to meet the equivalence test by the EU.[66] Unfortunately, Birnhack forgets that similarity in substance does not necessarily mean identical substance.[67] Data protection legislation is more contextual than substance. Factors such as political environment, economical, legal and cultural aspects are vital. They affect how the substance/content is interpreted and applied and hence determine the adequacy of the overall protection framework.

Diversity in legal culture and structures,[68] perceptions and understanding of the right to privacy (or the concept privacy)[69] has an impact on how a country interprets the basic content and core

---

[60] Bygrave, L.A., Data Protection Law: Approaching its Rationale, Logic and Limit, Kluwer Law International, 2002, p. 2.

[61] Birnhack (n 12), p. 513; Olinger, H. N et al., 'Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol.39, No. 1, pp. 31-42; See also Makulilo, A.B., 'Data Protection Regimes in Africa: too far from the European 'adequacy' standard?', International Data Privacy Law, 2013, Vol. 3, No. 1, pp. 42-50, at p. 50.

[62] On the AU 23rd Ordinary Session in Malabo.

[63] AU Cyber Convention, Paragraph 3.

[64] ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection, in Abuja on 16 February 2010.

[65] SADC Data Protection Model Law of 2012.

[66] Birnhack (n12), p.512.

[67] See e.g., Greenleaf (n51).

[68] According to Friedman, legal culture means 'attitudes, values, and opinions held in society, with regard to law, the legal system, and its various parts'. It is 'those parts of general culture – customs, opinions, ways of doing and thinking – that bend social forces toward or away from the law and in particular ways. Accordingly, the legal culture is the one which 'determines when, why and where people use law, legal institutions or legal processes; and when they use other institutions or do nothing. In other words, cultural factors are an essential ingredient in turning a static structure and a static collection of norms into a body of living law. Adding the legal culture to the picture is

rules of the law and eventually the standards implemented within a specific local jurisdiction.[70] Given the fact that there is no definition or clear rule in determining the 'adequate protection',[71] suggests the need to look beyond the substance of the law.

The adoption of the GDPR brings some new dimensions on cross-border data flow. Under the GDPR, all entities outside the EU that process data related to the EU entities or Residents are automatically subjected to the Regulation. The Regulation also makes it a mandatory requirement for data processors to conduct privacy impact assessment for activities likely to pose higher security risks. What does this mean for Africa as a continent and to individual states? Based on the fact that, the Regional instrument (Malabo Convention), Sub-regional and national laws (with exception to South African POPI) are a blue-print of the 'outdated' DPD, would the continent go through an overhaul of the created data protection regimes or seek compromise with the EU? How can Africa attain the sustainability and harmonization of the data protection regimes *vis-a-vis* fluidity in technological developments, global data protection standards and the African legal culture?

---

like winding up a clock or plugging in a machine. It sets everything in motion; see Freedman, L.M., 'Legal Culture and Social Development', Law & Society Review, 1969, Vol. 4, No. 1, pp. 29-44, at pp.35-36. Basically legal culture is the totality of social attitudes, informed by culture and history and countries institutional characteristics and its legal traditions that give a certain rule a meaning and life.

[69] As an example on diverging understanding and treatment of 'privacy' which impacts the standards of regulations adopted by a certain community is given by Saad who compares the concept of privacy as perceived in Islamic communities as against the Westerners. In Islamic communities, privacy is aimed at prohibiting public humiliation of the individual even if it is something of a legitimate concern to the public. This is different from the Western concept of privacy which would seem to allow publication of information of a person's private life if there is legitimate concern. He continues saying that, 'even without the existence of law, privacy is a concept recognized in various cultures, but depending on cultural setting, each society has its own attitude and perception towards what amounts to privacy'. In illustrating this, the author proceeds with a comparative analysis of privacy perceptions among the Germans, Americans, French and English. He discovered that:…' the Germans marked of their private *Lebebentsraum* by closed doors, fences, and strict rules about trespass. German law, for instance, forbids the photographing of strangers in public places without their consent. Americans have open doors and no fences, but mark their social status with 'private' offices and 'private' secretaries. The French pack closely together in public, but rarely invite outsiders to their homes, even if they know them well. And the English, it seems rely mainly on their reserve: when an Englishman stops talking, that is a signal that he wishes to be left alone', Saad, A. R.., 'Information Privacy and Data Protection a Proposed Model for the Kingdom of Saudi Arabia' (unpublished). In African context too, authors like Olinger et al (n 61), explain that, privacy has been affected by the African culture of collectivisms as opposed to individualism which is the case in the Western culture. This means, unlike in the West where individualism is a pre- condition for existence of attitudes and values for privacy, in African states an individual cannot claim right to privacy as an individual in Africa lives in associations.

[70] In this context, Tabalujan emphasizes that, legal culture has an impact on the way privacy is perceived and interpreted, which means social beliefs and norms of the receiving community and the people's willingness and capacity to scour for, understand and obey new laws are important factors which help determine the success of law that is transposed; Tabalujan B.S, Legal Development in Developing Countries: The Role of Legal Culture, Singapore, 2001, p. 9. Allan Watson further elaborates on the role of legal culture in legal reforms when he said; 'All lawmakers, including legislators, are controlled by their thinking about law, their knowledge of concepts, and the parameters of legal reasoning that they have unconsciously set for themselves. The different sources of law have different impacts on legal change, but at all times and in all places the approach of the lawmakers is affected by their particular legal culture… This culture has to be understood and injected into the equation before one can begin to erect a theory of law and society'. Watson, A., Legal Transplant: An Approach to Comparative Law, 2nd Ed, London, The University of Georgian Press, p.108.

[71] This is despite the fact that Article 25 (2) of the Directive establishes rules in assessing the 'adequate level of protection' stating, 'regard shall be given to all circumstances surrounding data transfer operation or set of data transfer operations taking into account in particular the nature of the data, purpose and duration of the proposed processing operation(s), the country of origin and country of final destination, the rules of laws, both general and sectorial in force in the third country in question and the professional rules and security measures which are complied with in that country'.

1.2 Methodological Approach and Rationale

1.2.1 Research Problem

Initially the research was set to look at the lack of legal harmonization in data protection regulations in Africa and its effects on the protection of personal data. However, with the adoption of the Malabo Convention and GDPR in Europe, the research intends to assess data protection regimes in Africa (their approaches, the established frameworks and harmonization prospects) and the African place in the global data protection map. In doing so, the research looks into the challenges involved in developing balanced legislative frameworks in view of African local conditions and legal culture against globalized standards. This is done while focusing on the central theme of these reforms, i.e. data protection. The research looks into external motivations for reforms as well as internal environment for the reception and functioning of the data protection regimes in Africa. This is to enable a determination of the value and the future of data protection regimes within and beyond Africa.

It is important to keep in mind that privacy and data protection regulation in the Internet age is not a simple task. Borena Berhanu et al,[72] posit, 'With the proliferation of global information systems, particularly SNS that collect trans-border data, the regulation process require an understanding and involvement of different parties and cultures. Implementing privacy regulations, with the commitment of every player (businesses, government, and citizens in different parts of the world), needs a compromise and a finding of a common ground'. Hence, establishing data protection regimes calls for a more holistic rather than a monolithic approach.[73]

Furthermore, development in ICTs also alters standards of protection within trade networks. It means, a simple transplanting of a data protection regime in a 'copy and paste' basis may not yield the expected results. In fact, the APEC Framework is an example of this scenario. The APEC Framework transplanted the OECD Guidelines, at the time when it had more than 20 years since its formulation. As a result, the Framework proved redundant in regulating data protection in the modern technologies and their usage patterns.[74] Furthermore, the APEC framework (like many data protection laws in Africa) fails to recognize privacy safeguards as fundamental rights suggesting its unlikeliness to pass the 'adequacy' assessment.[75]

Initially, the reforms in African States were a response to restrictions in cross-border data flow under Articles 25 and 26 of the DPD. These provisions requires third countries to either

---

[72] Borena, B et al., 'Information Privacy Protection Practices in Africa: A Review through the Lens of Critical Social Theory', 2015 48th Hawaii International Conference on System Sciences.

[73] See commentators such as Bygrave, L.A., 'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, 2010, Vol. 56 , pp. 165-200, at p. 194; Svantesson, D.J.B., 'A "Layered Approach" to the Extraterritoriality of Data Privacy Law', International Data Privacy Law, 2013, Vol. 3, No.3, pp. 278-286; Moerel, L., 'The long arm of EU Data Protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by website worldwide?', International Data Privacy Law, 2011, Vol.1, No.1, pp.28-46; Moerel, L., 'Back to Basics: When does EU Data Protection Law apply?', International Data Privacy Law, 2011, Vol.1, No.2, pp. 92-110.

[74] Greenleaf, G., 'Australia's APEC Privacy Initiative: The Pros and Cons of the "OECD Lite"', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 1-6; Greenleaf, G., 'APEC Privacy Principles: More Lite with every version', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 105-111; Greenleaf, G., 'APEC's Privacy Framework: A New Low Standard', Privacy Law & Policy Reporter, 2005, Vol. 11, pp.121-124.

[75] Makulilo (n 26), p. 218.

implement their own personal data protection laws with adequate (similar) levels of protection; enter into standard compliant contract(s) or face data flow restrictions from EU Member States. The former option appears to be an easier and more forthcoming route. The latter option proves, from experience learned from the US-EU Safe harbor and the Privacy Shield, undesired option and can only be tolerated in compelling situations.[76]

Consequently, data protection reforms in Africa took a form of direct importation of the DPD rather than adoption of a new law or refashioning of existing rules. In most States, no serious discussion or public consultations were conducted.[77] It is possible this is caused by lack of expertise in the area of data protection, hence making the reforms a mere legal drafting process. The process ignored the crucial aspect of public consultation, a very important step in validating legal reform processes.[78] More fascinating is the fact that the reforms in privacy and data protection were done through Ministerial Departments[79] instead of the conventional route through law reform agencies.

The 'cut and paste' of the DPD approach as a 'strategy' to reform data protection regimes in Africa may still not bring the expected results. Greenleaf in his analysis of the OECD

[76] US-EU Safe Harbour was able to come to a conclusion first because both US and EU are powerful and highly independent economic entities hence have comparable bargaining power which eliminates the possibility of one party to dictate the terms leading to a 'cooperative form of policy coordination' and the fact that EU is the US biggest trading partner and this is evidenced by the fact that, a year after coming of the Directive 95/46/EC into force, US had 350 billion dollar in trade with EU. Long, W.J and Quek, M.P., 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbor Compromises', Journal of European Public Policy, 2002, Vol.9, No. 3, pp. 325-344, at p. 326; see also, Roos, M., 'Definition of the Problem: The Impossibility of Compliance with both European Union and United States', Transnational Law & Contemporary Problems, 2005, Vol. 14 No. 3, pp1137-1162.
And against all odds, the EU (during negotiations) still insisted that the only way to provide adequate level of protection is through legislation. Farrell, H., 'Negotiating Privacy across Arenas: The EU-US "Safe Harbor" Discussions' in Héritier, A.,(ed)., Common Goods: Reinventing European and International Governance, Rawman & Littlefield, Boulder/New York/ Oxford, 2002, pp.101-123 at p. 107. Yet despite passing the 'adequate test in 2000, Article 29 WP insists that the approach does not provide adequate level of protection, and such determination was made as *'affirmative action'* or '*Adequacy without qualification'* resulting to the Commission itself drafting reports on its weakness to provide 'adequate level of protection', Makulilo(n 26), pp. 214-215; see also, Article 29 Working Party., 'Working Document of Functioning of the Safe Harbor Agreement', 11194/02/EN,WP 62, (adopted on 2 July 2002); European Commission., 'Commission Staff Working Document on the Implementation of the Commission Decision 520/2000/EC on the adequacy protection of personal data provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S Department of Commerce', SEC82004) 1323, Brussels, 20.10.2004.

[77] This is except for South Africa which took about twelve years of serious discussion and considerations both of the law, its nature, effect and acceptance in the local environment based on the local understanding and circumstances before it was finally adopted in 2013. See also Makulilo, A.B., 'Data protection and law reform in Africa: a systematic or flawed process?', International Journal of Technology, Policy and Law, 2016, Vol. 2, Nos. 2/3/4, pp. 228-241 at p.233.

[78] Commenting on Mauritius perspective, the EU consultant report noted lack of awareness in privacy and data protection from both private and public sectors and including the office of the Prime Minister who was front liner in adoption of the law, Confidential report, 'Ensuring the compliance of the data protection legislation and principles of Mauritius with EU standards, 2011'; the fact that made Makulilo to assess enforcement practice and came up with a an observation that the Commissioner was accepting the defense of 'ignorance of law' or 'lack of awareness of law' in determining complains lodged before her, Makulilo, A.B., 'Mauritius Data Protection Commission: an analysis of its early decisions', International Data Privacy Law, 2013, Vol.3, No.2, pp.131-139. Even the Mauritanian data protection Commissioner at one point suggested her office's lack of expertise in the area by requesting the government to hire an international expert on data protection to assist her in the discharge of her everyday duties as a data protection Commissioner, Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.14.

[79] Makulilo (n 77), pp. 231-232.

Guidelines, Convention 108, the APEC framework and the EU Directive said, 'similarity does not necessarily means identical substance',[80] [81] and even the language difference used on similar rules can bring different results on the same subject matter.[82] Moreover, adequacy determination basically assesses two aspects, the content of protection offered and the mechanism in place for the implementation of the law. Besides, based on the European Commission practice in assessing adequacy of protection it reveals that, the assessment goes beyond the above levels set by the DPD and Article 29 Working party in WP 12 and WP 4;[83] it looks at what Makulilo refers to as 'extraneous latent considerations' not envisaged by WP 12 or WP 4 and the DPD. There are political considerations, the economic importance of the country to the EU and amount of data likely to be transferred between the third country and EU Member States.[84]

Article 29 Working Party confirms this when it declared that the assessment criteria set should not be set in a stone; 'in some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements.[85] This eliminates the element of predictability and brings uncertainty even when third countries have imitated the accepted standards within the EU data protection instruments; good example is Tunisia. It also means, a country may not transpose the DPD (or any other framework) nevertheless she can pass the adequate protection determination; a good example being the State of Israel whose adoption of data privacy law pre-dates[86] the DPD but has passed the 'adequate protection' standard.[87]

The additional and quite mystified evaluation procedure and assessment criteria above the two known and publicized (within the DPD, WP 12 and WP 4), give third states under reform little reference in satisfying the 'adequacy' test. In fact, the 'unknown' methodologies applied in the assessment process have raised a lot of questions on their implication for policy making in third countries.[88] One of such reports is the commissioned report to the Research Centre on IT and

---

[80] Makulilo (n 77), p. 231.

[81] Taking an example of two African countries (South Africa and Mauritius) influenced by the EU Directive, adopted comprehensive data privacy law with similar principles but without substantial identical substance and scope. The South African law extends its protections to juristic persons with specific protections to personal data of children while Mauritanian law protects only natural persons without specific protections to children data. Further on export of personal data Mauritian law is premised on 'adequacy' standards set by article 25 of the EU Directive, South African Law made a sight departure, it is not based on 'adequacy' standard as provided under article 25 of the EU Directive rather standard provided under article 26 of the EU Directive applicable when a country fails to pass the 'adequacy' standard. Both approaches are economic based. See also Makulilo (n 26).

[82] "…in order to transport a single word without distortion, one would have to transport the entire language around it….. in order to translate a language, or a text, without changing its meaning, one would have to transport its audience as well', Hoffmann, E., Lost in Translation, London, Minerva, 1991, pp. 272-275; see also Legrand, P., ' What '*Legal Transplants*? in Nelken, D and Feest, J., (eds), Adapting Legal Cultures, HART Publishing, Oxford-Portland-Oregon, 2001, pp. 55-69 at pp. 57-61; who explains the important role of a language in understanding, implementing and validity of a rule across cultures.

[83] Article 29 Data Protection Working Party 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, DG XV D/5025/98, adopted on 24 July 1998) and Article 29 Data Protection Working Party 'First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy' (WP 4, DG XV D/5020/97-EN final, adopted on 26 June 1997)

[84] Makulilo (n 26), p. 177.

[85] Article 29 Data Protection Working Party (n 83).

[86] Privacy Protection Act 5741-1981 (as amended).

[87] See Commission decision of 31 January 2011 on the adequacy of the protection of personal data in third countries Article 25(6) of Directive 95/46/EC available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm accessed on 20.04.2017

[88] Makulilo, A.B., "Data Protection Regimes in Africa: too far from European 'adequacy' standard?", International Data Privacy Law, 2013, Vol.3, No.1, pp.42-50.

Law, University of Namur, Belgium by the European Commission in 2010. The EC wanted to assess the level of data protection in four African countries; these reports raise questions about the methodology used to make adequacy decisions, and its implications for policy making in third countries.

The situation has set researchers and academicians in a goose chase with Graham Greenleaf and Lee Bygrave emerging with conclusions suggesting that, the less interaction with the third country, the more relaxed assessment rules.[89] They offer an example of New Zealand's clearance as providing 'adequate level of protection' despite obvious weaknesses of the law, saying the fact that New Zealand geographical isolation, unlikeliness of EU data transfer to New Zealand and the unexpected reciprocal of marketing with EU limiting data transfers between the two regimes is the reasons that facilitated the positive determination. The inference by Graham and Bygrave above clearly reflects the hard reality of article 25 (2) of the DPD which provides for criteria for assessment in somewhat ambiguous terms. It provides;

> 'The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are compiled within that country'.

What the literature and practice suggests is that, 'adequate protection' assessment is not only unpredictable but also unrelated with the transplanting of the DPD. The 'adequate' finding is subjective and dependent on factors beyond the content of the law and authorities established therein. There are other likely patterns of influence as suggested by Makulilo, Greenleaf and Bygrave above such as country's 'significance' to the EU and its social economic and political stance. Hence, the approach used in Africa to transpose DPD may seem to be a safe and cheap approach and likely to provide the 'adequate protection', but in reality this may be far from the truth.

Secondly, apart from the fact that determination of adequacy goes beyond what is provided in the DPD and WP 12 and WP 4, still no satisfactory details are provided within DPD or elsewhere to offer assistance to that end;[90] and worse still, Member States may as well have different judgment on adequacy requirement.[91] This means a certain practice or law or regime may pass the 'adequacy' determination by the European Commission but fail the same by a particular country and hence restriction of cross border data transfers between such EU/EEA Member State and the third country. A good example here is the case of US-EU Safe Harbour Agreement (SH) which had passed the 'adequacy' determination by the Commission in 2000 but

[89] Greenleaf, G and Bygrave, L.A., 'Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection', Privacy Laws & Business International Report, 2011, No. 111, pp. 8-9 at p. 9.
[90] EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final, 2.4.1.
[91] Greenleaf and Bygrave (n 89).

received a different determination in Germany by the *Düsseldorfer Kreis*[92] ('Dusseldorf Circle'). The *Düsseldorfer Kreis* had decided that SH should not be relied upon by US data importers as meeting the 'adequacy' standards. The decision required German data exporters to carry out minimum checks to ensure that data importers are not only SH certified but also adheres to data protection principles therein.[93]

Again, adequacy of protection may change with time and or circumstances. The Safe Harbour Agreement is yet an example for this. The agreement was considered to create adequate protection for trans-border data transfer between US and EU Member States. This was until on 6 October 2015 when the Court of Justice of the European Union declared the Commission's 2000 Decision on EU-US Safe Harbour invalid. On 6 November 2015, the European Commission adopted a Communication on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement by the Court of Justice in Case C-362/14 (*Schrems v Data Protection Commissione*). The aim was to provide an overview of an alternative tool for transatlantic data transfers in the absence of an adequacy decision. The Agreement has now been replaced with the Privacy Shield Agreement. Yet, the validity of the Privacy Shield is being questioned. This came after the US president signed an Executive Order to enhance public safety within US. The Executive Order amends section 12 of the US Privacy Act and arguably weakens the EU citizens' protection under the Privacy Shield.

In the absence of clear rules, a positive 'adequate protection' determination on third countries is left to a chance and mercy of the Commission and individual EU/EEA Member States. Moreover, the 'adequacy' assessment, gives primacy to privacy and data protection to EU/EEA citizen over the citizen of third country in question [94](refer to the above scenario regarding the Privacy Shield). The approach is likely to undermine third countries' citizens' individual rights and the expected protection if interests of both parties are not well considered in reforms.

In June 2017 when the GDPR comes into force, it will have far more effects to trans-border data flow that the DPD. The GDPR applies to controllers and processors beyond the EU as long as their processing activities relate to or targets EU Member States or individuals from EU Member State. Article 3(1), the Regulation applies to any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, 'regardless of whether the processing itself takes place within the Union or not. Article 3(2) refers to the targeting, by non-EU established controllers and processors, and of individuals 'who are in the Union', for the purposes of offering goods or services to such subjects or monitoring their behaviours. This connecting factor is further specified by Recital 23.

In relation to international transfer of personal data, the GDPR has not changed much the rules which existed under Articles 25 and 26 of the DPD. However, the GDPR tighten the rules

[92] This is a working group of all German supervisory authorities (DPAs) considered by its members as equivalent to Article 29 Working Party but publishes its opinions in a form of 'resolutions' which reflects the position of supervisory authorities.

[93] In this decision which was reached on 28/29 April 2010, the *Düsseldorfer Kreis* resolved to sanction any data exporter who fails to carry out measures to ensure 'adequacy protection' by the US based data importer. see Schmidl, M and Krone, D., 'Germany DPAs Decide EU-U.S. Safe Harbor May Not Be Relied Upon Exclusively', http://www.bnai.com/GermanyDpas/default.aspx cited in Makulilo (n 26), p. 209.

[94] Greenleaf and Bygrave (n 89).

regarding the data subjects' consent on trans-border data transfers. In this case, the GDPR requires all data processors to make sure that the data subject has been sufficiently informed of all the risks of transfer before data can be transferred to a third country.

The framework established under the GDPR requires also a prompt system for data breach notifications, accountability framework and insists on privacy by design by data controllers and processors. The GDPR also gives more power to data subjects regarding their rights to data access and deletion (Art. 17). Article 79 of the GDPR provides that the data subject who considers that his or her rights under the GDPR have been infringed, may choose to bring proceedings before the Courts of the Member State where the controller or processor has an establishment or, alternatively, before the Courts of the Member State where the data subject himself or herself resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers. Article 82(6) clarifies that the Courts of the same Member State have jurisdiction over actions for compensation of the damage suffered as a result of the said infringement.

Chapter V (Articles 44 through 49) of the GDPR governs cross-border transfers of personal data. Article 45 states the conditions for transfers with an adequacy decision; Article 46 sets forth the conditions for transfers by way of appropriate safeguards in the absence of an adequacy decision; Article 47 sets the conditions for transfers by way of binding corporate rules; Article 48 addresses situations in which a foreign tribunal or administrative body has ordered transfer not otherwise permitted by the GDPR; and Article 49 states the conditions for derogations for specific situations in the absence of an adequacy decision or appropriate safeguards. Under the GDPR, adequacy decisions are also subject to periodic review to determine whether the entity still ensures an adequate level of data protection (Recital 107). In the periodic review, the Commission consults with the entity, and considers relevant developments in the entity and information from other relevant sources such as the findings of the European Parliament or Council (Recital 106).

Looking back into Africa, the ongoing reforms may create an enforcement challenge. First there is lack of clarity of the protection offered. Yes, the Malabo Convention, Sub- regional instruments and national laws have adopted comprehensive frameworks for data protection, in the EU style. However none of the available instruments define or even attempt to provide the meaning of privacy within their contexts. Overall, 'privacy' is still an abstract concept in African.[95] Makulilo once asserted, 'there is neither concept nor theory that uniquely deals with privacy in African cultural context'.[96] And although scholars consider privacy as an indispensable structural feature of liberal democratic political systems,[97] not only the Western democracies of the so called first world[98] but also to third worlds like Africa, the African Charter on Human and

[95] Bakibinga, E.M., 'Managing Electronic Privacy in the Telecommunications Sub-sector: The Uganda Perspective', Africa Electronic Privacy and Public Voice Symposium 2004,
http://thepublicvoice.org/events/capetown04/bakibinga.doc accessed on 20/05/ 2014; this is differentiated from Europe for instance, where privacy is a concept based on human dignity and hence a fundamental right.
[96] Makulilo (n 26), p. 277.
[97] Cohen, J.E., 'What Privacy is For?', p. 19; http://ssrn.com/abstract=2175406 accessed on 10/05/2014.
[98] Bygrave (n 60), p.35.

People's Rights[99] lacks provision on right to privacy within its Basic Human Rights provisions. This omission has been considered by Bygrave as a result of African collectivist culture that makes privacy a less important value.[100] It is therefore unclear whether the adoption of the EU frameworks also implies the adoption of the conceptual framework concerning the concept privacy.

The reforms came as a package and did not spare time for the understanding of the concept and maybe christening within local contexts/legal cultures. It is therefore not surprising that data protection is often related with aspects beyond the protection of human rights and fundamental freedoms such as eTrade, cybersecurity, and development strategy. Data protection is viewed only as a 'means to an end' than a fundamental human right.[101] The assumption in the present research is that, data protection legal reforms in Africa are nothing than a response to protect threaten economies;[102] this is why, Bygrave noted, 'even the instruments have less emphasis on privacy and data protection as human rights rather as means to consumer confidence and overcoming trans-border data flow restrictions'.[103]

Understanding of privacy in certain context is crucial in regulating the interests and values which data protection laws aims to safeguard. Bygrave insists, 'the way in which one conceptualizes the interests and values served by these laws is not just an academic interest but has significant regulatory implication. It is pivotal to working out the proper ambit of the laws and, concomitantly, the proper mandate for data protection authorities'.[104] Frowein and Peukert emphasizes on the clarity of the concept; considering the fact that the right to privacy challenged many legal systems of liberal States in the late half of the 20th century.[105] Its understanding is crucial in ascertaining its objectives and affects its protection in a given context. Hence, as long as the broad consensus is that data protection laws are aimed at safeguarding the right to privacy of individual persons against potential intrusive data processing practices, its understanding and contextual conceptualization is essential. More so because its understanding is also necessary in explaining and discharging supervisory and enforcement powers of the data protection

---

[99] OAU, African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), 27 June 1981, entered into force 21st October 1986.

[100] Bygrave, L.A., 'Privacy Protection in a Global Context: A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, pp. 319-348 at p. 343; see also Bygrave (n 73); Bakibinga (n 94), pp. 2-3 and Olinger et al (n 61), pp. 35-36, who through the concept of Ubuntu: *Umuntu ngumuntu ngabantu abanye* translated as 'a person is a person through other persons' explains 'the culture of transparency and openness in *ubuntu* would not understand the need for personal privacy or able to justify it. Thus personal privacy would rather be interpreted as "secrecy". This "secrecy" would not be seen as something good because it would indirectly imply that the *Ubuntu* individual is trying to hide something- namely her personhood……..there is little room for personal privacy because the person's identity is dependent on the group. The individualistic cultures of the West argue that personal privacy is required for a person to express his true individuality. With *Ubuntu* individuality is discovered and expressed together with other people and not alone in some autonomous space, and hence personal privacy plays no role in this *Ubuntu* context'.

[101] Although most of these countries have, within their constitutions the right to privacy which could also provide shadow protection to personal data, it would have been difficult for courts to determine the extent of rights and duties and infringement thereof and in any case this framework could not survive the rigorous standards for countries to exist in the globalized world.

[102] Bygrave (n 100); Bygrave (n 73).

[103] Bygrave (n 14), pp. 76 and 82; Greenleaf (n 51).

[104] Bygrave (n 60), p.7.

[105] Frowein, J.A. and Peukert W, Europaische Menscheurecht Konvention: EMPK-Kommentar, Kehl an Rhein: NP Engel, 1996, p. 338.

authorities, proportional to, and in safeguarding other societal interests and values in data processing.

Regardless of the motivations behind data protection legal reforms in Africa, the present thesis does not insinuate similarity in concept or value of privacy between and within African States. After all studies like one conducted by Korff[106] suggests the existence of considerable uncertainty about exactly which interests and values are promoted by data protection laws; despite extensive researches, publication and in-depth analysis made on the subject.[107] As a result, many data privacy laws fails to specify the interests and values they protect,[108] some specify the objectives in general terms such as, protection of personality or fundamental rights[109] or as narrow as protection of personal integrity.

It is surprising to see privacy reforms in Africa neglects conceptualization of privacy as debates are more focused on whether privacy is a concept worth protecting in Africa. Scholars such as Gutwirth,[110] Bygrave[111] and Bakibinga[112] believe due to African collectivist culture, privacy stand little chance. Gutwirth goes further illustrating how even the privacy rights within African Constitution have been watered down by the collectivism culture, rendering the right irrelevant and ineffective. His arguments are based on the fact that privacy rights in African Constitutions were adopted from colonial masters based on the Western concept of privacy. He considers the Western concept of privacy as unfitting to African systems, unless proclaimed by African States and the legal systems.[113] Bakibinga speaking in Ugandan context suggested, 'in the myriad of privacy definition and conceptual myopia, there is a need for defining privacy in a way accepted by the society, given the emphasis on communalism versus individualism'.[114]

One would expect the reforms to have been the awaited opportunity for institutions (such as the AU) to give statements on the state and value of privacy in Africa and what it means within the context. This oversight may lead to failure in analyzing the adequacy and exactness of the concept privacy or its ability to generate lucid and coherent regulatory measures in data protection. Moreover, interpreting and enforcement authorities such as Courts put more weight on the 'objects' and 'purpose' of the law, and relatively little attention to literal meaning of the legal text or legislator's intentions.[115]By not conceptualizing privacy, it is nearly impossible to know the objects or purposes it serves.

---

[106] Korff, D., 'Study on the Protection of the Rights and Interests of Legal Persons with Regards to the Processing of Personal Data relating to such Persons', Final Report to the EC Commission, October 1998; see also Napier, B., 'International Data Protection Standards and British Experience',Informatica e diritto, 1992, Vol. 2, No.1 , 1992, pp. 83-85.

[107] Mallmann, O., Zielfunktionen des Datenschutzes: Schutz der Privatsphare, korrekte information. Mit einer Studie zum Datenschutz im Bereich von Kreditinnformationssystemen, Frankfurt am Main: A Metzner, 1977, p. 10 cited in Bygrave (n 73), p. 172.

[108] Bygrave (n 60), p.8.

[109] See e.g., Directive 95/46/EC Article 1 (1) and Convention 108 Article 1.

[110] Gutwirth, S., Privacy and the Information Age, Lanham/Boulder/New York/Oxford/ Rowman & Littlefield Publ., 2002, p. 24.

[111] Bygrave (n 100).

[112] Bakibinga (n 95), pp. 2-3.

[113] Gutwirth (n 110), pp. 25-26.

[114] Bakibinga (n 95).

[115] Bygrave (n 60), p.36.

Despite the ongoing debates and perceived uncertainties in value of privacy in Africa; reforms in data protection continues to take place in different African States and at Regional and Sub-Regional levels. Perhaps the effects of globalization in technology transfer, internet usage patterns and their inherent threats is the reason for these reforms;[116] but more certain is the modest threat posed by the DPD[117] [118] and the influence of international patrons[119] and data protection experts.[120] One undeniable fact is that the EU intends and continues to set pace in data protection regulation by providing 'global data privacy standards'.[121] Graham Greenleaf suggests that the only way to have these standards implemented properly is for 'Council of Europe to settle and publicize appropriate policies on accession that are appropriate, transparent and do not reduce EU Data Privacy standards',[122] or strive to include those principles in what Bennet and Raab[123] refer to as 'strong consensus' fair information principles; or initiate reforms

[116] See arguments by Gutwirth (n 112); Mayer, J., 'Globalisation, Technology Transfer and Skill Accumulation in Low-Income Countries', United Nations Conference on Trade and Development, Geneva, August, 2000; and Wiley, J., 'The Globalisation of Technology to Developing Countries', Global Studies Student Papers, Paper No.3, http://digitalcommons.providence.edu/glbstudy_students/3 accessed 16/07/2014.

[117] See Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), p.78, where Mauritian Prime Minister urging members of the National Assembly to adopt data protection law in EU style to avoid being cut off from data flow; see also South African Law Reform Commission, Issue Paper 24, Project 124, Privacy and Data Protection, http://www.justice.gov.za/salrc/ipapers/ip24_prj124_2003.pdf ; Discussion Paper 109, Project 124, Privacy and Data Protection, http://www.justice.gov.za/salrc/dpapers/dp109.pdf narrates the influence of art 25 to the adoption of South African data privacy law; also this is narrated by the unsuccessful accreditation application made by Burkina Faso, Mauritius, Tunisia and Morocco for 'adequacy protection' under article 25 of the EU Directive, see these reports in CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Burkina Faso, 2010; CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Mauritius, 2010; CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Tunisia, 2010; CRID, Analyse du Niveau d'Adequation du Systeme de Protection des Donees dans le Royaume du Maroc, 2010.

[118] See commentators such as Bygrave (n 73).

[119] African countries in data protection reforms have been receiving legal technical and financial assistance from International organization mainly the International Telecommunications Union (ITU), The European Commission through their project in Support for Harmonization of the ICT Policies in Sub-Sahara Africa (HIPSSA) which was launched in 2008; the United Nations Conference on Trade and Development (UNCTD) through its 2006 cyber law reform project in East Africa and the European Union. Also, Francophone countries are receiving legal technical support from France while on the other hand the United Kingdom, through its Article 19 (acting as an international non-governmental organisation) have been critically assessing data protection laws in Africa in line with the EU Directive standards. So far the Article 19 made such comments in relation to Kenya and Nigerian data protection draft Bills, the comments are accessible under Article 19., 'Kenya: Draft Data Protection Bill critically limited', http://www.article19.org/resources.php/resource/2825/en/kenya; Article 19., 'Nigeria: Personal Information and Data Protection Bill', http://www.article19.org/resources.php/resource/3683/en/nigeria; a fuller discussion is found in Makulilo (n 77).

[120] Experts such as Graham Greenleaf and international bodies involved in data protection reforms such as the European Commission illustrate the EU Directive as being a universal instrument in data protection and the need for its global application [Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories', Journal of Law, Information & Science; EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final respectively]; Other experts arguing along the same lines includes Lee Bygrave, Serge Gutwirth and Gus Hosein.

[121] EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final; Greenleaf, note 117, supra; also as article 25 of the EU Directive can be interpreted.

[122] Greenleaf (n 51), p.69.

[123] Bennett, C and Raab. C., The Governance of Privacy: Policy Instruments in Global Perspective, 2006, MIT Press, pp. 12-13; The principles include accountability, purpose identification, collection with knowledge and consent limited collection to where necessary for purpose, use limited to identified purpose or with consent,

with principles established within the two earliest international instruments on data privacy as a guide to what is minimal requirement of a data privacy law[124] and ensure their existence beyond 'the paper'.[125] Perhaps this could be of assistance, but until that happens, what should third countries to the EU do? Specifically, how should Africa approach reforms in privacy and data protection?

With the EU broad role in global governance,[126] the current reforms at EU level affects data protection legal frameworks in Africa; perhaps even posing a greater challenge to the ongoing reforms agenda and the existing data protection systems. As long as data protection is a global phenomenon with EU determined to create universal data protection standards and equivalence in legal frameworks; defining values and declare them to be of global necessity, Africa is left with no choice but to follow the cue.

The above literature draws a picture of two pulling sides, on one side is the EU with intentions to strengthen and expand its influence and data protection standards as universal principles, and forging to ensure that EU legal framework for data protection serves as 'universal law'[127] but without provision of a roadmap to third countries who are nonetheless subjected and judged against such standards; and on the other hand are third countries struggle to fit within the universal standards based on the little guidance provided and limited knowledge of the basic concepts underlying the overall framework within which privacy and data protection operate. Moreover, given the complex relationship between privacy and social norms, a thorough consideration not only on the legal text but also the recipients' unique legal culture, political and socio-economic contexts needs to be looked upon. This should be in light of the global trend and economy to determine how such principles fit both local and universal standards in data protection,[128] after all the 'adequacy' determination is assumed to deliberate on all these elements.

The challenge with which the present thesis undertakes is to study and explain privacy values and perceptions in Africa; the legal reforms in privacy and data protection in Africa and how the reforms can be projected within the local as well as in the global context. The ultimate objective is to draw up suggestions on way forward in reforming privacy and data protection laws in compliance with wide accepted standards. In light of the fact that the EU is determined to strengthen data protection principles and their enforcement outside EU in line with the Lisbon

---

disclosure likewise, retention only as long as necessary, data kept accurate, complete and up-to-date, security safeguard, openness on policies and practice, individual access and individual correction.

[124] Greenleaf summarizes them as 1. Data quality - relevant, accurate, & up-to-date); 2. Collection-(limited, lawful & fair; with consent or knowledge; 3. Purpose specification at time of collection; 4. Notice of purpose and rights at time of collection(implied); 5. Uses & disclosures limited to purposes specified or compatible; 6. Security through reasonable safeguards; 7. Openness re personal data practices; 8. Access- individual right of access; 9. Correction - individual right of correction; 10. Accountable- data controller with task of compliance. However, the inclusion of all or limited criteria within these principles will depend on specific country circumstances. See Greenleaf (n 51), p. 8.

[125] Greenleaf (n 51), p.12.

[126] Mayer, H., 'Europe's Post Colonial Role and Identity', in Adebayo, A. and Whiteman, K(eds), The EU and Africa: From Eurafrique to Afro-Europa, C. Hurts & Co Ltd, United Kingdom, 2012, Chapter 22.

[127] EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final, 2.4.2.

[128] Makulilo, A.B., 'Privacy and Data Protection in Africa: A State of the Art', International Data Privacy Law, 2012, Vol.2, No.3, pp. 163-178 at pp. 171-172.

Treaty[129] with the aim to create 'equivalent' levels in data protection through approximation of national laws.[130]

1.2.2 Research questions

The literature confirms that African States' emerging data privacy legal reforms are transposing EU Directive 95/46/EC in the absence of any grounding definition of the concept privacy or motivation to preserve it in relation to processing of personal data but rather to encourage economic outsourcing as the primary motivation. In this context, the present study undertakes to address the following questions crucial in determining the appropriateness and viability of these reforms within and beyond Africa.

i. Are the forces that propel African data protection/privacy reforms justifies transplanting of the Western frameworks for data protection.

ii. Are the objectives of the Western data protection frameworks adaptable within African context and in view of African cultural values?

iii. How can the reforms strike a balance between globalization in data protection regulations and the localization of data protection while abreast with user patterns and challenges posed by technological development?

iv. What is the future of data protection/privacy in Africa?

1.2.3 Research Methods

1.2.3.1 Empirical Legal Research

Generally data collection involved a range of methods: unstructured interviews, questionnaires distributed by way of online survey and documentary reviews. Interviews and questionnaires were conducted to gain insights from the stakeholders' perceptions, values, experiences, beliefs and attitudes towards privacy and data protection in Africa. These methods provided an insight on the challenges and prospects in reforming and in implementing the laws within their contexts. Last but not least was the interview with data protection project manager (for AFAPDP) and consultants involved in the drafting of the Tanzania Draft Personal Data Protection Bill. These were approached to get a real experience with reform activities. Documentary review assisted with in depth understanding of the processes involved in reforms, considerations and motivations for these reforms. They were also used to analyze and symmetrize on ground understanding and expectations of such reforms with the actual reforms.

[129] Greenleaf (n 51), p.79.
[130] Directive 95/46/ EC, Recital 9.

To measure the reliability and confirm validity of the data the researcher was mindful of the need to have internal validity, diverse reality and reliability. To ensure internal validity multiple stakeholders and methods of data collection were employed. Triangulation was employed for internal validity of data. In doing so, documentary review was conducted before the interviews to gain insight over the subject matter and specific local perceptions. The review was once again after the interviews and collection of questionnaires to verify data. The interview was also conducted to different categories. As suggested by Golafshani[131] that, 'Triangulation is typically a strategy (test) for improving the validity and reliability of research or evaluation of findings.' This method, according to Patton strengthens the study by combining different methods allowing the researcher to get multiple insights about a particular reality.[132] Constructivism which according to Golafshani[133]allowed the researcher to view knowledge as a socially constructed and its ability to change based on circumstances. Constructivism was used to validate diverse realities.

Nature of this thesis necessitated the researcher to employ constructivism so as to look deeper into the subject matter instead of observing surface features of the emerging and existing legal systems. This approach has been advised by Johnson[134] whenever dealing with diverse aspects of legal systems for purposes of reforms. The research dwelled into legal cultures, privacy foundations, historical developments and social-technological changes with impact on the data protection legal frameworks. An understanding of these aspects was necessary to explain the reform trends while keep in mind varied social realities and influences of change. Finally, the data collected both in form and context ensured reliability and the consistence use of the documents.

Data analysis started with the coding of interviews and questionnaires to bring more evocative meanings and to identify patterns, consistencies and variations. Based on variety of data and methods used and time available, the research used 'lamper' coding.[135] Data coding was done in two cycles. Simultaneous data coding system was employed to detect similar and varying values. The first data coding cycle involved raw data from all participants of the interview and questionnaires. This was followed by the creation of notes with comments and reflections on the data codes. The third step was the segregation, grouping, regrouping and re-linking of data to construe meanings, explanations to the data and building theories. This enabled the testing of existing theories about privacy in Africa with the generated theories from the interpretation of the data collected. This process not only involved deductive approach in seeking answers to the research questions and explaining the working theoretical frameworks, it also involved inductive approach in search of theories that reputes the research questions and working theoretical frameworks. The coding process was performed manually. Analogy was also involved. The process of analogy was used in inspecting individual attributes of the legal texts from case studies (Senegal and Tanzania) and the blue print (the EU framework for data protection) to determine

---

131 Golafshani, N., 'Understanding Reliability and Validity in Qualitative Research', The Qualitative Report Volume, 2003, Vol. 8, No. 4, pp. 597-607 at p. 603.

132 Patton, M. Q., Qualitative Evaluation and Research Methods, (3rd ed.), Sage Publications, Thousand Oaks, CA, 2002.

133 Golafshani (n 137).

134 Johnson, S. D., 'Will our research hold up under scrutiny?', Journal of Industrial Teacher Education, 1995, Vol. 32 No.3, pp. 3-6.

135 Lumping is an expedient coding method allowing the researcher to get to the essence of categorizing a phenomenon; Saldana, J., The Coding Manual for Qualitative Researchers, SAGE Publications Ltd, 2009. p. 20.

how fitting these frameworks are. This was also helpful in developing a thesis on the future of data protection in Africa.

1.2.3.2 Comparative Law Approach

Since the research deals with data protection reforms in Africa in view of global trends, a comparative study of data protection law was taken. Comparative study, as suggested by David and Brierley[136] is an essential approach when dealing with harmonization of international law, through a glimpse of other legal systems. In doing so, an observer gets ideas for future development, warnings of possible difficulties and opportunities. It also allows a look at one's own legal national system and look at it more critically without moving it from first place on the agenda.[137] This approach was crucial in understanding essential elements in reforming data protection in Africa in light of international trends but in consideration of Africa's unique systems and institutions. Legal comparative, as asserted by William Baker[138] allows for an understanding of the ideological purposes behind the laws and legislations dealt with. It is a practical approach in deciding legal transplantation and legal development or reform.

The comparative analysis involved on one hand two countries, Senegal and Tanzania against each other, and on the other EU DPD and three countries namely France, Germany and United Kingdom. Within EU, the analysis was limited to some aspects on the explication of the aims and principles within the EU Directive. Accuracy and departures in implementation of the EU Directive is also discussed in view of providing an understanding of what Kuner refers to as minimum and maximum standards (a bandwidth) for data protection enshrined in the DPD by EU Member States[139] and most likely third countries, in reform process. In this respect, France, Germany and United Kingdom were selected as case studies. The decision to use variety of EU Member States law and practices was based on the understanding that, despite all Member States implementing the same Directive, their laws and practice differs considerably in structure, content and approach[140] consequently interpretation against the DPD ranges from compliance, inconsistence or violation.[141]

Senegal represents civil law countries while Tanzania represents common law countries, the two dominant legal systems in Africa.[142] [143] Selection to study Senegal and Tanzania is first based on

---

136 David, R and Brierley, J.E.C., Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law, (3rd ed), Stevens & Sons, London, 1985, p. 10.
137 Wilson, G., 'Comparative Legal Scholarship' in W.H Chui, and M. McConville, (eds), Research Methods for Law, Edinburg University Press, 2010, pp. 87-103 at p. 87.
138 Barker, W. B., 'Expanding the Study of Comparative Tax Law to Promote Democratic Policy: The Example of the Move to Capital Gains Taxation in Post-Apartheid South Africa', Pennsylvania State Law Review, 2005, Vol. 109, pp.101-125.
139 Kuner, C., European Data Protection Law: Corporate Compliance and Regulation (2nd Edition), Oxford University Press, UK, 2007, pp. 34-35.
140 See Kuner (n 139), p. 33; Greenleaf (n 51), p.73.
141 See Analysis and Impact Study on the Implementation of Directive 95/46/EC in Member States, 2003.
142 Time, V.M,'Legal Pluralism and Harmonization of Law: An Examination of the Process of Reception and Adoption of Both Civil Law and Common Law in Cameroon and Their Coexistence with Indigenous Laws', International Journal of Comparative and Applied Criminal Justice, Spring 2000, Vol. 24, No. 1, pp. 19-29, at p. 19.

their difference in legal culture. Secondly, Senegal, within the francophone countries, had a very active data protection Commissioner, Dr. Mouhamadou[144] who was involved in the local and international activities towards promotion of privacy and data protection. Senegal has also strong civil society organizations such as JUNCTION[145] involved in public awareness and pushing the government towards enforcement of privacy rights and data protection. On the other hand, Tanzania is still working on its draft personal data protection bill.[146] Researcher's familiarity with country's legal system was one of the reasons for its selection, but also is the fact that, the researcher had already studied the personal data protection bill and published a report in the Privacy Laws & Business International Reports.[147] Hence the researcher's knowledge of the country's legal system especially on privacy and data protection issues influenced the choice as it would minimize field research costs that would be involved if another country was to be selected. A selection of two different legal systems was to be able to probe how (if so) their differences affected the adoption and reforms by transposing a regime with international origin.

1.3 Chapter Overview

The thesis is structured into six chapters. Chapter 1 is *introduction*; setting out the research agenda of this study. It includes a statement of the problem, research questions and research methodology. Chapter 2 is titled *Transposition and Practice of the EU Directive on Data Protection*. This chapter is devoted to the EU data privacy reforms and practices in selected States notably Germany, UK and France. It provides an introductory foundation on the discussion of the subsequent chapters. Chapter three is titled *Privacy in the African Culture and Customary Legal System*. The chapter illustrates how 'privacy' is viewed in Africa. The chapter provides for different terminologies used to refer to 'privacy' and scholarly discussion on the nature and value of privacy in Africa. Within this chapter, the African traditional legal system is also explained. Chapter four, '*Privacy Regulations and Institutions in Africa',* examines the legal structure and systems for the enforcement of human rights in Africa. Chapter five is titled, *Data Privacy Reforms in Senegal and Tanzania*. The chapter focuses on reform processes in the two jurisdictions in Africa by looking into the influences that lead to the reform processes, examine elements that affect(s/ed) (positively and negatively) the process and how local institutions shaped the nature

---

[143] The less dominant legal system was imposed by Portuguese and the Northern of African countries dominated by Shari'a law with peculiarities of Arab and Islamic cultures which need a more focused study. See suggestion in Makulilo (n 26), p. 473.

[144] See participarion in several local and international workshops some explaining the status of privacy and data protection in Senegal and others are offering understanding on the need and nature of privacy and data protection law. He is also a member of the Francophone Group of reflection on the establishment of an international instrument on protection of personal data and privacy within the AFAPDP, and a member of the editorial team of the ECOWAS Supplementary Acts on personal data, electronic transactions and the Directive on Cybercrime. More can be seen in the Commission's Website through; http://www.cdp.sn/ accessed on 22/05/2014.

[145] A Senegalese Association aims at promoting and protecting human rights. JUNCTION in collaboration with Privacy International has been a driving force towards privacy and data protection in Senegal. For more activities in this regards visit, www.jonctions.org.

[146] See the press release of 31 March 2014 at the Ministry of Communications, Science and Technology Website http://www.mst.go.tz/index.php/78-news/94-taarifa-kuhusu-undaaji-wa-sheria-salama-ya-matumizi-ya-mtandao accessed 22/05/2014.

[147] Boshe, P., 'Evaluation of the Data Protection Bill in Tanzania', Privacy Laws & Business International Report, 2014, No. 127, pp. 25-26.

and type of legislation in place and or reform process. Chapter 6, *Conclusions and Future of African Data Protection Regimes* offers conclusions retorting research questions and filtering major findings and reform patterns. The chapter also offers a thesis on the future of the African data protection regimes.

2. Transposition and Practice of the EU Data Protection Directive

2.1 Introduction

This chapter provides a holistic survey and discussion on the transposition of the EU Data Protection Directive in selected EU countries. The essence of the chapter is the fact that the European Union plays a pioneering role in the world in the field of data protection. Consequently, understanding adoptability and practicability of the DPD within the mandated context is necessary before making an analysis of the same in different contexts.

The discussion takes the form of parallel comparison between specific provisions and practices in different jurisdictions in Europe against the provisions of the DPD. The object is to see how the provisions of the DPD have been transposed and interpreted in different contexts and at different levels, and how different interpretations and practices affects(ed) the efficacy of the transposed DPD provisions and its objectives.

This discussion focuses on three countries, Germany, France and United Kingdom (UK). Germany is selected because the writing of this thesis was done in Germany; hence convenience in accessing relevant materials and information on the Country's data protection framework. Moreover, Germany is considered as a country which best demonstrates a variety of approaches in transposition of DPD.[148] [149] France is studied because the subject of the thesis involves Senegal as a case study. Senegal was a France colony, and today, France still has a substantial influence on Senegal legal and political affairs. In fact, it is France, through the AFAPDP who initiated and assisted Senegal in the adoption of the new data protection legal framework in the EU style. Moreover, Senegal is among Francophone countries which have recently adopted the Francophone Binding Corporate Rules under the guidance and support of France. The UK is studied because is an ex-colonial master to Tanzania; Tanzania being the second case study of this thesis. The UK is assessed to determine its influence on common law countries in Africa such as Tanzania. Accordingly, UK law still applies to its former colonies. For instance, Tanzania through the Judicature and Application of Laws Act Cap 358 R.E 2002 applies the common law of England, the doctrine of equity and statutes of general application in force in England in 1922.[150] Similarly, case laws decided by English Courts have a high persuasive authority to the Courts in Tanzania. The assumption is also made on the fact that, the UK being a common law country, she is the closest 'neighbour' likely to inspire the approach to which Tanzania (or any common law country in Africa) may adopt the reforms. Logically, data protection regimes being 'foreign', a cue from the UK may be taken to reduce a likelihood of failure in the adequacy determination.

This chapter illustrates best (or worst) transposition or practices concerning the objectives of the DPD. The survey and discussion take no particular ideological position, rather an objective approach is taken, in which case criticisms in law or practice in any data protection regime is

[148] Kuner(n 139), p. 13.
[149] Germany being a Federal State has Federal Data Protection Act that applies to processing practice of the Federal government and to private actors with a Federal Data Protection Commission to oversee its implementation. Furthermore, each state (*Länder*) has its Data Protection Act with separate DPAs. Germany has also implemented specialized regulatory mechanisms such as the adoption of *Telemediengesetz* of 2007.
[150] Judicature and Application of Laws Act, s.9.

made. This stance is crucial in providing proper and evidence-based recommendations to countries under privacy law reform on the best shoals to navigate in transposing/implementing the DPD or any other legal regimes or codes on data protection.

It should also be clear that the discussion in this chapter is mainly an overview. The aim is to provide a basic understanding of the main instruments on data protection and practice. It is in no way an attempt to provide a comprehensive understanding of the overall EU system on data protection. The objective is to provide key aspects for consideration in transposing the DPD into local legislation as well as the content, context, practices and enforcement frameworks. As Kuner suggests, the first step to implementing the DPD is to understand the instrument of law and the legal traditions which it springs. This is a foundation to understanding detailed issues of local data protection laws.[151] However, in light of the breadth of the topic, this chapter deals with specific aspects of the DPD, mainly some basic concepts and core rules that define the overall mechanism for privacy protection on personal data. Also, the thesis does not deal with sector specific data protection instruments to avoid cosmetic treatment on those specific instruments.

2.2 Synopsis and Objectives of the EU Data Protection Directive

As explained in chapter one, the DPD was adopted on 24 October 1995 giving the Members States three years for its transposition into domestic law. The DPD is yet the longest and most comprehensive instrument on data protection[152] with 72 recitals and 34 articles within eight chapters; but lacks explanatory memorandum. Therefore the *travaux préparatoires* to the DPD serves a significant role as interpretation reference.[153] EU Directive covers both automated and manual[154] data processing, either structured or in filing state, in public and private sectors for identified or identifiable natural person.[155] There is, however, an exception to this scope. The DPD does not apply when data processing in public sector concerns matters falling outside the European Community Law[156] or when in private sector the processing involves personal data by natural person in the course of purely personal and household activities.[157]

The EU Directive sets two main pillars in the protection of personal privacy with regards to the processing of personal data. The first pillar provides for substantive law and the second pillar provides for a procedural law (enforcement mechanism). The substantive law consists of its scope, definition and more important to the protection, the basic data protection principles which are more or less the same those within the OECD Guidelines and Convention 108. Also, it establishes a framework for trans-border data transfer under Chapter IV (Articles 25 and 26)

---

[151] Kuner(n 139) pp. ix-2.
[152] Bygrave (n 14), p. 53.
[153] Makulilo (n 26), p. 159.
[154] In case of manual processing data must be (or intended to) form part of structured filing system, see Articles 2 (c), 3 (1) and Recital 15.
[155] Directive 95/46/EC, Articles 2 (c), 3 (2) read together with Recitals 12 and 27.
[156] These are activities falling under 'second pillar' and 'third pillar' involving public security, defence, state security and activities of a state in areas of criminal law.
[157] Directive, Article 3 (2).

prohibiting the Member States from transferring data to third countries unless such third countries ensure 'adequate level of protection'.

The DPD came with two main objectives stated in the Recitals. First is the promotion of internal market of the EU through harmonization and strengthens the existing regulations to allow free flow of personal data between member states.[158] Second is to safeguard data subject's privacy right with regards to the processing of data.[159] According to Recital 23,[160] this was anticipated by an adoption of legislation in conformity with the DPD protection standards.[161]

The DPD is however not solely tied to the concept privacy as Roos suggests. Its main focus is on personal data. This makes its protection to data processing wider beyond those acts considered privacy-sensitive in their own right.[162] This is evidenced by the fact that the DPD contains rules encouraging freedom of expression,[163] freedom of information,[164] preventing discrimination and improving efficiency. Through these provisions, the DPD provides for definitions of concepts, rights and obligations and clarifies the scope of the data protection rules for processing of personal data, (including a special category of processing), an establishment of supervisory authority and rules on trans-border data flow including transnational oversight arrangements.[165] Basically, the DPD provides a general framework for Member States to

---

[158] See Directive 95/46/EC; Article 1 (2) and Recitals 3, 5, 7, 9 and 11.

[159] See Directive 95/46/EC, Article 1 (1) and Recitals 2, 3, and 10; see also *Rechnungshof v Osterreichischer Rundfunk and others* [2003] ECR I-4989 paras 39-45.

[160] Directive 95/46/EC, it states, 'Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes'.

[161] Directive 95/46/ EC, Recital 9 states, 'Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; Whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community'.

[162] Roos, A., 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', LL.D Thesis, UNISA, 2003, p. 17.

[163] Directive 95/46/EC, Article 9; Case C-101/01 Bodil Lindqvist, [2003] ECR I-12971, paras 88-90, where the Court held that the provisions of the Directive do not restrict the exercise of the general principles of freedom of expression or other freedoms and rights which are applicable within European Union and enshrined under article 10 of the ECHR. Nationals and Courts implementing the Directive are responsible in determining the balance between the rights and interests in question; See also explanation offered by Article 29 Working Party on their 'Recommendation 1/97 on Data protection law and the Media', WP 1, 25 February 1997.

[164] Although there is no specific provision within the directive, Article 29 Working Party opined that the directive should be read as complementing the right to information, and although there is no hierarchy between the right to data protection and right to freedom of information, the two a complements each other. And accordingly the European Commission Regulation provides whenever collision occur (as it can be foreseen in some circumstances) balance of interest in two rights is to be found on case to case basis to resolve tension between the two rights. See Article 29 Working Party, 'Opinion 5/2001 on the European Ombudsman Special Report to the European Parliament following the draft recommendation on the European Commission in Complaint 713/98/IJH' , (WP 44, May 2001) and EC, Regulation 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding Public Access to European Parliament, Council and Commission documents [2001] OJ L 145/43 respectively.

[165] Chapter I (Articles 1-4) contains general provisions, definition of concepts, the object and scope of the Directive; Chapter II (Articles 5-21) contains rules on processing personal data lawfully. It has principles for criteria for legitimate processing (including special category of data processing), data quality, data subject participation,

implement into their national laws,[166] what Bygrave refer to as 'comprehensive vision of what protection of data privacy should involve with a relatively rigorous set of rules'.[167]

2.3 Background and Basis for Privacy Protection in France, Germany and UK

In Germany and France, data protection laws came as an inevitable means to regulate government misuse of personal data. In Germany, the first data protection law (also the first comprehensive data protection law in the world) was enacted in 1970 in the state of Hesse. The primary goal of this law was to safeguard the large State-owned databases and provide for transparency in the processing of personal data. The Federal Data Protection Law (*Bundesdatenschutzgesetz*) was enacted on 21st January 1977. However, a huge proclamation to the protection of personal data came about in 1983 as a consequence of the adoption of a Census Law (*Volkszahlungsurteil*).Upon this adoption; the Constitutional Court (*Bundesverfassungsgericht*) declared a personal right to information self-determination (*Informationelle selbstimmung*) when enforcing Article 2 para 1 of the Constitution (*Das Grundgesetz*).[168] This was a result of a law suit instituted by 34,000 citizens to challenge the government collection of statistical census. Citizens feared this may lead to surveillance by government and that the statistical census was an unjust invasion of personal privacy. As a result, the Court ruled that the Census Act was partly unconstitutional and annulled it. The Court in translating the constitutional right to privacy created a personal right to information self-determination. Today, the right to information self-determination is the central principle underlying data protection in Germany.[169] [170]

---

confidentiality, security and notification to supervisory authority; Chapter III (Articles 22-24) has provisions on judicial remedy, liability and sanctions; Chapter IV (Articles 25-26) contain rules on Transborder data flow; Chapter V (Article 27) provides for codes of conduct; Chapter VI (Articles 28-29) contain rules of establishing supervisory authority by member states and a requirement for setting up a 'working party' to look after individual rights with regards to processing of their personal data; Chapter VII (Article 31) is on implementation measures by the Community; FINAL PROVISIONS (Articles 32-34) on the timeframe and how member states are to comply with the Directive.

[166] Raab, C.D and Bennett, C.J., 'Protecting Privacy across Borders: European Policies and Prospects', Public Administration, 1994, Vol.72, pp.95-112.

[167] Bygrave (n 14), p.59.

[168] However, the Federal Supreme Court had recognized the right to personality since 1954 in the *Leserbrief [1954] N.J.W. 1404, B.G.H.* when enforcing article 1 of the Constitution (GG), and according to *Frischzellen-Kosmetik B.G.H. 1984, 681,* 426 this right continues even when the person dies; a dead person has a right to protection of his reputation as well. See also *on Hannover v Germany (2005) 40 E.H.R.R. 1* which opined that the right to privacy provided in Germany places it in a middle level between France and UK privacy protection.

[169] Zurawski, N., 'Increasing Resilience in Surveillance Societies: Germany Country Reports' http://irissproject.eu/wp-content/uploads/2014/06/Germany-Composite-Reports-Final1.pdf accessed 22/07/2016, p.2; Korff, D (ed)., Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Case study Germany, 2010; See alsoWolfgang, K., 'Germany' in Rule, J.B and Greenleaf, G (eds)., Global Privacy Protection: The first Generation, Edward Elgar, Cheltenham, Uk and Northampton, MA, US, 2008, pp.80-106.

[170] In the Court order of 24th January 2012 in *BVerfG, 1 BvR 1299/05* The Federal Constitution Court emphasizes the principle of information self determination to be the ground rule in data protection in Germany. In the case, the Court rules sections 111-113 of the Telecommunications Act (Telekommunikationgesetz) which allow for the collection and storing of data and their usage for automated processing as violating the right to information self-determination declaring the provisions as null and void. The English version of the case is available at http://www.bverfg.de/e/rs20120124_1bvr129905en.html.

The right to information self-determination carry 'the idea that citizens hold the right to be informed about the uses of their data when collected, used or forwarded by public or private bodies and enterprises; and the right to determine (within the boundaries of the applicable law) what data they give away……..Although the term "informational self-determination" cannot be found in the GG (basic law) and only appears in the 1983 ruling, it has become the guiding principle of all data protection law that followed in Germany.'[171] Today, the right to privacy is explicit in the Federal Constitution (GG) under Article 10 guaranteeing the secrecy of postal and (tele) communication against tapping and interception; and article 13 which provides for physical privacy against inviolability of dwelling house.[172]

The 1977 Federal Data Protection Law was amended on the 23rd of May 2003 when Germany transposed the DPD. Previously, the law was amended in 1990, 1994, 1997 and 2001. However major amendments occurred later in 2009.[173] The 2009 amendments strengthened the protection to personal data against market usage of data lists and employment data. The law also enhanced data protection authority powers to enforce the law and requires a controller to provide a report for data breaches, which further enhances the security and integrity of personal data.

Germany being a Federal government with 16 States (*Länder*) has a Federal Data Protection Law and specific States Data Protection Laws with Data Protection Commissioners in each State. The Federal Data Protection Law remains to regulate Public Federal authorities, State administrators (when a State law lacks specific provision) and private bodies (in the latter case when data processing systems and or automated filing system are for commercial or professional use). The State Data Protection Laws regulate Public sector within specific States. The States' Data Protection Commissioners also oversees private sectors' compliance with the Federal Data Protection Law within their States. Clarity must be made here, that all the 17 data protection laws in Germany do not differ in substance, they all base on the same principles. There could be minor differences in interpretation of the principles, but the principles are consistent.[174]

This right to information self-determination is the anchor to data protection laws not only in Germany but of the world today. From this principle, standards have been set in usage and dissemination of personal data while ensuring data security and providing data subjects with the right to participate in protection of their data held in private and public institutions. German Courts continue to widen the scope of Article 1 (1) and 2 (1) of the Federal Constitution to meet current development in technology. A case of *1 BvR 370/07*[175] is an example where the Federal Constitution Court ruled article 2 (1) and 1 (1) of the Federal Constitution includes guarantees to

---

[171] Zurawski (n 169), p. 3.

[172] According to article 13 (2) GG, home search can only occur upon Judge's authorization and (articles 13 3-7) when there is justifiable suspicion of serious criminal activities/ infringement of a law. Hence search will be granted in preservation of public safety and protection of people in the dwelling house.

[173] Bundesdatenschutzgesetz [Federal Data Protection Act], December 20, 1990, BGBl. I at 2954, as amended.

[174] Zurawski (n 169), p. 5.

[175] The English version of the case note *BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267)*, of 27 February 2008, is available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html see also press release following the judgment, Press Release No. 22/2008 of 27 February 2008, *Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void* available at http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html;jsessionid=EC00A2D06207165C62A3D5C96F74110D.2_cid370 both accessed on 01/03/2016.

confidentiality and integrity in the information technology systems. For Germany, the Data Protection laws, apart from transposing the DPD, they are considered as an extension of the Constitutional right to privacy. According to Zurawski, they 'support claims by citizens and gives them a strong tool to challenge infringements and modify acts and new laws that may infringe and impact on privacy rights and informational self-determination.'[176]

In France, the data protection legislative reforms were triggered by an article in the *'Le Monde'* titled 'SAFARI haunts French'.[177] SAFARI was a government project aimed at interconnecting all files with citizens' data to easily identify them for administration purposes. This article revealed government plan which led to a commotion by the public over their privacy and security of their personal data. Consequently, the French government was forced to establish a Commission to oversee the project and make sure the use of IT does not unreasonably infringe the personal privacy or endanger the security of personal data. Four years later, the French government enacted the Data Protection and Personal Liberty Law (*Loi Informatique et Libertés*).[178] This law established the CNIL (*Commission Nationale de l'Informatique et des Libertés*) as an administrative body to oversee the protection of personal data.

In 2004, France transposed the DPD. The transposition necessitated France to amend the 1978 law to align with the DPD; although most of its provisions were already in line with the DPD.[179] Nonetheless, on the 20th of October 2004 the law was amended, specifically on regulation and the use of cookies.[180] The amendment also gave the CNIL more obligations in relation to data protection this includes the mandate to promote practices by institutions and bodies of the EU and cooperate with other Data Protection Authorities in promoting data protection that is consistent across Europe in line with the DPD.[181]

Unlike Germany, France had no explicit Constitutional right to privacy, although she recognized a tort to privacy since 1858, which received codification in 1970 under the Civil Code. Furthermore, France adopted the ECHR since 1974.[182] Consequently, in 1995, the Constitutional Court implicitly ruled the Article 2 of the 1789 Declaration of the Rights of Man and the Citizen

[176] Zurawski (n 169), p. 6.
[177] Published in March 1974.
[178] Law No. 78-17 of January 1978.
[179] Nicole Atwill, 2012; available at https://www.loc.gov/law/help/online-privacy-law/france.php accessed on 02/03/2016.
[180] The law was amended by Act No. 2004-801 of 7 August 2004 and an implementing decree No. 2005-1309. It was later amended by Decree 2007-451 of March 25, 2007 [modifiant le décret 2005-1309 du 20 octobre 2005 pris pour l'application de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 du 6 août 2004 [Decree 2007-451 amending decree 2005-1309 of October 20, 2005, implementing law 78-17 on Information Technologies, Data Files and Civil Liberties].
[181] Other amendment to the Franch DPA includes the 2009 amendment through Law 2009-526 on the simplification and clarification of the law and procedures *(Loi 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procedures*); 2010 amendment through Organic Law 2010-704 of June 28, 2010, relating to the Economic, Social and Environmental Council (*Loi organique 2010-704 du 28 juin 2010 relative au Conseil économique, social et environnemental*) and in 2011 amendment through Law 2011-334 of March 29, 2011 relating to the Defender of Rights (*Loi 2011-334 du 29 mars 2011 relative au Défenseur des droits*), and through Ordinance 2011-1012 of August 24, 2011, on Electronic Communications *(Ordonnance 2011-1012 du 24 août 2011 relative aux communications électroniques*).
[182] Official Journal January 3, 1974, published pursuant to Decree No. 74-360, Official Journal May 4, 1974.

(*Déclaration des droits de l'homme et du citoyen de 1789*) to include respect for privacy.[183] This makes Germany and France the earliest countries to have comprehensive data protection laws with supervisory authorities in Europe. In fact, it is argued that the DPD was inspired by these two regimes.[184]

The United Kingdom, being a Common Law country and a Monarchy does not have a written Constitution. However, the right to privacy had been enforced through the law of confidence preventing an unauthorized disclosure of personal information[185] as a breach of confidence.[186] The UK has never recognized or enforced privacy as the common law tort of privacy[187] rather as the right against invasion of private lives and protecting private sphere. According to Taker, the development of the right to 'information (data) privacy in the UK, involves Court interpretation of the tort of breach of confidence following the jurisprudence of articles 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms on the right to privacy.[188] This evolution changed the Courts' approach from '*the information is confidential*' to 'the *information private'*.[189] The change of approach is mainly attributed to the adoption of the Human Rights Act in 2000. In 1998, the UK transposed the DPD which came into force in 2000.

2.4 Analysis on Transposition of the EU Directive in France, Germany and UK

Transposing the DPD requires a proper understanding of its provisions which Bygrave[190] admits is no easy task due to the nebulous manner in which many of its provisions are formulated and the paucity of authoritative guides on their meaning. It can even be more confusing for those unfamiliar with legal traditions from which it springs.[191] The DPD was formulated in general terms, yet with great details on what domestic data protection laws should provide as a baseline protection and which cannot be derogated from. To ensure equivalence in protection, EU Member States were to transpose it in the form of a legislation adoption. However, with Recital 9 giving member states room for *manoeuvre*, Member States had leeway to define the context of their laws and establish enforcement structure to fit their local legal culture; of course, as long as the framework erected 'meets the requirement of clarity and certainty in legal situations.

---

183 Décision 94–352DC du Conseil Constitutionnel du 18 Janvier 1995, available at http://www.conseil-constitutionnel.fr/decision/1994/94352dc.htm; accessed on 29.02.2016: This decision was confirmed in 1999 in Décision 99–416DC du Conseil Constitutionnel du 23 juillet 1999, available at http://www.conseil-constitutionnel.fr/decision/1999/99416/index.htm both accessed on 29/02/2016.

184 Nicole Atwill, 2012; available at https://www.loc.gov/law/help/online-privacy-law/france.php accessed on 02/03/2016.

185 *Prince Albert v. Strange, 1 Mac & G 25 (1849).*

186 According to *Hellewell v Chief Constable of Derbyshire [1995] 1WLR 804*, the main principles on the law of breach of confidence is based on good faith to protect idea which can be valuable and mundane. It does not matter whether or not confidential relationship exists.

187 *Wainwright and another v. Home Office*, (2003) UKHL 53, (2003) 4 All ER 969.

188 Keith, T.I., 'An examination of the commercial and non-commercial appropriation of persona within the United Kingdom, with a comparative analysis with common and civil law countries', LL.M thesis, Durham University, 2011, p. 11.

189 Ibid, p.13.

190 Bygrave (n 14), p.56.

191 Kuner (n 139), p. 2.

Consequently, as an effect of diversity in legal cultures and structures, perceptions and understanding of the right to privacy (or the concept privacy) countries interpreted the DPD's basic content and core rules differently. Regardless of similarities in rules transposed by each country, the interpretation process and local foundations of the right to privacy (where data protection emerged from) affected the nature and quality of protection offered. Some Member States imposes stronger measures while others impose comparatively weaker measures.

2.4.1 Definition of Basic Concepts

2.4.1.1 Natural and Juristic Persons

The concept 'person' has been given different meaning and scope in domestic laws by the Member States. While the DPD defines a person as natural person[192] with the Article 29 Working Party clarifying the scope of the provision to cover only living being,[193] there are countries that extend the meaning of a 'person' to cover juristic persons[194] and dead persons. Kuner explains the variation in the meaning of the concept 'person' beyond 'living being' by arguing that, Article 1 of the DPD read together with Article 2(a) and Recital 24[195] allows for such extension to suit specific circumstances, and so the definition can safely be construed to cover 'persons' beyond the natural person.[196] He agrees that the DPD intended a person to be a natural person but deliberates that it allows a Member States to extend the meaning to fit individual circumstances. France and the UK both adopted the definition as spelt in the Directive while Germany under Section 2 of the *Bundesdatenschutzgesetz* (BDSG) a person includes a natural and juristic person as well as private law associations.

2.4.1.2 Personal Data

Based on the definition of a person, the DPD considers 'personal data' to be information relating to natural, identified or identifiable person.[197] [198] Also, *ECtHR* in *Amann v. Switzerland*[199] clarified the scope of this provision. The Court specifies personal information to include such

[192] EU Directive, Article 1 (1).
[193] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p. 22.
[194] E.g., Denmark.
[195] Directive 95/46/EC; Recital 24, which states 'Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive'.
[196] Kuner (n 139), p. 77.
[197] EU Directive, Article 2 (a).
[198] Personal identifiers include personalized numbers such as social security numbers, biometric data such as fingerprints, digital photos or iris scans. The Directive 95/46/EC under Recitals 14,15,16, 17 and 26 states It does not matter in which form or format the data is. Data identifier can be written, spoken communication, images, closed-circuit television (CCTV) footage or sound, in electronic form, on paper or biometric sample. Consequently, any data, not personal per se but tied to a person, and which, with further research can reveal identity of a person is, for purposes of the directive, personal data. See further elaboration offered in *ECtHR, Von Hannover v. Germany, No. 59320/00, 24 June 2004; ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005; ECtHR, Peck v. the United Kingdom, No. 44647/98, 28 January 2003; Kopke v. Germany, No. 420/07, 5 October 2010; ECtHR, P.G and J.H v. the United Kingdom, No. 44787/98, 25 September 2001.*
[199] *ECtHR, Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000.

personal information originating from professional interaction not only on private interactions.[200] The idea behind the Court's clarification is to allow an individual to be able to pursue development and fulfils one's personality.[201] Consequently, any information relating to a natural person whether in a domestic or public sphere is construed as personal data and therefore falls within the protection regime established by the DPD.[202] The definition took a relative approach to what is persona data.

In this regard, the key to understanding, interpreting and implementing this provision is its requirement that any data that is 'personal, an identifier, or identifiable of natural person' is personal data.[203] As long as a link can be established between specific data and a natural person (either by decoding/decrypting data) such data becomes personal data; on contrary if a link cannot be established between specific data and a natural person then such data is not personal data. This, as Kuner suggests, creates a presumption that data are usually personal unless it can be clearly shown that it would be impossible to tie data to an indefinable person.[204]

The United Kingdom has been considered to have a complex and difficult to understand and use, yet very weak data protection regime.[205] She has been criticized for undermining data protection by narrowing the application of concepts through Court interpretation. About what constitutes personal data, UK has, through the Court of Appeal in the *Durant Case*[206] issued a ruling narrowing its meaning hence limiting data subjects' right to access personal information held by data controllers. According to the Court ruling, section 7 of the DPA on access of data subject to information held, was never meant to be a 'key' to allow access to all documents mentioning the data subject's name or any or all data retrieved by putting the data subject's name into a search engine. Consequently, the Court ruled, to qualify as personal data, information must be biographical and must have the concerned data subject as the central focus. Hence, a mere appearance of a person's name in records/files is not sufficient to make such information personal data. And although in 2014 the Court of Appeal in *Efifiom Edemii* v *The Information Commissioner and The Financial Services Authority*[207] clarified that, a name could be personal data as long as the name is not so common, the definition still deviates[208] from the DPD definition.

---

[200] *ECtHR, Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, para 65.
[201] *Coeriel & Aurik v the Netherlands* (1994) Comm 453/1991, para 10.2, reported in, inter alia, (1994) 15 HRLJ, 422; Bygrave, L. A, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, 1998, volume 6, pp. 247–284 at p. 253.
[202] See further *Niemitetz v. Germany*, 13710/88, 16 December 1992, para 29; *ECtHR, Société Colas Est and others v. France,* Application no. 37971/97, Judgement of 16 April 2002, § 40; *Coeriel & Aurik v the Netherlands* (1994) Comm 453/1991, para 10.2, reported in, inter alia, (1994) 15 HRLJ, 422; Bygrave, L. A, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol. 6, pp. 247–284 at p. 253; De Hert, P and Gutwirth, S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., et al (Eds), Reinventing data protection?, Springer Science, Dordrecht, 2009, 3-44 at p. 15; Boshe, P., 'Interception of communications and the right to privacy: commentary on Zitto Zuberi Kabwe's political saga', Open University Law Journal, 2013, Vol.4, No.2, pp.1-5.
[203] See further Kuner (n 139), p. 91.
[204] Ibid.
[205] EPIC,
[206] [2003] EWCA Civ 1746.
[207] [2014] EWCA Civ 92.
[208] Scholars such as Lorber criticized UK's approach as being in divergence on her obligations under the EU Directive. See Lober, S., 'Data Protection and Subject Access Requests', Industrial Law Journal, Vol. 33, No. 2, 2004, pp. 179-190, at p. 189: See also Chalton, S., 'The Court of Appeal's interpretation of "personal data" in *Durant v FSA*: a welcome clarification, or a cat amongst the data protection pigeons?', Computer Law and Security Report,

Nevertheless, the Court considered itself as being faithful to section 7 of the DPA and the DPD's intentions. As a result of UK divergence, WP 29 issued guidelines on the concept and its scope.[209]Regrettably, the UK still failed to correct her misinterpretation based on the WP 29 guidelines forcing the European Commission to issue her a formal warning for failure to implement the DPD.

On the other hand, Germany[210] and France[211] have wider definitions of personal data. In France, personal data is any information relating to a natural person who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to him. It means any data that may lead to an identification of a person is considered personal data. This includes a name, photograph, sex, ID numbers such as social security numbers, motor vehicle registration numbers, place or date of birth, address (physical or virtual) or biometric data such as digital prints or even a person's voice. It follows, therefore, even anonymized or encrypted data, if it can be deciphered and reveals the personal identity, is personal data.

In Germany, personal data means any information concerning personal or material circumstances of an identified or an identifiable person.[212] According to Douwe Korff, for Germany law to know whether information qualifies as personal data the test is relative. He says, 'the question of whether data "can be" linked to a specific individual depends (in German legal thinking too) on the knowledge, means and capabilities of the person handling the data. Certain data can, therefore, be "personal data" for one person (who can link them to a certain individual) but not "personal data" for another person who cannot relate them to the individual.'[213] It follows then, in the two jurisdictions, to qualify as personal data, information must be in a way that it allows an identification of a person, distinguishing him/her from other persons. The same forms the EU jurisprudence as decided by the CJEU in the *Promusicae* case.[214] The three scenarios are different from the case in UK where mere biographical information is not considered as personal data. In the UK personal data is contextual, a personal name can be considered a personal data in one context and not so in another.

UK does not consider IP addresses as personal data. Even in her transposition of the ePrivacy Directive 2002/58/EC through Privacy and Electronic Communications Regulations of 2003, IP addresses are never mentioned. In France and Germany, up until 2016 only static IP addresses constituted personal data. In relation to dynamic IP addresses, the Court of Appeal in France had ruled[215] that dynamic IP addresses did not constitute personal data. In the Court's opinion, dynamic IP addresses such as those collected on internet based searches do not, even indirectly,

---

2004, Vol. 20 No. 3, pp. 175-181 and Jagessar, U and Sedgwick, V., 'When is personal data not "personal data": The impact of Durant v FSA', Computer Law and Security Report, 2005, Vol. 21 No. 6, pp. 505-511.

[209]Article 29 Working Party's Opinion 4/2007 on the concept of personal data (WP 136).

[210] Korff (n 169), pp.3-4.

[211] Section 2 DPA.

[212] Section 3, Para 1 BDSG states that 'personal data' means any information concerning the personal or material circumstances of an identified or identifiable natural person ('data subject').

[213] Korff(n 169).

[214] CJEU, C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, 29.01. 2008. See para 45.

[215] Anthony G. vs. SCPP, 27 Avril et CA de Paris and Henri S. vs. SCPP 15 Mai 2007; See also L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes [The IP Address is Personal Data for All the European Data Protection Agencies], CNIL (Aug. 2, 2007), http://www.cnil.fr/la-cnil/actu-cnil/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/ accessed 23/07/2016.

allow identification of a physical person. Similar ruling was pronounced in Germany at the Federal level and some States. Explaining this position, a District Court in Munich opined that dynamic IP addresses lack the attributes for determinability since only the access provider could combine an IP address with individual person but not a service provider. And since the laws in Germany prohibit access providers from handing over the information identifying individuals, a mere dynamic IP address cannot be used to identify a person.[216] In contrast, Berlin and Koln consider dynamic IP addresses as personal data. The District and Regional Courts in Berlin respectively ruled that dynamic IP addresses are personal data.[217] Explaining their position, the Courts were of the opinion that, as long as the web provider can identify the person by combining the IP address and personal information, then both static and dynamic IP addresses are persona data. WP 29 came around to clarify the position. In their opinion of June 2007, the Working Party said IP addresses are personal data. Later in 2008, the ECJ affirmed the opinion of the Working Party in the case of *Promusicae* by ruling IP addresses as personal data. Of latest is the case of *Breyer v Bundesrepublik Deutschland,*[218] where the CJEU ruled that dynamic IP addresses constitute personal data. With the coming of the GDPR, IP addresses, both dynamic and static are, according to Article 4 read together with Recital 30, personal data.

2.4.1.3 Filling System

The DPD defines filing systems to include 'any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.'[219] The UK law considers filling system narrowly compared to the DPD. UK law defines a filling system as a set of data which is structured either by reference to individuals or by reference criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. This narrow meaning has been further narrowed by the ruling in the *Durant* case where the Court clarified that 'where not computerized, [filing system] would need to resemble the efficiency, accessibility and sophistication of a computerized system, allowing a data controller ready access to requested information.'[220] This means, as explained by Jagessar and Sedgwick;

> 'If a person has to 'leaf through files, possibly at great length and cost[s] to see whether it or they contain information relating to the person requesting information... [this would] bear no resemblance to a computerized search and therefore would not qualify as a 'relevant filing system.'[221]

Although in essence, the Court here was trying to lessen controllers' burden relating to access requests, the implication is the narrowing and divergence in standard in the meaning and scope between automated and manual filing systems. The Court went further declaring that it is not sufficient to constitute 'filing system' only on the basis that the files are structured by identifiers such as names or date. The data should be organized in a way that would enable one to isolate

---

216 In *AG München, decision of September 30th 2008 - 133 C 5677/08.*
217 In *AG Berlin-Mitte, decision of March 27th 2007 - 5 C 314/06* and *LG Berlin, decision September 06th 2007 - 23 S 3/07.*
218 Case C-582/14, CJEU, decision of 19 October 2016
219 EU Directive Article 2(c).
220 *Durant v FSA* [2003] EWCA Civ 1746, para 35.
221 Jagessar and Sedgwick (n 210), p. 507.

particular aspects of the personal information referred to.[222] To constitutes a filing system as intended under the law, one need not leaf through files to find relevant data. On the other hand, German law differentiates between manual and automated data while France disregards the DPD categorization regarding 'decentralized' and 'dispersed' systems.

2.4.1.5 Consent

Consent under the DPD is a requirement for processing of personal data. Under Article 7(a) of the DPD, consent is considered sufficient as long as it is not ambiguous. The UK law, like the DPD does not clarify what constitutes a valid consent. Korff[223] believes, the law suggests that a consent can be sufficiently 'implied', it need not be signified. This approach is relatively weaker than that of France[224] and Germany.[225] The BDSG goes further than the DPD by explaining what constitutes a valid consent. BDSG states, for consent to be valid, it must be informed and given freely by a person concerned. The consent requirement under the BDSG became stricter with the 2009 amendments. The amendment obliges data controllers to properly inform data subjects of the intended purposes of processing on collection.[226] The information that is given to a data subject, as explained by Korff, 'must be very specific[227]as to enable data subjects to make an informed decision as to whether or not to give their consent. In extension to what the DPD provides, the BDSG provides for a form of consent, something that the DPD did not stipulate. The Law requires consent to be in written form, or in exceptional circumstance, the law accepts digital forms or digital signature as signalling consent to contracts concluded online.[228] In Germany, as in France, data subject's consent is required for any subsequent processing of personal data whereas in UK initial consent is sufficient for subsequent processing of personal data.

The coming of the GDPR has prompted the ICO to reform the status and mode of the consent. According to its GDPR Consent Guidelines of March 15, 2017, [229]proposes that consent must be written or verbal statements acknowledging consent. However, if consent is implied, it should be by a clear and affirmative act to which the giver understand that the acts constitute consent to a certain obvious purpose. The Guidelines also suggests a possibility of withdrawal of consent and expiration of consent after a certain period.

---

[222] *Durant v FSA* [2003] EWCA Civ 1746, para 35.
[223] Korff, D., 'Report on Implementation of the Data Protection Directive: Comparative Summary of National Laws', Cambridge-UK, September 2002, p. 27.
[224] Keith (n 188), p. 115.
[225] BDSG, Section 4 a (1).
[226] It must be remembered that in Germany, there are different regulations for public and private sector. Section 4 (2) BDSG regulates public sectors. The provision requires data controllers to collect data directly from the data subject so as to give them an opportunity to exercise their rights including consenting the prospective processing activities.
[227] Korff (n 169), p. 17.
[228] See *Formgesetz,* 13. Juli 2001 and *Signaturgesetz,* 16. Mai 2001.
[229] Available at https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/

2.4.1.4 Data Controller

Different from the DPD, the BDSG and the French law defines 'data controller' broadly to refer to any person or body collecting, processing, or using personal data on his or her behalf or commissioning others to do the same.[230] The UK law provides for a definition of a data controller as any person who determines the purpose for which and the manner in which any personal data are to be processed.[231]

2.4.1.6 Data Processor

The DPD considers data processor as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[232] The concept has not been defined under the BDSG. The UK[233] and France[234] adopt the DPD definition of a data processor. However, the UK adds an explanation to it; that, employees are not to be considered as processors.

2.4.1.7 Third Party

A third party is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorized to process the data.[235] While France does not provide for third party, the UK and Germany has adopted the above meaning as stipulated by the DPD. In the UK the law uses slightly different phrasing although with the same meaning[236] while in Germany the law restricts the concept to persons carrying processing activities under the instruction of the data controller within the EU and the EEA only.

2.4.1.8 Recipient

The DPD considers a recipient as any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. However, the authorities which may receive data in the framework of a particular inquiry are not regarded as recipients.[237]

---

[230] BDSG, Section 3, Para 7.
[231] UK Data Protection Act 1998, Section 1 (4).
[232] EU Directive, Article 2 (e).
[233] UK Data Protection Act, Section 1.
[234] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 35 (2).
[235] EU Directive, Article 2 (f).
[236] The law uses '…authorized to process data for the data controller or processor' instead of 'under the direct authority of the controller or the processor' as phrased in the DPD.
[237] EU Directive, Article 2 (f).

2.4.2 Data Protection Principles and Processing Conditions

2.4.2.1 Criteria for legitimate processing of 'ordinary data'

The French, German and UK laws transposed similar principles for data protection as stipulated in the DPD. However, the scope and context in the application (based on judicial interpretation) differs. The extent of protection is also affected by the varied meanings and scope of operating terms as discussed in the above sub-section. For instance, in Germany, the primary criterion for legitimate processing is a free consent, processing based on law or to fulfil a legal obligation. This is also the position proposed under the DPD.[238] France, on the other hand, considers free consent as a primary determinant of a legitimate processing activities[239] while the two other categories, i.e. processing based on law and to fulfil legal obligation are an exception to the primary rule.[240] A major diversion is made in the UK law. In the UK, the law does not consider consent as a requirement for legitimate processing; instead, the law requires the processing to be 'fair and lawful'.

2.4.2.2 Criteria for legitimate processing of sensitive data

In the processing of special category of data (popularly known as sensitive data) the DPD under Article 8 sets a rule that such data may only be processed with an explicit consent.[241] The DPD has listed a number of data considered 'sensitive'[242] to which the Members States have adopted and some extend the list further. In principle, the DPD requires Member States to prohibit processing of sensitive personal data. The PDP further gives States room to allow the processing of sensitive personal data as an exception but upon certain conditions. In the processing of sensitive data the French law requires an express consent; and an additional requirement is made to genetic and biometric data which, apart from an express consent, requires DPA's authorization. In Germany, prior processing authorization or a prior checking of the data by the DPA is required before any data considered sensitive can be processed.

[238] EU Directive, Article 7 (a).
[239] Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 7.
[240] Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 7 (2-5).
[241] EU Directive, Article 8.
[242] These include 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life; See EU Directive, Article 8 (1).

2.4.2.3 Data Protection Principles

Collection and processing principles The DPD stipulate the needs for data controllers to ensure certain conditions are met in order to sufficiently ensure personal data is secured.[243] First, the DPD stipulates that, 'data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.'[244] It means, collection of personal data should be limited and defined by its purpose to process with clarity and specificity. In clarifying 'purpose' WP[245] insists that the purpose of processing must be clear to allow determination and quantity of data required. In illustrating this fact, the Working Party stated, ambiguous, generic or broad description of purpose such as 'improving user experience' or 'marketing purposes' are not sufficient determinants of purpose.[246] In enforcing this provision, the UK law provides that, 'data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'[247] The law has expanded the principle allowing collection of data for multiple purposes and processing activities. ICO clarifies this saying, processing for other purposes is not prohibited by the law as long as the processing is compatible with the original purposes.[248] In determining compatibility of purposes, ICO provides that one;

> '…should bear in mind the purposes for which the information is intended to be used by any person to whom it is disclosed….. Because it can be difficult to distinguish clearly between purposes that are compatible and those that are not, we focus on whether the intended use of the information complies with the Act's fair processing requirements. It would seem odd to conclude that processing personal data breached the Act on the basis of incompatibility if the organization was using the information fairly…… If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you have to consider whether this will be fair.'

It is safe to interpret that, what ICO is saying is that, as long as processing is fair, further the processing is legal under the UK law. The DPD under Article 6 (1) (b) was meant to give controllers flexibility to determine a further use of personal data. To come to a proper conclusion on compatibility, WP recommends that, the controller to look into the context in which data was collected and reasonable expectation of the data subject with regards to further processing. Treacy and Bapat[249] in clarifying WP opinion believes that the WP emphasizes on 'the need to look at the nature of the relationship between the data controller and the data subject and the balance of power, which includes not only the information provided to the data

---

[243] EU Directive, Article 6.
[244] EU Directive, Article 6 (b).
[245] Article 29 Working Party, Opinion 03/2013 on purpose limitation as set out in Article 6(1)(b) of the Data Protection Directive 95/46/EC, (WP 203) April 2, 2013.
[246] Ibid, p. 52; See also Rauhofer, J., 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?', EDPL, Vol 1, 2015, pp. 5-15.
[247] UK Data Protection Act, Schedule 1: Part 1, Para 2.
[248] UK ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-2-purposes/ Accessed 23/07/2016.
[249] Treacy, B and Bapat, A., 'Purpose limitation – clarity at last?', Privacy & Data Protection Journal, 2013, Vol. 13 No. 6, pp. 11-13 at p. 12.

subject, but also a consideration of 'what would be customary and generally expected practice in the given (commercial or otherwise) relationship'. Of course, this will also depend on the extent of sensitivity of data and processing operation involved. Hence, as the authors' advice, there is a need to take into account positive and negative effects of proposed further processing activities and potential privacy invading effects of such actions to data subjects.[250]

The WP further recommends the implementation of additional safeguards such as data encryption, aggregation, PETs in any further processing as a remedial tool to ensure compatibility. The fairness principle by ICO as a warranty to further processes seems to be short of the DPD data compatibility exception. According to ICO, fairness means being transparent to individuals about how their information will be used.[251] It further elaborates that 'assessing whether the information is being processed fairly depends partly on how it was obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair……The Data Protection Act says that information should be treated as being obtained fairly if it is provided by a person who is legally authorized, or required, to provide it'. In effect, personal data are always to be treated as being obtained fairly if they were received from a person who was authorized by law as long as the rules regarding information to data subjects are complied with.[252]

In Germany, this principle is, in addition to what is stipulated under the DPD, requires that data must be collected directly from the data subject[253] and must be kept in minimal. According to Knorff, in Germany, purpose limitation is the very heart of the Germany Law.[254] This is the idea behind the Germany's 'data reduction and data economy' rule which has been enshrined in the law.[255] This is the reason the German DPAs issued several press releases in 2015 to object CoE proposals to weaken the purpose limitation principle in the GDPR by making it legitimate for the same controller to process personal data for 'incompatible' purposes as long as the processing is for legitimate interest of the controller or a third party.[256]

The rule as applied in German requires that collection of personal data must be as minimal as possible for the intended purpose. To enforce the aspect of 'purpose specification', the rule requires, as explained by Knorff, organization and structuring of tools for data processing to ensure economy of data in the processing activities. Inevitably, this enforces structural requirements for processing systems, which as per section 3 (a) also includes data anonymization or pseudonymization whenever possible. [257] [258]

Article 6(1) (c) of the DPD also supports the idea of 'data minimization' stating that data must be 'relevant and not excessive in relation to the purposes for which they are collected and/or

[250] Treacy and Bapat (n 249)
[251] UK ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/ accessed 23/07/2016.
[252] Korff (n 106), p.8.
[253] BDSG, Section 4 (2).
[254] Korff (n 169), p. 12.
[255] BDSG, Section 3.
[256] Visit www.bfdi.bund.de and www.datenschutz.hessen.de to access the press release.
[257] Korff (n 169), p. 15.
[258] The exception to this rule is under section 28 in application of the '*principle of proportionality'*.

further processed.' The idea is to restrict data collection to such data as directly relevant with reference to specific processing purposes.

In France, Article 6(3) provides for a similar principle as the one provided under the DPD. Accordingly, for further processing and the question regarding compatibility of data, the CNIL controls this through the process notifications by data controllers.[259]

The above principle also enforces the obligation not to retain personal data longer than necessary for the purposes for which it was collected. Under the DPD the principle is termed as the data retention principle which requires retention of data for so long as is necessary for the purpose for which they were collected. This principle had been further enhanced in 2006 by the adoption of the European Data Retention Directive in 2006.[260]

One of the major aspects of data protection regulations is the maintenance of quality, reliability and integrity of personal data. Article 6(1) (d) of the DPD enforces the above principle by enacting data quality principle. This principle insists on the relevance, accuracy and completeness of data for the purpose.[261] In essence, this principle obliges data controllers to ensure data is kept accurate an up to date.

Transparency and accountability A controller has obligations to keep data subject informed on the use of their data and to ensure compliance with their processing activities with the law. The DPD Articles 10, 11 and 12 advocates for transparency. They require data subjects to be informed of the processing activities relating to their data, to ensure transparency and allow data subjects exercise their rights to access. As expressed by AWP,[262] accountability ensures controllers are keen with their obligations. This includes putting in place measures to guarantee compliance with data protection rules in a context of processing operations and documenting processing activities as a proof and to demonstrate measures taken in adherence to the law. Transparency involves the right of data subject to access information about his data and involved processing activities. Furthermore, access rights are considered to have dual nature, first is the right to access one's data and second the right to request for amendment, block or deletion of the data. This aspect has been clarified in *College van Burgermeester en wethouders van Rotterdam v. M.E.E. Rijkeboer.*[263]

In the UK, the law requires that information on processing activities should be provided or made readily available in so far as practicable. This, as clarified by ICO means, 'data controllers must be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data [and] handle people's personal data only in

[259] Korff, D (ed)., Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Case study France, 2010, p. 9.
[260] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC of 15 March 2006, OJL 105, 13.04.2006, p. 54- 63.
[261] EU Directive, Article 6 (1) (d) 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.'
[262] Article 29 Working Party, Opinion 2/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010.
[263] ECJ, case C-553/07, 7 May 2009 in paras 51-52.

ways they would reasonably expect'.[264] However, on the other side of the coin, data subjects' right to access has been hugely limited by the decision in the *Durant case*. By narrowing the meaning of personal data and filling system, data subjects' access right has also been affected. This was the Court's holding that a determination of whether or not data is personal data, consideration should be made as to 'whether or not the data is significantly biographical; that is, where the data conveys information beyond a person's mere involvement in particular occurrence'.[265] The Court also directed that, where the focus of the data is not on the specific person, a mere mentioning of a person's name in a document or file does not necessarily affect the data subject's privacy to confer the subject access right.[266] This interpretation, according to Rempell,[267] is inconsistent with the spirit of the DPD. He argues that the DPD's definition of personal data is not to be subjected to any limiting interpretations. Although the wording in the UK's DPA are consistent with the wording in the DPD regarding what is personal data, the Court of Appeal in the *Durant* case erred itself in interpretation of the concept. In effect, under the UK law, mere appearance of personal biographical details in a file do may not qualify it as a personal data to warrant subject's right to access and other related rights.

In France, despite the fact that the right to information forms the CNIL doctrine, the law does not have provisions requiring data controllers to inform data subjects of the processing activities when the respective data was not collected directly from the data subject.[268] This goes contrary to the spirit of the DPD. The DPD requires data subjects to be informed of the data collected from other sources (if they are not already aware of the collection) for purposes of fairness. Again, French law proves to be inconsistent with the DPD in this aspect, unlike the UK law which is keen and emphatically on the information to data subjects. However, with regards to subjects' access right, once data subject requests access to data, a data controller is obliged to respond to the request within two months. Consequently, a data subject can, under Article 40 of the French law request for deletion, rectification, block or updating of the data.

In German BDSG, the right to access to personal data extends to non-structured files. Section 19 of the BDSG requires the data controller to provide, upon request, to data subject with access to any data related to them, including information on the source of data, recipients of the data and purposes for processing and storage of the data. In fact, Section 33 obliges data controllers to inform subjects of the collection of data on the first instance. The information which data subject must be provided with must include a type of data and the purpose for the collection, nature of processing activities and identity of the controllers and recipients, (if any). This obligation is in line with article 10 of the DPD.

Data security and confidentiality Data security and confidentiality are provided for under Articles 16 and 17 of the DPD. A controller and any person under controllers' instruction must process data only as per controllers' instructions.[269] In enforcing this requirement, the controller is to ensure

[264] UK ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/accessed 23/07/2016.
[265] *Durant v FSA* [2003] EWCA Civ 1746, para 35, Para 28.
[266] Ibid.
[267] Rempell (n 29), p. 825.
[268] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 11 (1) (c); Korff(n 259), p.20.
[269] If the controller involves agents or third parties, the DPD obliges the draw of contract on legal relation between the controller and processor/agent with access to personal data under the authority of the controller. As such, all

that personal data is sufficiently secured. The DPD suggests the use of both technical and organizational safe guards. To comply with the provisions, the UK law requires data controllers to take 'appropriate technical and organizational measure' in light of the technological development. The law makes reference to security against 'unauthorized or unlawful processing or accidental loss. The similar provision is provided under the French law where controllers are required to take all necessary precautions with regard to the nature of the data and the risks of processing to prevent such data from being altered, damaged and against unauthorized access by third parties.[270] On the other hand, German BDSG goes beyond the above security requirements. The BDSG does not only require the provision of the technical and organization safeguards; it explicitly refers to the use of encryption and PETs to counter technological development that may have an adverse effect on data security.

The three jurisdictions took a risk-based approach in implementing the DPD requirement on security and confidentiality of personal data. The enforcing authorities in the three jurisdictions have gone an extra mile by publishing guidance advocating for the use of encryption as means to enforce confidentiality especially on personal data processed on the cloud.[271]

Furthermore, with regards to sensitive,[272] professional and official confidential data, the law in Germany, under Section 42a requires data controllers to notify data subjects and the DPA of any data breach including unauthorized access or unlawful processing of personal data when such breach poses a significant harm[273] to the rights and protected interests of data subject.[274] The law imposes a duty to the controller to eliminate the breach and secures the data. In France, a similar requirement is imposed on registered electronic communications service providers. The providers are duty bound to notify the DPA and the data subject[275], within twenty-four hours of data breaches regardless of their gravity.[276] The UK law has no corresponding obligation under the law; however, in practice, the ICO imposes an obligation to DPA to report serious breaches. According to ICO, cases that qualify to report include those with potential harm to individual rights and the sensitivity of compromised data.

Trans-border data transfer The DPD establishes a regime for international data flow. The regime restricts the flow of information to third countries without an adequate framework for data protection.[277] The DPD does not have a precise measure to determine 'adequacy' of data protection frameworks but offers no guideline to such determination. To have an adequate data protection framework, a country must have both the substantive measures (data protection

persons engaged by the controller. The controller is further made liable to ensure compliance to data protection rules to all data processed by processors or agents under instruction.

[270] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 34.

[271] See the FFC, Report on the legal obligations for encryption of personal data in Europe and Asia, 2013.

[272] BDSG, Section 3 (9).

[273] Although the law has not provided the meaning of 'significant harm' it is assumed that the determination is left to the controllers.

[274] For cases involving a large number of data subjects, the law, to reduce a burden to the controller, requires that the breach notification to be published by way of advertisement in at least half a page in at least two national daily newspapers or a means with similar exposure (Section 42a).

[275] Notification to data subject is conditioned upon the effect of the breach to subject's privacy rights.

[276] Section 34 and Decree 2012-436 of 30.03.2012.

[277] EU Directive, Article 25.

principles) and procedural mechanism for enforcement. In short, a country should have guiding legal principles, an independent supervisory authority and a good level of compliance.

When a country lacks an adequacy protection, EU Member States are prohibited from transferring personal data unless the transfer is made under Article 26 of the DPD. Article 26 permits transfer to third countries without an adequate level of protection as an exception to the general prohibition. This can happen if the EU Member State and the third country have executed a Standard Contractual Clause subject to EC approval; in case data is to be sent to an affiliation in a third country, parties can implement Binding Corporate Rules for data transfer; or an individual data subject can consent to the transfer.

In this aspect, German BDSG took a different approach as that proposed in the DPD. Germany looks at the 'adequacy' or protection offered by the recipient of data in the third country and not the 'adequacy' or protection offered by laws and regulation in the third country. An illustrative example is a decision taken by the *Düsseldorfer Kreis*[278] ('Dusseldorf Circle') cautioning German DPA's from accepting a blanket 'adequacy' decision made about the Safe Harbour, urging them to consider each data importer independently of SH determination of an adequate protection by the European Commission. This decision required German data exporters to carry out minimum checks to ensure that data importers are not only SH certified but also adhere to data protection principles therein.[279] On the other hand, UK and France adopted the framework suggested by the DPD. The UK goes further by declaring an acceptance of any declaration made by the CoE on third parties regarding provision of adequate level of protection while France has, in 2015 announced to grant single authorization to a group of companies that adopts BCRs.[280] However, following the *Schrems* decision in 2015 on the validity of SH, CNIL ordered data controllers to stop all data transfer to the US by the end of January 2016 or invoke the use of Modal clauses or BCRs on a transfer of personal data to the US.

2.4.3 Enforcement Mechanism and Data Protection Authorities

2.4.3.1 Enforcement

As part of a safeguard measure, the DPD under Article 19 requires countries to create a system of notification of all wholly or partly automated processing. To address this aspect, the French law took a different approach; instead of imposing the requirement to notify, it requires data controllers to register with the DPA and obtain authorization especially on processing activities by a public body and when processing involves sensitive data. The law requires only a

[278] Is a working group of all German supervisory authorities (DPAs) considered by its members as equivalent to Article 29 Working Party but publishes its opinions in a form of 'resolutions' which reflects the position of supervisory authorities.

[279] The decision was reached when Safe Harbour was still regarded as providing adequate level of protection before it was invalidated by the ECJ in 2015. In this decision which was reached on 28/29 April 2010, the *Düsseldorfer Kreis* resolute to sanction any data exporter who fails to carry out measures to ensure 'adequacy protection' by the US based data importer. see Schmidl, M and Krone, D., 'Germany DPAs Decide EU-U.S. Safe Harbor May Not Be Relied Upon Exclusively', http://www.bnai.com/GermanyDpas/default.aspx cited in Makulilo (n 26), p. 209.

[280] See CoE Report analysis of transposition, p. 32; According to the announcement by the CNIL, once a company adopts BCRs it will not need any subsequent authorisations for transfers to third countries.

notification of the period for data retention. Similar to France, the UK law requires registration of all data processing activities. Unlike France, in the UK data controllers do not need prior authorization to process personal data neither are they required to notify the DPA on the data retention period. Germany has diverged from the requirement of notification[281] and registration; the law imposes stricter requirement but with the same objective. It requires every data controller to appoint a data protection officer.[282] The data protection officers oversee compliance with the data protection law. In a case of failure to appoint data protection officer, the data controller is obliged to seek DPA authorization with every processing activity. Notification requirement, as in France is also required on data retention period.

2.4.3.2 Data Protection Authority

The DPD requires any data protection framework to establish an independent supervisory authority.[283] The independence referred to by the DPD is the functional independence. To achieve this independence, scholars argue that the authority must avoid unnecessary dependence on other bodies, which may undermine its functional independence or create such an assumption;[284] as elaborated in *European Commission v. Federal Republic of Germany*,[285] that any direct or indirect influence to the authority functionality undermines the requirement of Article 28 (1) of the DPD. No body must have either actual or perceived functional influence over the authority.

The Court elaborated that, the ultimate goal of Article 28 is to allow these authorities to act objectively and impartially hence guarantee effectiveness and reliability in enforcing national laws in protection of individual rights in the processing of personal data. To ensure its independence, Article 28 (2) requires the authority to equip itself with personnel who possess legal and technical expertise to enable the discharge of its functions freely.

The laws in the UK, France and Germany provides for the establishment of such an independent authority. However, in practice, these authorities leave a lot to be desired. For instance, the ICO, UK's data protection authority has limited enforcement powers. ICO is more of a pragmatic body than punitive. It may pronounce a controller as being in breach of the law but cannot issue any fine.

Before January 2016, Germany had ten of the sixteen *Länder* as part of the Ministry of interior and the Regional Government as sub ordinate authorities.[286]This means the Regional Government was under the instruction of the respective Ministry. The remaining six *Länder* the supervisory authorities oversee the processing activities, but the determination of lawfulness and

[281] Notification is only required in processing activities for in anonymized and non-anonymized commercial transfers and for marketing and opinion researches.
[282] BDSG, Section 4 (f) (1).
[283] EU Directive, Article 28.
[284] Makulilo (n 26), p. 189; Bygrave (n 60), p. 70.
[285] ECJ C-518/07, Paras 18-25.
[286] These included Baden-Württemberg, Bavaria, Brandenburg, Hessen, Mecklenburg-Vorpommern, Rhineland-Palatinate Saarland, Saxony, Saxony-Anhalt and Thuringia. [see article 35 BDGS]

appropriateness of such processes was reserved for the Ministry.[287] As a result of this interaction between the Ministry and the *Länder* authorities, the ECJ[288] ruled the *Länder* as not having sufficient independence based on the fact that they are part of the Regional Administration and subject to State scrutiny. In its defense, Germany elaborated that, the State scrutiny over the *Länder* is simply a routine administration's internal monitoring mechanism which has no effect on the independent functionality of the authorities. In rejecting this argument, the ECJ stated that the 'requirement of independence precludes any external influence, whether direct or indirect which could call into question the performance of the DPAs of their tasks and competences descending from the Directive'. However, the Germany Parliament (*der Deutsche Bundestag*) decided to strengthen the independence of both the Federal and States' (*Länder*) Data Protection Authorities. The DPAs are, as of January 2016 independent of the Ministry of interior and the Regional Government which existed since 1978 and continued after the adoption of the DPD. The presently, the Federal DPA reports to the Parliament, and his/her decision is subject to judicial review.[289]

2.5 Conclusion

In the context of the DPD, Korff advised on uniformity in transposition of definitions as the key to proper and sufficient implementation. He suggested that even a minor change in the wording of definition can have significant effects in the application/applicability of rules. He illustrated the situation, 'As a result of seeming minor additions or variations, some data will be regarded as 'personal' in some countries but not in others; some processing systems will be regarded as (sufficiently structured) 'filling systems' to fall within the law in one country, but as insufficiently structured or easily searchable and thus outside the law in another'. This situation reflects what has been shown in the discussion above, for instance, in relation to the UK definition of the filing system and personal data as compared to the DPD, France and Germany.

Perhaps the hard truth is explained by Legrand that a total harmonization is impossible because, one, the meaning of law in different cultures can never be the same, and two, the meaning cannot survive the journey (in case of transposing the law). The meaning of a legal rule is thus contextual but more importantly a function of application of the rule by its interpreter, of the concretization or instantiation in the events the rule is meant to govern. In elaborating this position, He posits:-

> 'This ascription of meaning is predisposed by the way the interpreter understands the context within which the rule arises and by the manner in which she frames her questions, this process being largely determined by who and where the interpreter is and, therefore, to an extent at least, by what she, in advance, wants and expects (unwittingly?)

[287] These include the Bremen, Hamburg, Lower Saxony and North Rhine-Westfalia.
[288] *European Commission v. Federal Republic of Germany*; ECJ C-518/07.
[289] Information published online on 29.12.2017 with title ‚*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wird ab 01.01.2016 eigenständige oberste Bundesbehörde und gibt einen Ausblick über die 2016 anstehenden Aufgaben*', available at https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/27_Update%20BfDI%202.0%20-%20Ausblick%202016.html Accessed on29.03.2017

> the answers to be. Hence, the meaning of the rule is a function of the interpreter's epistemological assumptions which are themselves historically and culturally conditioned. These prejudices are actively forged, for example, through the schooling process in which law students are immersed and through which they become impressed with the values, beliefs, dispositions, justifications, and the practical consciousness that allows them to consolidate a cultural code, to crystallise their identities, and to become professionally socialised. Inevitably, therefore, a significant part of the very real emotional and intellectual investment that presides over the formulation of the meaning of a rule lies beneath awareness, because the act of interpretation is embedded, in a way that the interpreter is often unable to appreciate empirically, in a language, in a morality, and in a tradition, in sum, in a whole cultural ambience that guides the experience of a concept —what Hans-Georg Gadamer would refer to as a "pre-understanding" *("Vorverständnis")'*.

In the present context, Germany is considered to have the strictest framework for data protection standards. On the 24th February 2015, Germany adopted a new Consumer Protection law which enables consumer protection associations to file cases on behalf of data subjects for violation of their rights. More specifically, the consumer organization may file cases against data controllers who use personal data for advertising and marketing, in opinion researches or use of geographical data to track or trace data subjects for promotion purposes. Perhaps this is attributed to Germany history and the constitutional foundations of the right to privacy. Country's history, judicial and political will have led to varied doctrines affecting the nature, aims and objectives of data protection laws and their judicial interpretation as illustrated in the above discussion. Nevertheless, the importance of, at least, principles of data protection has an importance in achieving the equivalence in protection and objective enforcement across jurisdictions.

France law provides for a similar context as provide by the DPD and in few instances stricter protection. Moreover, apart from her being a member of the EU, France is also part of the Association of French-speaking Data Protection Authorities (AFAPDP) drafting, adopting and enforcing different conventions and data protection regulations. Thus, France enforces not only EU regulations but also conventions, agreements, and regulations adopted under the AFAPDP. For this reason, France is likely to have one of the technological and user pattern responsive frameworks for data protection in Europe.

The United Kingdom has to a larger extent transposed similar contents as the DPD. Unfortunately, judicial interpretation of the law has undermined the level of protection offered to personal privacy and data security. Consequently, regardless of the similarity in texts, UK data protection framework provides for a lesser protection as compared to Germany and France.

3. Privacy in the African Culture and the African Customary Legal System

3.1 Introduction

Africa is a Continent of fifty-four States and six dependent territories. The Continent is known for political instability, civil wars, poverty, unstable and feeble corrupt legal systems. Although Jane Williams argues, that governance situation has been improving in the last decade.[290] This chapter examines the concept 'privacy' and its meaning in Africa. Moreover, this chapter discusses privacy perceptions and how they determine development and functionality of privacy and data protection in Africa. In this way, it looks at the weaknesses, strengths and opportunities these perceptions have in responding to changes and global dynamics with regards to data protection. In understanding contextual framework, the chapter also examines related terminologies used with privacy.

The chapter is the foundation for the analysis of the case studies in chapter five. It demonstrates that the need to understand contextual knowledge of certain framework and cultures is inevitable in developing or changing such frameworks. This is especially with privacy regimes as they regulate social behaviors which are highly influenced by specific culture. In which case, David Nelken argues, creating privacy and data protection frameworks 'needs cautious designing in reflecting social values of a particular culture since such values affect privacy perceptions, meaning and they are the foundations of the jurisdictions creating and supporting privacy regimes. Consequently, a privacy framework needs to conform to the cultural context in which it is located for it to be effective.[291]

Culture defines law, its purpose, where and how it is to be found.[292] Arguably, even when the rule is imported, its application is contextual. Its effectiveness depends on the ability of the interpreter to link the rule with cultural foundations and employ what Krygier refers to as a positive sanctions and persuasions to ensure compliance.[293] Hence, by decoding African perceptions and understanding of the concept privacy, and its regulation, the chapter lays a foundation to determine acceptability and workability of imported regimes (or any other local regimes) in Africa. In doing so, it allows identifying strength, weaknesses and flaws within those regimes and the overall reform process against the core objective of privacy and data protection laws.

3.2 Africa: Political, Socio-Economic and Technological Context

Africa is the second largest continent after Asia, with 22.4% of global mass (30.2 million square kilometers). It has a population of over one billion people with an average growth of a

[290] Williams. J., 'UPDATE: Sources of Online Legal Informatics for African Countries', Published May/April 2015 on http://www.nyulawglobal.org/Globalex/African_Law1.htm accessed on 03/07/2015.
[291] Nelken, D., 'Towards a Sociology of Legal Adaptation' in Nelken, D and Feest, J (eds), Adapting Legal Cultures, Hart Publishing, USA, 2001, pp. 25-26.
[292] Ibid.
[293] Krygier, M., 'Is there Constitutionalism after Communism?: Institutional Optimism, Cultural pessimism, and the Rule of Law', International Journal of Sociology 1996-1997, Vol. 26, No. 4, pp.17-47.

population of approximately 2.5 million per annum. (World Bank Report). Africa is made of 54 independent States. Politically, the African States have presidential systems of government; with a President as the head of State and head of government. Most States practice multi-party political system.[294] This has not always been the case. When African States got their independence around 1960s-1970s, they inherited Constitutions which defined a type of government and political powers. These Constitutions were regarded as imposed to the African States by the departing colonial masters. These Constitutional contained principles considered 'alien' to Africans. The Constitutions introduced separation of powers, the rule of law, parliamentary supremacy, and judicial independence; bills of right and introduction of the multi-party political system.

Independent Constitutions did not last long as the emerging States amended or replaced them with new Constitutions legitimizing authoritarian rule with either military governments or single-party regimes. This was done under the guise of self-discovery and socialist ideology, and on a political argument that the independent Constitutions were neo-colonial devices designed to ensure 'the preservation of imperial interests' in the newly emergent state. [295] Basically, the new governments watered down the essence of constitutionalism and democratic governance.[296] The new Constitutions were modelled as Constitutions of power, not liberty or limitation; empowering African ruling elites with outmost ruling power. Prempeh describes the situation as a creation of 'the notion of African managers to newly sovereign…could or should be restrained constitutionally in their exercise of power whereas previous European colonialists had not been was deemed a contemptuous insult…the result was the rise of Africa's imperial presidents'.[297]

The end of the 1960s, as a result, witnessed derogation of democracy, gross violation of human rights with impunity across the Continent. The ruling parties which had become intolerant of opposition politics stifled democracy and sacrificed constitutionalism on the altar of political greed.[298] This resulted in civil wars; *coup d'etats* with military overthrew governments to rectify socio-economic and political messes by these governments. Unfortunately, the military regime fell into the same faults as civilian administration.[299] This, together with the collapse of the USSR as a super power after the cold war, rendered African economy stagnant and African States had to surrender themselves to international donor communities (World Bank, International Monetary Fund e.tc.) in efforts to rescue the devastated economy.

To access economic reliefs, African states had (as a condition from donor organizations) to go through 'structural adjustment programmes' (SAPs). SAPs required African states to liberate their political systems by introducing multi-party political systems, democratic elections, adherence to bills of rights and good governance; most of the features of the Independence

---

[294] Gentili, A. M., 'Party systems and Democratisation in Sub-saharan Africa', Paper presentation at the Sixth Global Forum on Reinventing Government, Seoul, Republic of Korea, 24-27 May 2005.

[295] See Prempeh, H.K., 'Africa's "constitutionalism revival": False start or new dawn?', International Law Journal, Vo.l5, 2007, pp. 469-506 at pp. 473- 474; See also Nyerere, J.K., Freeedom and Development/Uhuru na maendeleo, Oxford University Press, 1973.

[296] Mbondenyi, K. M and Ojienda, T., 'Introduction to and overview of constitutionalism and democratic governance in Africa' in Mbondenji, K.M and Ojienda, T (Eds)., Constitutionalism and Democratic Governance in Africa: Contemporary Perspectives from Sub-Saharan Africa, Pretoria University Law Press, 2013, p. 4.

[297] Prempeh (n 295), pp. 480 and 482.

[298] Mbondenyi and Ojienda(n 296).

[299] Umuzurike, U., The African Charter on Human and Peoples' Rights, 1997, p. 22.

Constitutions. This marked the third phase in the constitutional making in Africa. The states adopted or amended their Constitutions to incorporate liberal constitutional principles. This explains the revival in constitutionalism in the continent in the last two decades.

Today, single-party parliaments, military juntas and presidents-for-life no longer dominate the political map of the Continent as they did at the end of the 1980s.[300] Few countries are moving into the fourth phase of constitutional making, strengthening liberal constitutional principles, imposing limits to executive powers, grant the judiciary independence and parliamentary supremacy and guarantee important civil and political liberties. The new wave prompt scholars such as Gyima-Boadi to refer to the situation as the 'rebirth of African liberalism'.[301]

Social-economic Africa is the least developed Continent with majority of its people living below poverty line, high prevalence of diseases and malnutrition. It has comparably weak physical and knowledge infrastructure, poor telecommunications and transport facilities.[302] Yet, in terms of natural resources, it is one of the richest, with 50% of the world's gold, most of the world's diamond and chromium and 90% of the world's cobalt (Williams 2009). However, Africa accounts for less than 2% of the global trade.[303]

Africa's economy is still regarded as agrarian (pre-industrial) with little export. Agriculture which forms the largest sector of its economy faces challenges for lack of technology, viable industries, draught conditions, capital and researches;[304] misguided economic policies, corruption and uncaring (neglecting governments). For the same reasons, the mineral sector and tourism are yet to be fully utilized despite wealth in these areas. Furthermore, fifteen nations are landlocked, with no direct connection with global market; as such, their participation in the global economy relies on international cooperation with neighboring States with ports and shipping services. As a result, 'there is only handful of African countries with GNP above $1000,[305] with just as many countries reporting GNP below $200.[306] However, it was projected that growth in Africa's economy would occur in 2014. The boost is a result of global economy and improvements in regional business environment, but a bigger role is played by increased domestic demand.[307]

Although there is arguable growth in GDP, this does not reflect the real living standard of an African. Research conducted by Boston Consulting group (BCG) and the Tony Blair African Initiatives concluded that GDP is not a perfect measure for living standards in Africa. Levels of well-being are out of whack with its GDP. Hence a mere GDP growth does not translate into a

---

300 Prempeh (n 295), p. 471.
301 Gyima-Boadi, E., 'The re-birth of African Liberalism' in Diamonds, L and Plattners, M.F (Eds), Democratization in Africa, John Hopkins University Press, 1999; See also Diamonds, L., 'Introduction to Democratization in Africa', in Liberalism' in Diamonds, L and Plattners, M.F (Eds), Democratization in Africa, John Hopkins University Press, 1999.
302 Dogbey, G. Y., 'Towards Strategic Vision for a Continent in Distress' in Adesida, O and Oteh, A (Eds), African Voices - African Visions, The Nordic African Institute, Stockholm, Sweden, 2001, pp. 37-38.
303 Arieff, A. et al., 'The Global Economy Crisis: Impact on Sub-Saharan Africa and Global Policy Responses', CRS Report for Congress, 2010, p. 8.
304 Makulilo (n 26), p. 268.
305 Botswana, Cameroon, Libya, Namibia, South Africa.
306 Chad, Ethiopia, Guinea-Bissau, Malawi, Mozambique, Somalia, Tanzania.
307 World Economic Report, p.6.

well-being of an African.[308] Ignoring any statistics, Africa is still categorized as less developed with slow economic growth for lack of investment capital, researches and high debt burdens.

Technology Africa has experienced tremendous growth and ICT diffusion, innovation and penetration of technological devices in the last two decades.[309] More use of technology is embarked and encouraged as a strategy to deal with socio-economic challenges facing Africa. Technology is also used as means to cease opportunities that may benefit Africa. This is the reason for Africa-wide policy changes in the 1990s. The changes were instilled by development agencies including the Pan African Development Information System (PADIS) and international institutions such as the World Bank, IMF and UNESCO. African States were urged to adopt comprehensive national ICT policies as a strategy towards socio-economic development. Another instrumental motivation was the Maitland report of 1985 which warned of the missing link between telecommunications and development.[310] This resulted in a major ICT sector reforms, with adoption of an ICT policies, privatization and or liberalization of incumbent telecommunication companies in most of the African States.[311]

This gave rise of trade competition, increased innovation and growth of technology and hence evolution in the ICTs. This, however, does not imply that technology in Africa came in the 1990's. Mainframe computers were introduced in Africa in the 1960's. This was followed by mini computers in the 1980's. The mini computers came as part of global initiatives urging countries to contribute to central data banks so as to have access to cooperative information resources.[312] This is yet another reason which necessitated formulation of ICT policies in the 1990's. The acquisition, training, usage of computer database in both public and private sector increased massively, as a result adoption of ICT policies and regulation became necessary.

ICT is now used in Africa to accelerate economy, poverty reduction as well as improving governance and administration, and training in the education sector. Technology has, to a large extent enabled Africa to tap into advantages of technology in business and investment at the local and international level. Unfortunately, despite the growth in ICTs, overall sector performance is low compared to the global average. The only area that Africa has high growth is in the area of cellular penetration. Africa has performed well compared to the rest of the world.[313] The future of technology is also promising as investors worldwide view Africa as the future because African population is considered readily to engage with new technological-based tools to improve their life standards.

Africa is increasingly becoming a key player in acquiring, generating and applying technological knowledge to development challenges. It is also the fastest growing in mobile technologies

---

[308] Murphy, T., 'Why it's so difficult to measure progress and well-being in Africa', http://www.humanosphere.org/basics/2013/05/another-attempt-to-measure-well-being-in-africa/ Accessed on 17/07/2015.

[309] Borena, B et al., 'Information Privacy Protection Practices in Africa: A Review Through the Lens of Critical Social Theory', 48th Hawaii International Conference on System Sciences, 2015, pp.3490-3497 at p. 3491.

[310] ITU., 'The Missing Link', Report for the independent communications for World Wide Telecommunication Development, 1985.

[311] This is in exception to Ethiopia which is still in monopoly of communication sector.

[312] Stefano, K., 'Computer Diffusion in Black Africa: A Preliminary assessment' in Shubash, B and Bjorn-Anderson, N., (Eds), Information Technology in Developing Countries, Holland: Elsevier Science Publisher B.V, 1990.

[313] Borena, et al (n 309).

compared to the rest of the world. For instance, by 2012 there were 54 million Facebook users in Africa. Although, as Borena et al, argue, regulation and managing of the use of ICTs does not correspond to its innovation and development nor does it corresponds to monitoring and control the operation and usage of SNS. Despite the growth in usage, Africa is entirely dependent on imports of technology, innovations and platforms (SNS) from developed countries. There is also limited knowledge on the risks, effects and loopholes for abuse of privacy, cyber and related crimes that comes with the use of technology and the internet. As a result, there are growing incidences of misuse of technology, unauthorized sharing of confidential information, breaches of security and incorrect profiling.[314]

3.2 Conceptualizing Privacy

The concept privacy is hard to define (or even understand) with precision. The difficulty in having a precise definition is based on the fact that the concept is said to be elusive, transitory[315] and contextual;[316] it also means different thing to different people;[317] it is a concept which 'has [a] protean capacity to be all things to all lawyers.[318] Its meaning may vary and can be determined based on individual interaction with the society, culture and technology. Its character is also a question of debate; whether privacy is a state/condition, a claim or a right.[319] Nevertheless, it is important to understand and describe the interests that privacy is meant to protect; at least for jurisprudential reasons, in bringing legal certainty when the right to privacy is legislated and implemented. This can be done by identifying its scope, interests it protects and proper mechanisms for its regulation and implementation.

In Africa, the concept has been borrowed from Western jurisdictions where it is believed to have originated. Unfortunately, the borrowing came blindly without contextualizing it within the local settings. The African scholars also avoid the task of conceptualizing privacy; instead, they use the concept without any clarification on its applicability or propriety in the African context.[320] At this point, understanding privacy value is necessary for articulating, developing and applying its principles. It is also crucial in identifying necessary measures for its protection and for jurisprudential reasons.

Chapter one to this thesis illustrated an understanding of what privacy is. Simply put as a right to be left alone[321] or right to self-determination. However, simply saying '*right to be left alone'* does not

---

[314] Borena, et al (n 309).
[315] Neethling, J., 'The Concept of Privacy in South African Law', The South African Law Journal, 2005, Vol.122, No.1, pp.18-28.
[316] Cohen, J.L., 'What Privacy Is For' , Harvard Law Review, 2013, Vol.126, pp. 1904-1933.
[317] Neethling(n 315); See also *A R Miller The Assault on Privacy (Computers, Data Banks and Dossiers) (1971)* 25; *Bernstein & others v Bester & others NNO 1996 (2) SA 751 (CC) at 787–8*.
[318] Gerety, T., 'Redefining Privacy', Harvard Civil Rights-Civil Liberties Law Review, 1977, Vol. 12, No. 2, pp. 233-296, at p. 234.
[319] Bygrave (n 73), p. 169.
[320] Makulilo (n 26), p. 326.
[321] This approach to explain privacy receives many critics as being too vague and overly broad for the concept privacy. See Gavison, R., 'Privacy and the Limits of Law', Yale Law Journal, 1980, Vol.3, No.89, pp. 421-471 at p. 438; Hunt, D. L. C., 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for

say much about the right to privacy. It calls for questions such as one posed by Mark Hickford, 'left alone how and when? It gives possibility of extreme wide interpretations of situations which can be construed as entailing right to privacy but may fail to predict concrete outcomes and or when or how to intervene in one case but not another'[322] There is a danger of being interpreted to apply situation not intended to have been covered at the time of its conception.

Summarizing debates on the subject, Bygrave[323] came up with four principal ways of defining privacy. The first one is based on *non-interference*; second is based on *limited accessibility*, the third one is based on *information control* and the fourth links privacy to *intimate* or *sensitive* aspects of persons' life. This is not far from what EPIC and Privacy International suggests; that privacy safeguards four things; *personal information, bodily privacy, communications privacy* and *territorial privacy*.[324] This is similar to what legal scholars have come to agree as a form of protection for liberal self.[325] Better described by Neethling[326] as an ability of a person to determine his private facts and hence the scope of his interest in privacy; the power of self-determination which is the essence of person's privacy and therefore also of his right to privacy.

In the absence of universally agreed definition, it is, safe to say privacy gives the individual control over their private lives against intrusion, physical or otherwise.[327] The case of *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smith*[328] elaborated that 'private' does not refer only to an individual within his intimate space but also in social capacity in which people act. Also, according to the ruling in *Niemitz v Germany*[329] as well as in *Coeriel & Aurik v the Netherlands,*[330] [privacy protection] extends to persons' professional activities and certain activities done in public sphere.[331]

Neethling has made a plausible analysis in differentiating privacy and other personal rights often mistaken as infringement of privacy. Disturbance of person's peaceful life is one such instance. Neethling cites the case of *Pretorious v. Minister of Correctional Services*[332] as an example. In the case the Court ruled that broadcasting of radio programmes in prison cells is an infringement of 'right to acoustic privacy'. According to Judge Bertelsmann, acoustic privacy is a right of a person not to be invaded by any broadcast which the individual has not consented to be exposed to.[333]

Development for Canada's Fledgling Privacy Tort', Queens Law Journal, 2011, Vol.1, No. 37, pp. 167- 219 at pp. 180-181.

322 Hickford, M., 'A Conceptual Approach to Privacy', Miscellaneous Paper 19/ New Zealand Law Commission, October 2007, Wellington, New Zealand, p. 19-20.

323 Bygrave (n 73), p.70.

324 Electronic Privacy Information Centre and Privacy International, 'Overview of Privacy' in Privacy and Human Rights Report, 2006.

325 See e.g., Kuner, C., 'International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review, 2009, Vol.25, No.4, pp. 307-317 at 308.

326 Neethling (n 315).

327 See also Cuijpers, C., 'A Private Law Approach to Privacy: Mandatory Law Obliged?', SCRIPTed, 2007, Vol.4, No.4, pp.304-318, at p.312.

328 No. 2001 (1) SA 545 (CC) at 557.

329 Application No. 13710/88; 16th September 1992 at Para 29.

330 (1994) Comm 453/1991, Para 10.2, reported in, inter alia, (1994) 15 HRLJ, 422.

331 De Hert P. & Gutwirth S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., et al (Eds), Reinventing data protection?, Springer Science, Dordrecht, 2009, 3-44 at p. 15.

332 2004 (2) SA 658 (T).

333 Ibid, p.631.

Neethling's argument on the ruling is that, there was no real infringement of privacy since there was no acquaintance with personal facts contrary to the determination and the will of the person involved, but rather an infringement of sensory feelings; a physical sensation of inconvenience, discomfort, unpleasantness, tiredness, irritation or disgust generated through victim's senses.[334]

Daniel Solove is of a different opinion; he believes disturbing one's tranquillity or solitude invades ones privacy even though it does not involve acquaintance of personal information. He believes, as long as intrusion causes harm by interrupting people's attention and hence their activities, it amounts to a breach of personal privacy.[335]

Another misconception is identifying privacy with dignity. Narrating from South African experience, Neethling explains that, as long as to succeed in an action for invasion of privacy one must prove insult; it is a misjudgment of the right privacy. In reality, violation of privacy, insult may not be present at all. And privacy and dignity are independent interests of personality; although invasion of privacy may also affect personal dignity.[336]

Identity (defamation in other jurisdictions) is also misrepresented as a violation of personal privacy. Neethling explains that this is not an infringement of privacy since privacy is infringed only through acquaintance with or disclosure of true facts. Truthfulness is, therefore, an element of infringement of privacy. Hence, publicity which paints the plaintiff in a false light to public is infringement of identity but not infringement of privacy. Although infringement of privacy can be accompanied by infringement of identity, these two are separate personal interests.[337] Once again Solove has a contrary opinion to this. To Solove, dissemination of false or misleading information about a person amounts to an invasion of privacy. He calls it, information distortion.[338] As long as such information is tied to a certain person and affects how others perceive that person, allow others to judge his/her behavior and character, then this information harms one's privacy.

Arguably, there is logic in Solove's premises if one looks at data protection codes. Data subjects are given right to access, correct, update and request deletion. The logic behind this right is to make sure no misleading information about a person is processed. Misleading information affects personal privacy as much (or even more than) true information. Misleading information, if disclosed, has a potential to harm personality as it has an impact on how others perceive and judge one's character. Accordingly, privacy should, as Solove believes, be taken on harm oriented approach. However, I would slightly differ with Solove, invasion of privacy should only be when there is unauthorized acquaintance, process or storage of personal data not merely discomfort made to a person by other people who have neither access nor process his personal data. This harm should come from the value attached to personal information. Once used, there is a person who gains from its value at the expense of the other who gives up control of the information. This is why data subject has a right over whom and how others may benefit from his data; and how such data should reflect on his personality and character.

---

[334] Neethling (n 315), p.22.
[335] Solove, D., 'A Taxonomy of Privacy', University of Pennsylvania Law Review 2006, Vol. 154, No.3, pp. 477-560, at p. 477.
[336] Neethling, (n 315), p.23.
[337] Ibid, pp.23-24.
[338] Solove (n 335), p. 549.

In many cases, personal autonomy has also been viewed as an invasion of privacy. An example is when people are prohibited from doing certain things such as viewing or possessing pornography materials. This is justified on the ground that personal autonomy is related to the freedom of human self-determination which includes freedom to make decisions about one's private affairs. On the contrary, self-realization, as Neethling argues, does not involve an infringement of privacy since there is no acquaintance with private facts against the will and determination of the person involved.

In conclusion, Neethling revisits the American view; that right to privacy extends to patrimonial interests. To him, this is improper since privacy relates only to personal facts regarding a person in his condition of seclusion and not facts concerning immaterial properties such as invention, production process, trade secrets, book or creation of art. The objects may exist separately and independently of human personality. Therefore, it is incorrect to view an acquaintance with such immaterial property as an infringement of personality right of privacy.[339]

Neethling analysis narrates instances of misapplication of the right to privacy in South Africa for lack of jurisprudential understanding of the interest with which privacy is aimed at. His insistence on the subject is that privacy should be sought and defined by its existence and nature in factual reality.[340] As described by Hickford, privacy relates to 'those things or aspects of one's life that you, as an individual in social world, would have a reasonable expectation of exerting control over in terms of dissemination or disclosure should you wish to'. As further explained by Moreham;

> 'a person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about'. Something is therefore "private" if a person has a desire for privacy in relation to it: a place, event or activity will be "private" if a person wishes to be free from outside access when attending or undertaking it and information will be "private" if a person to whom it relates does not want people to know about it'.[341]

Based on Moreham view, privacy is viewed as a claim rather than a state or a condition of being. It is a claim a person has over his state of affairs, his information and his space which he considers private and intends it to be private. Basically, privacy is a claim of choice; one can choose elements and extent of publicity he desired about himself. Irwin Altman is of a similar view; he believes that privacy is a claim of choice which depends on one's ability to control interaction with others. To him, however, privacy regulation is a cultural pervasive process.[342]

Accordingly, privacy has two dimensions; informational privacy and local privacy.[343] Informational privacy comprises of all 'personal' information and facts about an individual; information which requires management in the social world. According to Hickford, the term

---

[339] Solove (n 335), p.26.
[340] Ibid, p.19.
[341] Moreham, N.A., 'Privacy in the Common Law: A Doctrinal and Theoretical Analysis', Law Quarterly Review, 2005, Vol. 4, No. 121, pp. 628-656, at p. 636.
[342] Altman, I., 'Privacy Regulation: Culturally Universal or Culturally Specific?', Journal of Social Issues, 1977, Vol. 33, No. 3, pp 66-84 at 68.
[343] Hickford, M., 'A Conceptual Approach to Privacy', Miscellaneous Law Reform Commission Paper no. 19, October 2007, Wellington, New Zealand, p. 6.

'personal information' should not be confused with 'private information' as information may be 'private' but not 'personal' at all.[344] And a person may have 'privacy' but not the 'right to privacy'. To have the right to privacy, 'there must be some valid norms that specifies that some personal information about, or experience of, individuals, should be kept out of other people's reach'.[345]

The local privacy is the privacy in one's space (control over access to oneself). Places inhabited by intimate relationships, places of solitude and those occupied/used in promotion of personal or professional growth such as in households, working places as well as in the public places. These two concepts, that is, informational privacy and local privacy, illustrates privacy as elaborated above by Lee Bygrave, EPIC and Privacy International and Neethling. It is also in line with provisions of Conventions on Protection of Right to Privacy such as Article 8 of the European Convention for the Protection of Human Rights and Freedoms and similar instruments.

Perhaps it is better at this point to look at privacy beyond abstract statements. And look at the elements of the right to privacy and instances or activities which invade privacy for abetter understanding of the concept. Invasion of privacy involves, at the first stage unauthorized access to personal information or premises. On the second stage, it involves unfair or illegal or unauthorized disclosure of information about a person or exposure to his/her person. The exposure includes personal information, images, grief or body in ways that allow others to form an opinion of his/her personality or character. The authenticity of information does not matter as long as such information is tied to a person and form basis of judgement upon his personality or character. There is also a disclosure of personal information obtained without authorization (illegal/unfair) or legally obtained but illegally or unfairly disseminated. This could happen if there is no knowledge or consent of the data subject or there is no legal basis for the processing of such personal data.

Invasion of privacy also happens when the collection is legal and fair, and dissemination is consented by a data subject or authorized by law, but dissemination went beyond the consented limits or the initial legal basis. This can happen when data is processed/shared to third parties without informing the data subject and obtain consent for the onward processing. It can also happen when personal data is processed to serve an unknown, unconsented aims and interests of others, what Solove refers to as data blackmail or appropriation.[346]

Interference with privacy can involve any of the activities mentioned above. It could be an unauthorized access to personal information or space, processing/dissemination of illegally/unfairly collected personal information or processing/dissemination of legally and fairly collected information without data subject's consent or legal authorization. It could also be the processing of personal data legally and fairly collected and with data subject's consent to processing but processed for secondary purposes, or to third parties without the knowledge or consent of the data subject; or processing of misleading and false information.

[344] Hickford, (n 343), p. 6.
[345] Ibid, p. 40.
[346] Solove (n 335), p. 549.

To avoid infringement of privacy, access to personal information or space must be allowed by the data subject or by law; and processing of personal data should be made upon informed consent of the data subject or on legal basis. The processing must be limited to the objects communicated and consented by the data subject or permitted by law. At all times, the data subject must be made aware of the context and circumstances from the point of access to the final process. This means privacy protection has two dimensions. It calls for cooperation between data controllers and data subjects in handling and usage of the personal data to avoid breach of privacy. Hence, on the one hand, data controller has a duty to inform and get consent from the data subject of all access and processing of data subject's data. On the other hand, the data subject has a right to know the kind of data held, purpose of processing and any secondary use of such data. The data subject has a right to access his/her personal information, rectify or update them in case of changed circumstances or errors. Data subject may also object to their processing all together.

To Irwin, purpose of privacy is to manage social interaction, establish plans and strategies for interaction with others and develop and maintain self-identity.[347] To borrow his word, he says;

> 'Privacy mechanisms define the limits and boundaries of the self. When the permeability of these boundaries is under the control of a person, a sense of individuality develops. But it is not the inclusion or exclusion of others that is vital to self-definition; it is the ability to regulate contact when desired. If I can control what is me and what is not me, if I can define what is me and not me, and if I can observe the limits and scope of my control, then I have taken major step toward understanding and defining what I am. Thus, privacy mechanisms serve to help me define me.[348]

However, because privacy is seen in the context of human interaction, socially and politically, a balance must be struck. Consequently, the right to privacy is not an absolute right. It operates on balance with other rights such as the right to information but also in line with other interests of a larger public. This is why most of the data privacy law exempts certain activities such as law enforcement, intelligence activities and other the public duties conducted by a public officer from the application of the law. In this aspect, Julie Cohen suggests that privacy should not be viewed as a right 'because the ability to have and manage it depends heavily on the attributes of one's social, material and informational environment'.[349] Since privacy goes beyond protection of an individual, it furthers fundamental public policy goals relating to liberal democratic citizenship, innovation and human flourishing. This is the reason privacy policy takes into account these purposes. Excessive regard to private life endangers civil liberties by leaving the body politic unattended.[350]

The right to privacy also overlaps with other fields of law and rights such as tort of defamation, right to liberty and trespass. This may explain the disassociation of privacy with other aspects of the law as narrated before; but again as Cohen argues, there is no single formulation of privacy

---

[347] Altman (n 342).
[348] Altman, I., The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Monterey, CA.: Brooks/Cole, 1975, p. 50.
[349] Cohen (n 316), pp. 19-20.
[350] Hickford (n 343), p. 35.

purpose, and neither is it a fixed condition as it changes with individual relationship, social and cultural context in boundary management.[351]

The evolving nature of privacy can also be seen in the change of terminology. In 1970's when privacy rights extended to the protection of personal data, scholars came up with a debate on the need to change the terminology to suit the changing circumstances. The use of terminology between 'privacy' and 'data protection' was examined. On the one hand, scholars argued that privacy has simultaneous existence and synonymous usage with data protection. Those arguing in this line based their arguments, first on the fact that privacy is used in the USA, Canada and Australia to refer to what is called data protection in European jurisdictions,[352] and secondly, the difficulty in drawing a line between the two concepts.[353] [354] With different view are those who believe that the idea that privacy and data protection is interchangeable. They argue privacy and data protection emerged from the central objective of the right to privacy, to protect against unjustified interference in personal life;[355] hence, they simply have a similar implication.[356]

The confusion led to the mutation of the two concepts giving rise to new concept 'data privacy'. According to Bygrave 'data privacy' is the best representative concept which also reconciles both sides to the controversy (the European and her counter parts USA, Canada and Australia) in policy discussions.[357] With this convergence, Makulilo argues that the two concepts are increasingly becoming synonymous and hence interchangeable in their use.[358] The same effect is observed by Kunner who believes this to be an effect of the movements towards an international framework for the protection of personal data and personal privacy.[359] As a result, whether a person uses the concept 'privacy' or 'data protection' or 'data privacy' it does not matter. What matters is the context in which the concepts are used; the principles (contents), scope and application of such principles.

However, for purposes of this thesis, the concept 'privacy' is preferred as opposed to data protection and data privacy. The use of the term 'data privacy' and 'data protection' may also be used in certain contexts to deliver the intended meaning without derogation. The reason is the fact that privacy is mostly understood in African context than the later concepts. Also, data protection reforms in Africa are still in their infant stage. Hence, terminologies such as data protection and data privacy are not of familiar usage to local communities. On the other hand, the concept privacy is well accustomed in the context of data protection and data privacy. The discussion debunks the concept privacy in African context in an effort to determine its value, perceptions and status within diverse African communities.

---

[351] Cohen(n 316), p. 7.
[352] Makulilo(n 26), p. 62, Bygrave (n 60), p. 1.
[353] See Kuner cited in Makulilo(n 26), footnote145 and Cuijpers in Makulilo(n 26), footnote 147.
[354] Despite the difficulty in drawing the line between the two concepts, academicians continue with the attempt to conceptualize them. Commentators like Christopher Kuner considers privacy as a broader concept upon which data protection emerged but believe the two concepts have overlapping objectives; others such as Cuijpers and De Hert considers data protection to have a broader application than privacy whose objective is to offer individuals control against intrusion of their private sphere whereas data protection goes beyond private sphere [Makulilo(n 26), footnotes 147 and 155]
[355] Makulilo (n 26), footnote 155 at p.4.
[356] Karanja cited in Makulilo (n 26), footnote 163.
[357] Bygrave (n 100), p. 321-322.
[358] See Makulilo (n 26), pp.73-74.
[359] Ibid, p.74.

3.3 Privacy Concept and Perception in the African Context

Privacy is understood more or less the same in different African communities. This is despite their diverging legal systems. Countries under Common Law system attribute same meaning to privacy as in the Western jurisdictions. African authors such as Makulilo believe this trait to result from the fact that the concept was imported from the Western, hence the borrowed meaning.[360] The most popular definition of privacy in African discourse is the one promulgated by Prof. Johann Neethling, believed to have originated from the USA. This definition was accepted by the Supreme Court in *Griswold v. Connecticut.*[361] It defined privacy as 'a condition which includes all personal facts which a person himself at a relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy'.[362] Its recognition in African goes beyond African literary works, Constitutional Court of South Africa has endorsed this meaning in *National Media Ltd v. Jooste.*[363]

Privacy concept receives a similar connotation in local African languages such as the Swahili language,[364] where privacy is known as '*faragha*'.[365] The same is defined in the Swahili dictionary as '*mahali pasipo wazi au pasipo watu; siri; upweke; mafichoni; kando; chemba';* translated into English as 'private sphere or in seclusion from people; secrecy; solitude; hidden; rim; closed'. In Francophone countries most of which are under Civil Law systems, uses the word *la intimité; le secret or la solitude*, to refer to privacy but as a right, it is referred to as *droit à la vie privée* (right to privacy)

In Islamic countries following *Shariah* law, the concept is *khususiat or alssrria* (خصوصية or السرية) which means privacy, confidentiality, or exclusiveness; it is also referred to as *eazila* (عزلة) which means isolation, seclusion, loneliness, desolation or solitude; also as *sirria* (سرية) which means confidentiality, secrecy, stealthiness, or wrap. Traditionally, this term had been to refer to a 'hidden military unit' using a secret convention in wild formations. However, as a right, privacy it is expressed as *Haqq al-xuSuuSiyya* (الخصوصية حق) According to the Quran (the Supreme Law) the right to privacy entails prohibition against spying, which according to verse 49:12, prohibits spying against one another and against intrusion to a private realm. The Quran on verse 24:27 continues, 'do not enter any houses except your own homes and unless you are sure of their occupants' consent'.[366] This prohibition warns further that, owners of houses not to enter their own houses through a back door or in sneakily manner.

From the above narration, privacy in African societies carries similar values and objectives as in the Western. However, its status and enforcement differ highly based on political stance and legal culture. Giving such example of diverse meanings of the concept privacy is Abdul Raman Saad who explains it with reference to the Islamic community. Saad compares the concept as

---

360 Makulilo(n 26), p. 326.
361 381 U.S. 479 [1965].
362 Neethling, J et al., Neethling's Law of Personality, Butterworth, Durban, 1996, p.36; Neethling (n 337), p.19.
363 [1996] 3 SA 262(A) 271.
364 Swahili is a Bantu language with a largest number of speakers in Africa.
365 Literally translated in English as 'privacy'.
366 The Quran even clarified the consent to the effect that even when one is invited to a house, one shall not overstay the invitation or act contrary to the scope of invitation. For example if invited to a feast, invitee should not do more than feasting and after the feast, invitee must exit the house as the purpose for the invitation is executed.

perceived in Islamic communities as against the Western perception. In Islamic communities, privacy is aimed at prohibiting public humiliation of the individual even if it is something of legitimate concern to the public. This is different from the Western objectives of privacy which would seem to allow publication of information of a person's private life or information if there is a legitimate public concern.[367]

Saad argues that, even without the existence of law, privacy is a concept recognized in various cultures, but depending on a cultural setting, each society has its own attitude and perception towards what amounts to privacy. In illustrating this, the author proceeds with a comparative analysis of privacy perceptions among the Germans, Americans, French and English. He says ...'the Germans marked of their private *Lebensraum* by closed doors, fences, and strict rules about trespass. German law, for instance, forbids the photographing of strangers in public places without their consent. Americans have open doors and no fences, but mark their social status with 'private' offices and 'private' secretaries. The French pack closely together in public, but rarely invite outsiders to their homes, even if they know them well. And the English, it seems to rely mainly on their reserve: when an Englishman stops talking, that is a signal that he wishes to be left alone'[368]

Human rights and individual liberties are argued to have existed in Africa long before colonization.[369] Of course, these principles were not in a written form hence no documentary evidence can be produced to this effect. Granted, Fremount speaks of the existence of at least one of the adoption of a written document enshrining these rights in Africa. He says, there was, in 1236, an adoption in *Kouroukan Fuga* (Kanbaga, Mali) of a Charter containing human rights. He cites the provisions of the Charter, articles 5 and 9 as stating;

> '[e]veryone is entitled to life and to the preservation of their physical integrity. Therefore, any attempt to deprive someone from his life is punished by death penalty'. Article 9 '[c]hildren's education is the responsibility of the whole society. Paternal authority is therefore exercised by all'.[370] Communities embraced and were tolerant of each other's rights and liberty as they co-existed. According to Keba Mbaye the fact that many traditional African religions co-existed also suggests the African acknowledgment and respect to human rights and liberties. He continues, 'many liberties co-existed….liberty of association, freedom of expression, the right to participate in affairs of the state and freedom of circulation. These rights were not conceived and experienced in terms of conflicts; rather, in terms of group rights and also of responsibilities.'[371]

These rights and liberty were in the form of duties to others and the society.

The right to privacy was not among the rights or liberties recognized. This is because Africans believe in the community than individuality. However, the right was later adopted within bills of

---

[367] Saad, A. R., 'Information Privacy and Data Protection: A Proposed Model for the Kingdom of Saudi Arabia', Abdul Raman Saad & Associates, Malaysia, 1981 p.5.
[368] Ibid.
[369] Frémont, J., 'Legal Pluralism, Customary Law and Human Rights in Francophone African Countries' Victoria University of Wellington Law Review, 2009, Vol.40, No.1, pp. 149-166, at p. 159.
[370] Ibid.
[371] Mbaye, K., Les Droits de l'Homme en Afrique (Second Edition) Pedone, 2002, pp. 71-73.

rights in independent Constitutions. The adoption of the right carries another story. In this regard, Frémont says 'each country has a different story to tell. For some countries, bills of rights were imposed by colonial powers before surrendering jurisdiction; for others, some time has had to pass after independence. What appears to be clear is that the presence of cultural factors explains their rapid emergence or not as does, among other things, the local legal environment. In almost all cases, mixed legal systems were in place (influenced by the Dutch, British, French, or Belgians) and superimposed on the tribal (or traditional) legal foundations.'[372]

In 1981 Africa as a Region adopted the African Charter on Human and Peoples' Rights. The Charter did not define what 'people' means but provided for all the rights under the UDHR except the right to privacy and the right against forced labour or compulsory labour. In relation to the right to privacy, it can only be assumed that the omission is based on the nature of the right, which, if granted may paralyze the whole idea of the Charter, i.e. promotion of communal values and African cultural norms, in this case, communalism *vis a vis* individualism. In fact, Evelyne Ankumah notes that one of the most notable and probably the most serious shortcoming of the Charter is the incomplete and imprecise formulation of guaranteed rights. As a result, the Charter offers little legal protection to an individual.[373]

African legal systems and legal culture are diverse based on the difference in languages, anthropology, religion and culture.[374] These aspects have also, to some extent been manipulated by colonialism. As a result, most African countries have pluralism legal systems, with customary African traditional legal systems,[375] mixed with a foreign legal system, (either Common law, Civil law, Roman-dutch or Islamic law).[376] Africa has profound cultural values which may affect how privacy is received, perceived and valued. The dominant is the sense of community which overrides the sense of individualism. An African idea of security and its value depends on personal identification with and within the community. This aspect has been a subject of scholarly debate in the privacy arena. Oliver Onwubiko, for example, explains this scenario as follows;

> 'Communalism in Africa is a system that is both supersensible and material in its terms of reference. Both are found in a society that is believed by the Africans to be originally 'God-made' because it transcends the people who live in it now, and it is 'man-made' because it cannot be culturally understood independent of those who live in it now…This community also, within this transcendental term of reference (God-made) becomes the custodian of the individual's ideas'.[377]

In Africa, the community, therefore, offers an individual psychological and ultimately security as it gives its members both physical and ideological identity. The aim is to produce and present an

---

[372] Frémont (n 369).
[373] Ankumah, E. L., La Commission africaine des droits de l'homme et des peuples. Pratiques et procédures, Londres, SADIC, 1995. p. 189.
[374] Baldelli, F., 'Legal Origins, Legal Institutions and Poverty in Sub-Saharan Africa', Master's Degree Thesis, LUISS Guido Carli University, 2009/2010, p.13.
[375] Onyango, P., African Customary Law: An Introduction, LawAfrica, Kenya, 2013.
[376] Baldelli (n 376), p.20. The author continues arguing that 'although colonialism shaped African legal system through legal transplants, erasing large part of customary law, African traditional law continues to persist even after colonialism. Twenty-seven countries in Sub-Saharan Africa have a legal system with French civil law influence; sixteen have a British common law system, two have a bi- juridical law system and one, Sudan, applies the Sharia.
[377] Onwubiko, O. A., African Thought, Religion & Culture, Enugu, SNAAP, 1991, p. 14.

individual as a community-culture-bearer. Since culture is a community property, it must be protected by the community.[378] Individualism or individual identity cannot take precedence over community identity. Thus individualism as an ideology and principle of life is not encouraged in Africa, even though it is not destroyed.[379] This is in contrast with the superstructure of the Western world which as Shahadah illustrates, 'elevates individual over the society and therefore enshrines an ethic of one against others in a situation of existential tension. All institutions of the West predicate their existence on the assertion of an individual as unique even without the group.

On African side, communalism is a moral foundation of African culture hence things incompatible with peoplehood are therefore generally incompatible with African values'.[380] As a result, individuals can only have rights by virtue of obligation they fulfil to the community. Davidson elaborates in these terms; '[The African] logic regarding legality in terms of individual obligations, not individual rights. At least in jural and moral assumptions, communities live at an opposite extreme from the "free enterprise individualism" which supposes that the community has rights only by virtue of the obligations it fulfils to the individual'.[381] Hence, unwillingness to share with people one's private or even public matters can be interpreted as bad manners or a sign of enmity. Putting this in a single sentence, Posner posits, privacy is therefore considered as a right of the deceivers to conceal shameful facts about themselves'. People are expected to discuss their issues freely and look for communal opinion or solution to one's problem/issues.[382] It follows then, terms like 'intimacy' in African context are not exclusive for particular friends but applying to a whole group of people who find themselves together through work or residential requirements.[383]

Optimist Shahadah believes, as much as culture drifts on the open ocean of interaction, technological development, pushed on by the winds of globalization, African culture changes. He believes, there is no longer such a thing as African monolithic purity cultures; but explains further that, the shifting dynamics of culture does not mean an alteration in the fundamental principles of the culture. And distinction must be made between practices of the people and their cultural ideal, what he calls 'the superego of the culture'. He gives an example of the rise of sexual immorality in African communities as a reality but explains that this does not mean immoralities are an aspect of culture; because these trends are not desirable and are not encouraged; they go against the superego of the cultural ideal. It means the ethics of the said culture remains static. And that one basic fact is that African cultures are communal as opposed to 'individualistic' and this one difference creates an entirely different paradigm and behaviors.

---

[378] Onipede, K.J and Phillips, O.F., Cultural Values: Index for Peace and Branding Africa, Ladoke Akintola University of Technology, Nigeria, p. 5.

[379] Olasunkanmi, A., 'Liberalism Versus Communal Values in Africa: A Philosophical Duel', IOSR Journal of Humanities and Social Science, 2013, Vol.12, No.5, pp.78-81, at p.80.

[380] Shahadah, A., 'African Culture Complex', http://www.africanholocaust.net/africanculture.html Accessed 12/03/2015.

[381] Davidson, B., The African Genius, Boston, 1969, p. 57.

[382] See Matondo, M.J., 'Cross-Cultural Values Comparison between Chinese and Sub-Saharan Africans', International Journal of Business and Social Science, 2012, Vol. 3, No. 11, pp. 38-45, at p. 40.

[383] Biko, S., I write what I like, New York, 1978, p. 41.

These cultural laws are about boundary-maintenance, which fundamentally inform notions of morality that in turn inform legislation and national hood.[384]

In Africa, culture is not only the people, their practices and beliefs; it's the whole process from legal, family to the political level. It instructs life with values and habits which service humanity and has a role in personal continuation. So, Africa identity is not one hard thing but a multitude of self-impose conditions which ideologically run fluidly across indigenous Africa; it is not a scientific observation but a cultural-political one.[385]

South Africa is the best illustration in this; it has both the Constitutional and Common Law right to privacy and statutory data privacy law. South Africa is also a country which has been judicially active in the area of privacy law more than any other African country. Both Common Law and statutory law define privacy as part of an individual's personhood. However, the Ubuntu philosophy[386]has influenced the conception of personhood within South African context. Consequently, because of Ubuntu, personhood is not determined by a person himself as in the Western jurisdictions but is also determined by others (community).[387] This is a departure from the Western culture with individualistic personhood conception and understanding of privacy. Africa has communalistic approach to personhood which represent rights and duties to a legal person.

With this argument, it means illumination of legal practices should be contextual, at least in Africa with its peculiar environment. Nicola Lacey explains the importance of contextualizing law and legal practices saying; 'legal practices lie not merely in an analysis of doctrinal language but in a historical and social studies of the institutions and power relations within which that usage takes place;[388] more so, with privacy, a concept which is hard to define, highly contextual, and with ever-changing values. Collin Bennett says, privacy is highly subjective, which means it varies by time, jurisdiction, ethnic group and gender. To have an acceptable privacy legal framework, individual concerned should be the one defining the contents and interests in privacy according to the context.[389] According to Neethling, to be able to conceptualize and regulate privacy, an understanding of personality interests in the pre-legal existence in factual reality is important. He argues that, by 'nature a person has a fundamental interest in particular facets of his personality (such as his body, good name, privacy, dignity et cetera), these interests exist autonomously de fact, independently of their formal recognition de jure.

In Africa, one major attribute is communalistic society. It pre-exists as a condition that determines attitude, practices and the value of the right to privacy has or can take. This alters the

---

[384] Shahadah (n 380).
[385] Shahadah (n 380).
[386] Ubuntu has been defined differently by scholars (e.g. Archbishop Desmond Tutu, Louw, Mokgoro, Mbigi, etc,). However to put it in simple terms, the concept Ubuntu refers to African philosophy which emphasises collectivist human relationship and assistance in everyday life. In Ubuntu, an individual is subjected under communal considerations. The concept is well developed in South African scholarship though it has its reflection in other African societies.
[387] Borena, et al (n 309), supra, p. 3494.
[388] Lacey, N., *A Life of H. L. A. Hart: The Nightmare and the Noble Dream,* Oxford University Press, Oxford, 2006, p. 219.
[389] Bennett, C., 'Information Policy and Information Privacy: International Arenas for Governance' Journal of Law, Technology and Policy, 2002, pp 385-406 at p. 389.

original concept of privacy as understood in the Western discourse and as borrowed in Africa. If we follow Neethling argument, that laws do not create new interests rather protects recognized pre- existing interests to promote justice, then it is prudent to understand the value, practices and interests in privacy in African context before any legal reform can take place. It is important because as Irwin emphasizes;

'Privacy regulation may be culturally unique in terms of particular behaviors and psychological mechanisms used to regulate it. Thus while capability for privacy regulation may be culturally universal, the specific behaviors and techniques used to control interaction may be quite different from culture to culture'.[390]

In the same premises Neethling opined that if the jurisprudential concept of privacy is in conflict with its nature *de facto*, it cannot be considered to be a scientific concept. That the legal principles based on an inaccurate understanding of factual reality will necessarily lead to uncertainty and contradictions and consequently, may produce unfair results.[391]

3.4 African Customary Legal System

The African customary 'legal' system has, like other modern systems, established jurisprudence with law enforcers and pre-prescribed sanctions. Unlike the modern systems, it lacks written codes but has a central focus on upholding cultural values and socially accepted norms. Jacques Frémont,[392] believes that the African customary legal system 'is a convergence of law as advanced by Hugo Grotius (moral principle/morality of law), John Finnis (natural law theory, i.e man's ability to gasp values directly) and the 'command' aspect from John Austin's theory.' Frémont beliefs are built from the idea that, this system is, unlike the modern law, not taught in schools and cannot be found in a written code, but its exists through man's comprehension and observation of community moral, values and practices which if not observed commands a punishment. The teachings and the main sources of the African law are songs, pithy sayings, proverbs and maxims.

The main objective of this system is to bring the community together. Therefore, the system primary aim in conflict resolution is geared towards understanding between parties and resolution of the dispute. The primary objective is not to punish a wrongdoer. It is a system which does not encourage winning or losing. Unlike the modern systems where winner wins all and loser loses all, the African customary system is guided by the principle of 'win a little - lose a little'. It is a system of compromise between parties to a conflict. In a modern world, we would say it is similar to the alternative dispute resolution system (ADR). This is not to say that there is no punishment; where necessary punishments are imposed in extreme cases such as murder. In such cases, the wrongdoer is banished from the community and s/he is never to return to the community.

---

[390] Altman (n 342), pp. 68-69.
[391] Neethling, J., Persoonlikheidsreg, Butterworth, Durban, 1979, p. 30.
[392] Frémont (n 369), p. 151.

The ultimate goal of the system is, as elaborated by Frémont to pull the society together;[393] not to create divisions by pronouncing a winner or a looser in a conflict but rather resolve the dispute in an amicable way. To achieve this aim, the conflict resolution process as described by Olaoba involves a demonstration of the culture in its radiant splendor and flame. 'This was why in pre-colonial African societies, peace and harmony somehow reigned supreme and often produced unique atmosphere for peace to thrive and development became dynamic.' Olaoba continues that some of the features includes 'performance stance ….. demonstration of the customs and norms, deification of the ethnical framework of the society and the trust of conflict resolution throughout the society thus creating conducive environment for the facilitation of peace and the enhancement of harmony. The process was anchored in dramatization of issues involved in a conflict;'[394] popularly known as 'drumming the scandal'. According to the author, the dramatization of the conflict has a purpose of allowing participants in the drama to get an in-depth understanding of the customs and norms bequeathed to them by their ancestors and criticize the wrong acts.[395] To be able to get a clearer picture of the process I would borrow Olaoba's illustration as follows;

> 'The dramaturgical device always involved a systematic radiation of all sides (scenes) to the conflict (drama). In a sense, the party to the conflict (litigants) normally resorted to adopting flashback (mnemonic memory) with a recitation model. The asides to the conflict were stage-managed by the witnesses who adequately provided the knots of denouement for the responding schemes of the adjudicators at all level of statecraft. The level of performance by the adjudicators is triangular, focusing or viewing the parties to the conflict, witnesses (two parties) and the audience (large crowed). Interestingly, the adjudicators must not only third and enthrall the audience so as to boost their morale in the interpretive analysis of conflict resolution tradition, they also had to ginger other dramatic personae on the stage to comply with dramaturgical devices.'[396]

Basically, the system used community cultural norms, traditions and values to regulate the community. As further explained by Frémon 'customary law calls for respect of social order in achieving group harmony which is un-derogated values and are preserved at all costs as they play a major role in the establishment of behavioral norms, which are usually very constraining. For all purposes, they organise the life of the family, the clan and the village. The translation of such solidarities, ideally, should be found in legal norms.'[397]

The conciliation process takes place in a public place; there are specialized institutions for conflict resolution such as Courts and Tribunals. They involve Chiefs, experienced elders or kings who can be said to represent the modern day judges or umpires. However, different from the judges and umpires, the Chiefs, experienced elders and kings had a different role; their role is not of a judge or umpire, they are the performers of the drama in demonstrating the customs and norms of the specific community. They are not the ones deciding the case between the litigants; rather the decision comes by a conciliatory process by the community. This involves the two communities from where the conflicting parties come from. The two communities would

[393] Ibid.
[394] Olaoba, O.B., African Traditional Methods of Conflict Resolution, NOUN, 2010. p. 7.
[395] Ibid, p. 8.
[396] Ibid.
[397] Ibid.

help in the reconciliation process and ultimately the litigants are left to resolve their conflict through a dialogue. Hence the decision is made in what Frémon terms as collegiality.[398] Litigants are also allowed to be represented by an orator or a sorcerer. The resolution would usually reflect principles of customary law as dramatized by the chief, an elder or a king during the process; the ultimate goal is harmony between communities and hence the conflicting parties.

This process involves sacrifices and fair compensation from the faulty party.[399]Once the reconciliation is reached, the drama would change its theme to a celebration mode. The reconciliation is celebrated and the parties and characters would dance celebrating 'wining a little and losing a little.' This marks the closure of the conflict and the hearing.

3.5 Conclusion

The previous chapter narrated the history in the enforcement of the right to privacy and the pre-existing understanding of the legal concept affects the nature of the law as well as its enforcement and interpretation. In Africa, different communities have defined what privacy is. However, the concept has never been legally defined or clarified within the African context. Furthermore, among the 54 African States, only two (Kenya and South Africa) have judicially enforced the right to privacy. The two countries enforced the constitutional right to privacy under tortious principles on personality rights. Eventually, even with its enforcement, privacy as a right on its own has never been given a meaning. With this history, it is worrisome whether the reforms in data protection and enforcement of personal privacy and data security can be objective and sufficient to the cause.

The African traditional justice system is very different from the modern justice system. This is both in terms of process, the relation between parties and the materials involved. From African perspective of justice, the modern justice system would seem complex and social unfriendly as it does not support the idea of social unification and harmony between parties instead it is founded on enmity between parties. Moreover, the rules are foreign in term of process and context. The modern justice system is further seemingly to have a monolithic approach while the traditional approach is a holistic approach. African justice system along with resolute the dispute aims at sustaining harmony and social unity while the modern system is considered to be opposite. The reforms in data protection in Africa have mainly adopted the EU data protection framework. Unfortunately, among the reformed systems, none have their data protection authorities harmonized to reflect pluralistic nature of African legal systems. It is also not clear whether the non-inclusion of the other existing legal systems within the enforcement authority may, in the long run, adversely affect the implementation of the laws.

[398] Ibid.
[399] Frémont (n 369), p. 154.

4. Privacy Regulations and Institutions in Africa

4.1 Introduction

Privacy is a human right issue. Therefore an understanding of the African human rights architecture, from Regional, Sub-regional to the national level is crucial in the understanding African privacy regimes. Review of the institutional layout and judicial trend on human rights protection as well as adjudication in general can help to sketch a picture on the status, value and the future of privacy and data protection in Africa. Through this chapter, the weaknesses and strength of the African human rights enforcement systems and privacy regimes are explored.

4.2 The African Union Human Rights and Privacy Protection Framework

The African Union (AU) was established in 2002, replacing the Organization of African Unity (OAU) after the African Heads of States adopted the Constitutive Act of the AU in Lome, Togo.[400] The Constitutive Act expresses the main objective of the AU as to strengthen human rights situation in Africa. This is the strongest point of departure from the OAU. The AU eliminated the principle of non-interference in international affairs and brought about an intervention approach to cases of conflicts, unconstitutional changes of governments and human rights abuses.[401] [402] The AU also vows to promote democratic principles and institutions, including people participatory and good governance.[403] In promotion of human rights, the AU undertakes to protect human and people's rights as accorded by the African Charter and other human rights instruments.[404] In doing so, the AU promises transparency by allowing people participation in the AU activities.[405] Unlike its predecessor, the AU has the power to impose sanctions on members who fails or refuses to comply with policies or decisions of the AU.

The AU through its institutions, specifically the Pan-African Parliament and the Peace and Security Council objectives are to "promote the principles of human rights and democracy in Africa" and to "encourage good governance, transparency and accountability in Member States",[406] "promote and encourage democratic practices, good governance and the rule of law, protect human rights and fundamental freedoms, respect for the sanctity of human life and international humanitarian law, as part of efforts for preventing conflicts".[407] In doing so, the AU makes specific reference to principles enshrined in the UDHR on fundamental human rights and

---

[400] The 36th Ordinary Session of the Assembly of Heads of State and Government. The Act entered into force on 26 May, 2001.
[401] Akokpari, J., 'Human Rights Actors and Institutions in Africa in Africa's Human Rights Architecture', Akokpari, J and Zimbler, D.S(Eds), Cape Town, 2008, p.7.
[402] Under article 4 (h) (i) (j) of the Constitutive Act 2000, the AU can intervene, upon a decision of the Assembly, in cases of war crimes, genocide and crimes against humanity; member states have the right to live in peace and security and they can request intervention from the AU in order to restore such.
[403] AU Constitutive Act, Article 3 (g).
[404] AU Constitutive Act, Article 3 (h).
[405] AU Constitutive Act, Article 4 (c).
[406] Protocol to the Treaty establishing EAC relating to Pan African Parliament, Annex I, Articles 3(2) and (3).
[407] AU Protocol establishing Peace and Security Council, Article 3(f).

freedoms and the sanctity of human life.[408] Furthermore, through the Political Affairs Department, advocacy policies are developed. Within this department, co-operation between AU members, CSOs and RECs on human rights issues are promoted.

4.2.1 Framework for Human Rights Enforcement

The African human rights system is solely based on the African Charter on Human and People's Rights (Banjul Charter) and its protocols. Through the Charter, two organs are established; the Commission and the Court. The system is more or less replication of the European system. The Banjul Charter[409] is the Regional human rights instrument guaranteeing all the rights provided and protected by international human rights instruments such as the UDHR, except for the right to privacy and right against force or compulsory labor. The Charter, unlike the UDHR, European and American human rights protection systems, has included civil, political and socio-economic rights in this single document. The AU believes, the exercise of these rights is complementary and therefore need not be separated. Accordingly, the Preamble to the Charter states; 'States parties have stated their conviction that civil and political rights cannot be dissociated from economic, social and cultural rights in their conception as well as universality and that the satisfaction of these latter rights is a guarantee for the enjoyment of the formers.'[410]

The Charter is 'unique' of human rights instruments. It emphasizes the importance of historical and values of African civilization in protection and enforcement of human rights. Consequently, enforcement of human and people's rights in African continent must conform to this. The preamble to the Charter explains the implementation of human rights in Africa as an inevitable correspondence to duties; and that there should be a link between civil and political rights against the existence of socio-economic and cultural rights. Hence, beyond the usual human rights protection and guarantees, the Charter provides additional individual duties to address the peculiar nature of African communities and culture. It imposes a duty of an individual to the family, the nation and to the international community.[411] There is also a duty to preserve African cultural values and the commitment to achieve African unity.

The preamble states;

> 'Considering that the enjoyment of the rights and freedoms also implies the performance of duties on the part of everyone;[412]
>
> Convinced that it is henceforth essential to pay particular attention to the right to development and that civil and political rights cannot be disassociated from economic, social and cultural rights in their conception as well as universality and that the

[408] AU Protocol establishing Peace and Security Council, Article 4.
[409] It was adopted in Nairobi-Kenya on the 27th of June 1981 and entered into force on 21st of October 1986, OAU Doc CAB/LEG/67/3 Rev 5 (1981).
[410] ACHPR, Para 5 to the Preamble.
[411] ACHPR, Article 27.
[412] ACHPR, Chapter II defines individual duties to include duties towards family, society and state. Further duties extend to legally recognized communities and international community.

satisfaction of economic, social and cultural rights is a guarantee for the enjoyment of civil and political rights.

Taking into consideration the virtues of their historical tradition and the values of African civilization which should inspire and characterize their reflection on the concept of human and peoples' rights'

The Charter has designated 'family' as a custodian of moral and traditional values and obliges states to see to it that family is supported as a unit and basis of a community. Article 18 states:

'State shall have the duty to assist the family which is the custodian of moral and traditional values of recognized by the community.'

Moreover, Article 17 (3) of the Charter further insists on states' duty in the promotion and protection of morals and traditional values as recognized by the community. In all aspects, the central theme of the charter is *'solidarity'* established under Article 29.

4.2.1.1 The African Commission on Human and People's Rights

The African Commission on Human and Peoples' Rights (ACHPR) was established by article 30 of the Banjul Charter. The Commission is an overseer of the compliance to the AU human rights instruments by the Member States. The Commission commenced its operations in 1987 as a quasi-judicial organ tasked with the interpretation and application of the Charter, Protocols and Human rights instruments ratified by the AU Member States.[413] All complaints on alleged violation of the Charter from an individual, a groups of individuals, NGOs and all African States, with exception to South Sudan which has not yet ratified the Charter, can be lodged with the Commission.[414]

The ACHPR holds two ordinary sessions a year. It can also hold an extraordinary session on the request of the Chairperson of the Commission or a majority of Commissioners. During the bi-annual ordinary sessions, the ACHPR considers periodic reports submitted by State parties, as well as reports from members of the Commission and its Special Mechanisms.[415] It is worth mentioning that, within the AU, there is also another self-standing body in the enforcement of human rights; the Committee of Experts on the Rights and Welfare of the Child. The Committee has the same mandate as the ACHPR except its mandate is limited to the implementation of the African Charter on the Rights and Welfare of the Child (ACRWC)[416] promoting, protecting and monitoring human rights relating to children.

Unlike the Banjul Charter, the ACRWC has, under Article 10 provided for the right to privacy. Also of importance is to know that, these two organs have no formal link, they operate independently of each other. African Commission on Human and Peoples' Rights has pursued a

[413] See, ACHPR, Article 45 and Protocol to ACHPR on the Rights of Women in Africa, Articles 26 (1) and 32.
[414] ACHPR, Article 47.
[415] Rapporteurs, committees and working groups.
[416] OAU Doc. CAB/LEG/24.9/49 (1990), entered into force Nov. 29, 1999.

more independent path from the AU. A pertinent example is the establishment of the headquarters of this Commission in Banjul, The Gambia, while the African Committee headquarters are based at the AU headquarters in Addis Ababa, Ethiopia.

In implementing the Charter, the Commission disregards the African states' legal systems, i.e. whether a monist or dualist state. The Commission regards the Charter to be binding to all AU Member States regardless of their systems or whether or not they have implemented legal measures to affect the Charter.[417] Accordingly, the Commission explained in *Civil Liberties Organization v Nigeria*,[418] that, if a Member State wishes to rescind its obligation under the Charter it must undergo an international process involving notice and not through a domestic procedure.[419]

Access to the Commission can be by a State party against another State party in violation of the Charter; by an individual or NGOs on their behalf or on behalf of others.[420] A Complainant can institute a communication (complaint) to the secretary general, the Chairman of the Commission and the concerned State Party. These communications are required to be confidential until such time as the Assembly of Heads of States and Government decides otherwise.[421]

Communications to the Commission can only be admissible when the local remedies have been exhausted and as long as the Complainant has not approached any other international jurisdiction.[422]However, Article 58 (1) to the Charter provides for exceptions to the rule. It allows the Commission to admit communications in the absence of 'exhaustion of local remedies' by an Applicant. Basically, the exception stipulates circumstances where there is difficulty or impossibility to exhaust local remedies and on cases that reveal the existence of a massive and serious violation of human and peoples' rights. In *Rencontre Africaine pour la De´fense des Droits de l'Homme v Zambia*[423] the Commission stated that it would be unreasonable to force Complainants to exhaust local remedies when such remedies, as a practical matter, are unavailable or ineffective. Accordingly, in *Nationale des Droits de l'Homme et des Liberte´s v Tchad*[424] the Commission admitted a communication which had not exhausted local remedies because it was of the opinion that it was impractical for the Complainants to get proper remedies in the local jurisdiction. The case involved a number of individuals with varied scope of the alleged violation. In admitting the case, the Commission stated that 'it can absolutely not demand the requirement of exhaustion of local remedies to cases in which the Complainant is unable to apply local Courts for every individual Complainant.'[425] The exception to the rule also applies when a Complainant,

---

[417] 129/94 Civil Liberties Organization v Nigeria, 9th Annual Activity Report [in Compilation of Decisions of the African Commission on Human and Peoples' Rights 1994–2001, IHRDA, Banjul 2002, pp.203–206].
[418] The 9th Annual Activity Report [in Compilation of Decisions of the African Commission on Human and Peoples' Rights 1994–2001, IHRDA, Banjul 2002, pp.203–206 at Para. 13.
[419] Keetharuth, S. B., 'Major African Legal Instruments', in Bösl, A and Diescho, J(Eds), Human Rights in Africa: Legal Perspectives on their Protection and Promotion, Macmillan Education, Namibia, Windhoek, 2009, p. 168.
[420] ACHPR, Article 55.
[421] ACHPR, Article 59.
[422] ACHPR, Article 56.
[423] (2000) AHRLR 321 (ACHPR 1996).
[424] RADH 2000 343 (CADHP 1995).
[425] Ibid, Para 30.

in fear of his life flees the country and therefore s/he cannot approach the local Courts;[426] the Complainant is dead,[427]or the Complainant cannot get legal representation in his/her country.[428]

The Commission, although possessing adjudicative powers, lack enforcement powers. The decisions rendered by the Commission are not 'judicial' decisions, are mere recommendations. As a result, not only the States but also the AU Assembly of Heads of States and Governments has been ignoring its recommendations. Christopher Mbazira[429] gives examples of such instance. This is when the Nigeria government executed Ken Saro-Wiwa in spite of a *note verbale* from the Commission that the execution should be halted until the case has been heard by the Commission. Also, the execution of Mariette Bosch by Botswana authorities four days after the Commission communicated its appeal for a stay. The Commission having no enforcement powers could not demand compliance. Church, Schulze and Strydom believe the Banjul Charter and the Commission have been built in the philosophy of negotiation and conciliation rather than the adversarial approach associated with adjudicatory mechanisms[430] hence the lack of enforcement powers by the Commission.

One positive aspect of the Commission is the room for individual participation. The Commission can, under Article 46 of the Charter, admit any individual with information or knowledge capable of enlightening the Commission on the subject matter of the case. Furthermore, rules 72, 76-77 of the Commission's rules of procedure allows the Commission to invite any person or NGO with knowledge on the subject matter of the case to participate in its deliberations. Of course, an individual or NGO participating in the deliberation will have the voting power.

The Commission can also embark into special tasks as an observer of rights. This can happen by request of the African Heads of State and Government by virtue of Article 45 (4) of the Charter. The Commission can also deal with violations in the absence of country, individual or NGOs' submission. By virtue of article 48, the Commission can launch an investigation against any AU member. This power enables the Commission to implement measures against violation or potential violation of human and peoples' rights.

4.2.1.2 The African Court on Human and Peoples Rights

The African Court on Human and Peoples Rights (AfCHPR) was established in 2006 through Article 1 of the Protocol to the Banjul Charter on the establishment of a Human Rights and People's Court. The Court is the Regional human rights tribunal with an advisory and contentious jurisdiction concerning the interpretation and application of the Banjul Charter. The Protocol establishing the Court states that the Court is established to complement the

[426] *Abobakar v. Ghana* (2000) AHRLR 124; ACHPR (1996).
[427] Forum of Conscience v Sierra Leone (2000) AHRLR 293; ACHPR (2000).
[428] Civil Liberties Organisation and Others v Nigeria (2001) AHRLR 75; ACHPR (2001).
[429] Mbazira, C., 'Enforcing the economic, social and cultural rights in the African Charter on Human and Peoples' Rights: Twenty years of redundancy, progression and significant strides', African Human Rights Law Journal, 2006, Vol.6, N.2, pp. 333-357 at p.346.
[430] Church, J et al., Human Rights from a Comparative and International Law Perspective, UNISA Press, 2007; p.259.

Commission. Presumably to 'reinforce and to complete the objectives of the Charter. This suggests, both the Court and the Commission coexist as independent bodies but within a mutually reinforcing relationship'.[431]

The Court has jurisdiction on the interpretation and application of the Charter and other international human rights instruments ratified by AU members.[432] The Court's jurisdiction extends to States that have ratified the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights. As of the time of preparation of this dissertation, 27 States have accepted Court's jurisdiction. The rest of the States are not subject to the Court's jurisdiction.

The jurisdiction of the Court is limited to cases instituted by the Commission (on behalf of individuals) and African based intergovernmental organizations. However, there are instances where an individual or a local NGO can institute a case to the Court. This is only possible when a Member State makes a declaration under Article 35 of the Protocol to accept the jurisdiction of the Court. Such application by individual or NGO is usually instituted as per Article 5 (3) of the Protocol. So far, only Tanzania; Burkina Faso, Ghana, Cote d'Ivore, Rwanda, Mali and Malawi have made such declaration. It means individuals and NGOs from States which have yet to make the declaration, their recourse in case of a human right breach is to institute their matter with the Commission.

The Court affords senior state and government officials with immunity from prosecution.[433] Consequently, heads of States and senior officers enjoy immunity for human rights infringements for acts done when they are in office. This is quite contrary to international law which allows international Courts to lift the immunity of the Head of State and senior members so as to end immunity. It is also different from other supranational Courts' practice. For example, the ICTR[434] and ICTY[435] expressly states that the official position of a person, whether the head of State or government does not relieve a person from prosecution or mitigate the prescribed punishment. A similar position is provided by the ICC. The Rome statute under Article 27 (1) declares equality of people on access to the Court and application of the rules of the statute regardless of one's official capacity.

The execution of the ACHPR by States is voluntary. The AU, in respect of State sovereign, uses a polite language in the Protocol establishing the Court, that 'State parties to the Protocol undertake to comply with the judgment in any case to which they are a party and to guarantee the execution within the time stipulated by the Court.[436]

---

[431] Pityana, N. B., 'Reflections on the African Court on Human and Peoples' Rights', AHRLJ, 2004, Vol. 4, pp. 121-129 at p. 126.

[432] The Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, Article 17.

[433] At its 23rd Ordinary Session in Malabo, Equatorial Guinea, the Assembly of the African Union adopted an amendment to the Protocol on the Statute of the African Court of Justice and Human Rights to immunize African leaders accused of committing serious human rights violations from criminal prosecution before the proposed African Court of Justice and Human Rights.

[434]ICTR Statute, Article 6 (2).

[435] ICTY Statute, Article 7(2).

[436] The Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, Article 30.

The rulings of the Court, as a principle of international law, do not directly repeal any law, set aside or nullify local judgment and or ruling or any administrative acts. They only have a declaratory effect; they are mere denunciations. The Court rulings of the ACHPR are directed to the AU Member States to remind them of their obligations under the Banjul Charter and other treaty obligations. It is the AU Member States who have the responsibility to execute the Court's judgments. The task to oversee the implementation and execution of the Court's judgments is upon the Council of Ministers.[437] Boukongou considers this mechanism as insufficient to ensure compliance 'given the diplomatic inertia within this authority'[438] regardless of the fact that the Member States also have a secondary obligation to report on their compliance or otherwise with the Court's judgments imposed upon them by the Assembly of Heads of States and Government.[439]

The Court can, apart from the declarations, issue remedial judgments (compensation or reparations), and in special cases, such as those in need of urgent intervention, the Court can adopt provisional measures to avoid irreparable harm to individuals.[440]

4.2.1.3 The Proposed African Court of Justice and Human Rights

In 2003, the AU adopted a Protocol for the establishment of an African Court of Justice. The Court was intended to have jurisdiction over economic integration and matters of political nature. This Court had never commenced its operations. In 2008, another Protocol was adopted. The Protocol proposes a creation of yet another Court; the African Court of Justice and Human Rights (ACJHR). Article 2 of the Protocol states;

> 'The African Court on Human and Peoples' Rights established by the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights and the Court of Justice of the African Union established by the Constitutive Act of the African Union, are hereby merged into a single Court and established as "The African Court of Justice and Human Rights'.

The proposed Court is replacing the ACHPR and the African Court of Justice (ACJ)[441] initially established by the Constitutive Act but whose operation was suspended in anticipation to the creation of the ACJHR. The Protocol establishing the ACJHR was adopted in 2008 and was to enter into force after 30 days upon deposit of the instrument of ratification by 15 AU Member States. So far, the Protocol has been signed by 30 countries and ratified by 5 countries only[442] out of the 54 AU Member States.

---

[437] The Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, Article 29.
[438] Boukongou, J. D., 'The Appeal of the African System for Protecting Human Rights, AHRLJ, 2006 Vol. 6, pp. 268-298 at p. 291.
[439] The Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, Article 31.
[440] Ibid, Article 27 (2).
[441] This Court was not discussed in the text for obvious reasons.
[442] The countries are Benin, Burkina Faso, Congo, Libya, and Mali.

The proposal is for the Court to have three sections; for general affairs, for human rights and individual criminal responsibility. Once the Court receives the required number of ratification, it shall have jurisdiction over the interpretation and application of the Constitutive Act and AU treaties. The Court will have the power to review decisions, assess the legality of legal instruments adopted by AU and organs created thereof. Also, the Court will be dealing with the determination of questions regarding the application of international law in the Region and Members' obligations under the International law including determining and issuance of reparations for breaches.

The Court, as with the ACHPR and ACJ, limits its access to State parties, AU organs and institutions and AU Intergovernmental Organizations. Access to the Court by individuals and national based NGOs will depend on the State's declaration accepting the Court's competence. And like the present Court, Heads of State and government and senior government officialsh have immunity from Court's prosecution for acts done during their tenure in the office.[443]

4.2.2 Privacy and Data Protection in the African Union

Privacy in Africa is regulated from the Regional, Sub-regional to the national level. At the Regional level all instruments providing for human, civil and political rights, contain provisions for the right to privacy with exception to the African Charter on Human and Peoples' Right of 1981. For example, the ACRWC and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and Convention on Cyber Security and Personal Data Protection of 2014 (the Malabo Convention).

4.2.2.1 Regional Regulation

The Malabo Convention was adopted on 27 June 2014, making Africa the second Region, after EU to adopt a data protection instrument. However, the Convention, unlike the EU-DPD does not only provide for data protection framework, rather has created two regimes; cyber-security regime and data protection regime. The Convention deals with three main subjects affecting online activities, e-commerce, cybercrime and security and data protection. Data protection regime established by the Convention is provided under Chapter II: Personal Data Protection. From the preamble, the objective of the Chapter is to protect privacy and promote free movement of information. The aim is to inspire harmonization of existing data protection legal regimes and invoke reforms to the Member States lacking or with weaker data protection regimes.

The established regime is modelled in a similar structure as the international instruments such as the OECD guidelines, Convention 108 and the EU-DPD. On processing of personal data, the Convention provides for seven principles of data protection, similar to those found in

[443] Article 46A of the Protocol on Amendments to the Protocol on the Statute of the African Court of Justice and Human Rights.

international codes, of course with some few adjustments.[444] The Convention excludes the regulation of personal data contained in temporary files made by technical intermediaries including the ISSP providers for automatic, intermediary and transitory storage of data. [445] Other exemptions are on the processing of personal data for purely domestic purposes and in personal context, as long as such data is not intended to be shared to or with 3rd parties;[446] and the processing of personal data for journalistic and research as long as it is done in accordance with the professional codes. Processing for artistic and literal expression is also among the exempted activities.[447] Processing of personal data involving data matching is restricted upon DPAs authorization.[448] However, the Convention contains no provision for data breach notifications.

The restriction is declared on the processing of sensitive personal data, save for a few instances where the Convention is making an exception.[449] The Convention definition of sensitive data includes the usual category of sensitive data but extends further to include data such as those of 'parental filiation' not usually found in other data protection codes. This could be based and justified on the belief as Greenleaf and Georges explains that, in Africa 'knowledge of the identity of a person's biological parents can be used in spells to harm them'.[450]

Decisions made based on automated processing of personal data are prohibited when such decision can substantially affect the data subject.[451] Furthermore, unlike other data protection codes, the established framework for data protection does not create restrictions on direct marketing. Instead, the restrictions are introduced under Chapter one of the Convention which creates the legal framework for e- Transactions.[452]

Furthermore, the established regime gives the Member States an obligation to establish an independent Data Protection Authority.[453] The composition and administrative powers of such authority are left to the determination of individual States.[454]

The framework for trans- border data transfer under the Convention restricts the transfer of personal data outside the AU to territories without adequate level of protection.[455] Sadly, the Convention leaves the AU Member States on cross road for failure to define what presupposes an adequate level of protection; and while it does not suggest free flow of data between parties to the Convention, it does not impose an adequate requirement to AU Member States regardless of whether or not they have ratified the Convention. Furthermore, by virtue of Articles 12 (2) (k) and 14 (6) (b), DPAs can authorize trans-border transfer of personal data regardless of the adequacy of protection offered by the recipient. Surprisingly, the Convention, unlike the other data protection codes, i.e. OECD; CoE and DPD, lacks derogation rule for trans-border data

444 Malabo Convention, Articles 16 – 23.
445 Ibid, Article 9 (2) (a).
446 Ibid, 9 (2) (b).
447 Ibid, Article 14 (3).
448 Ibid, Article 15.
449 Ibid, Article 14 (2) (a-j).
450 Greenleaf, G and Georges, M., 'The African Union's data privacy Convention: A major step toward global consistency?, Privacy Laws & Business International Report, 2014, No. 131, pp. 18 – 21 at p. 19.
451 Malabo Convention, Article14 (5).
452 Ibid, Article 6.
453 Ibid, Articles 11-12.
454 Ibid, Article 11 (3).
455 Ibid, Article 14 (6) (a).

flow. There are no provisions regarding Binding Corporate Rules or Model Contracts for transfer of personal data to third countries.

4.2.2.2 Sub-Regional Regulations

Africa has at least eight RECs, but only four are as yet significant in the data privacy context: ECOWAS (West); SADC (South), ECCAS and CEMAC (Central) and EAC (East). Economic Community of West African States (ECOWAS), West African Economic and Monetary Union (UEMOA), Economic Community of Central African States (ECCAS), Economic and Monetary Community of Central Africa (CEMAC), East African Community (EAC), Common Market for Eastern and Southern Africa (COMESA), Common Market for Eastern and Southern Africa (COMESA), Southern African Development Community (SADC).

(A) West African Region

The Supplementary Act on Personal Data Protection In the west Sub-region the ECOWAS[456] had, in 2010, adopted the Supplementary Act A/SA.1/01/10 on personal data protection. The Act is so far considered the strongest in the Region among the existing data protection instruments, including the Malabo Convention. Other scholars go further saying the Malabo Convention is a replica of the ECOWAS Supplementary Act. Makulilo asserts that 'even the scope and aims are the same except that, whereas the Convention applies in the territory of Member States of African Union, the Supplementary Act applies to any processing of personal data carried out in the UEMOA or the ECOWAS Member States'.[457]

The objectives of the Act as recited in the Recitals 10 and 11 of the preamble are the same as those in the Malabo Convention, that is, protection of privacy and promotion of free movement of information, and, also, to harmonize data protection legislations among the Member States existed before the Act. The Act provides for principles in the protection of privacy in chapter V; and like the Malabo Convention, the Act requires the establishment of the data protection authority to oversee compliance. The Act goes further specifying qualifications for the members of the proposed DPA. To be qualified, one must be qualified in the field of law, ICT and other fields of knowledge to achieve the objectives of the Act; unlike the Malabo Convention which provides for a list of people who may serve in the data protection authority. The Act has also clarified its enforcement, stating that the Act is an integral part of ECOWAS Treaty,[458] which means the ECOWAS Court of Justice is therefore mandated to enforce the Act.

The ECOWAS Court of Justice The ECOWAS Court of Justice was established in 2002 by article 2 of the Protocol to the ECOWAS Treaty. The Court was established to interpret and enforce the

[456] ECOWAS is an Economic Community for West African States with fifteen members including Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.
[457] Makulilo (n 26), p. 345.
[458] ECOWAS Treaty, Article 48.

principles of treaties and other legal regulation adopted within ECOWAS, as such, its jurisdiction extends to all instruments adopted by the Community. Within its jurisdiction, the Court task is to determine Members' obligations under international law and community instruments, the legality of Regulations, Conventions, Directives and all legal instruments adopted by the community, and enforce Members' human rights obligations. Access to the Court is by State party or a member of the Conference of State. The Court can also offer advisory opinions at the request of institutions and the Member States.

(B) East African Region

In the East African Sub-region there are two instruments for privacy protection; the Draft Bill of Rights for the East African Community of 2009 and the East African Community Legal Framework for Cyber Laws, Phase I of 2008 and phase II of 2011.

The EAC Draft Bill of Rights The EAC draft Bill of Rights was drafted to address the omissions in the national Constitutions of Member States and to harmonize the standards of human rights protection in the Sub-region. The Bill provides for the right to privacy under article 7. The provision makes good of the omission in the African Charter with regards to rights to privacy in the context of the EAC Member countries.

The EAC Legal Framework for Cyber Laws On the other hand, the EAC Legal Framework for Cyber Laws was proposed in 2006 by the EAC's Council of Ministers, seeing the need to establish a proper regulatory framework to nurture e-Government strategies at the National and Sub-Regional level.[459] Consequently, the task force on cyber laws was formed in 2007. The task force divided the reforms into two phases based on urgency and priority of addressed issues. Phase I address e-transactions, e-signature and authentications, privacy and data protection, property, domain names, taxation and freedom of information. On privacy and data protection, phase I stated; the objectives of the framework is to harmonize policies and regulations in the East African Community.[460] [461] Surprisingly, it neither proposes a specific framework nor model law. The framework only gives Member States obligation to create a framework for data privacy and non-binding recommendations towards legislating for such a framework.

The *travaux preparatoires* recommends baseline standards for the processing of personal data, encouraging members to comply with what the framework calls 'principles of good practice'. According to the Framework, the principles of good practice include accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security.[462]

---

[459] Legal Notice No. EAC/8/2007, East African Community Gazette, Vol.AT 1-No.0004, Arusha 30th December 2007; East African Community, Draft EAC Legal Framework for Cyber Laws, (Phase I) November 2008, p.3.

[460] See the EAC, Background Paper for the Second Meeting of the EAC Task Force on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008, (Annex I), p.2; also EAC, Report of the 2nd EAC Regional Task Force Meeting on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008, p. 6.

[461] EAC, EAC Legal Framework for Cyberlaws, (Phase I), p.5; EAC, EAC Legal Framework for Cyberlaws, (Phase II), p.3.

[462] Walden, I., 'East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework', Draft v.1.0, 2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008, p. 17.

The principles include data subjects' right to be informed of processing activities involving personal data and an opportunity to amend incorrect data.

Recommendation 19 of the Framework provides a blanket recommendation, urging the Member States to take into account 'fully' international best practices in the area without mentioning or making reference to any particular data protection framework as forming the 'best practices'. What is more surprising is the fact that, on all subjects dealt by the Framework I, the task force has provided a copy of a model law or recommended framework as an annexure; however, the same was provided in relation to data protection.

The Framework does not give recommendations on establishing DPAs, on the contrary, it cautions that such authorities, especially for developing countries will be costly. At the same time, the task force stresses on the fact that, in the instance, a Member States decides to establish a DPA, it is crucial that the DPA is established as an independent body from the Government in order to provide necessary trust and assurance in its regulatory activities.

The EA Court of Justice The EA Court of Justice was established in 2001 by Article 9 of the Treaty establishing the EAC. However, the Court does not have human rights jurisdiction. However, Article 27 (2) of the Treaty, gives the Council of Ministers powers to extend the Court's jurisdiction to include human rights issues. One may consider the Court's lack of human rights jurisdiction as ambiguity, since the Treaty to which the Court was established to enforce contains human rights provisions. So far, the Court has jurisdiction over trade and labor disputes. Somehow, the present jurisdiction of the Court reflects the EAC main objective, i.e. to achieve political federation.

(C) Southern Africa Region

The Data Protection Modal Law SADC[463] is another Sub-region with privacy regulation instrument. In 2012, SADC approved the draft Data Protection Model Law. Like the ECOWAS Act, the Model Law propels on the framework for data protection mimics the international codes on data protection. Consequently, the regime proposed is similar to the one established by ECOWAS and the Malabo Convention, but with some significant variations in their scope of application.[464] The SADC Model Law lacks preamble in an orthodox meaning and context as expected with model laws. Hence, it brings difficulties in interpreting the intentions and the context of the law. It also fails to give its objectives; however reading from the provided 'preamble', the protection of an individual right to privacy and harmonization of data protection policies and laws may be inferred.

The SADC Tribunal The SADC Tribunal was established in 2005 by Article 9 (g) of the SADC Treaty and the Protocol on the Tribunal. Although inaugurated in 2005, it commenced operation in 2010. Article 16 of the SADC Treaty confers the Tribunal with jurisdiction over interpretation

[463] The Sothern African Development Community (SADC) is a sub-regional grouping of fifteen countries: Angola, Botswana, Democratic Republic of the Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe.
[464] Makulilo (n 26), p. 359.

of the Treaty, and all other legal instrument adopted by the community. The Tribunal is also empowered to deal with members' dispute arising out of agreements, conflicts between the Member States or the Member States and legal or natural person. The Tribunal was established with a mandate to deal with human rights issues; however, in 2012, after a controversial decision rendered by the Tribunal against the President of Republic of Zimbabwe for breach of human rights and fundamental freedoms,[465] the Tribunal was stripped of its power to adjudicate over human rights issues. To achieve this, head of States and Governments, adopted a Protocol on the Tribunal, limiting its powers to interpretation of the SADC Treaty and other ratified instruments relating to disputes between the Member States.

Other Sub-regions, including COMESA, ECCAS AND UMA have no notable initiatives in the area of privacy and data protection; although some countries (such as Tunisia, Morocco) within these Sub- regions have adopted comprehensive framework for data protection.

4.2.2.3 National Regulations

The majority of African State Constitutions provides for privacy rights. However, the scope, context and mode of their implementation differ from country to country. Taking an example of Cape Verdean Constitution of 2010; it provides for two pillars for privacy protection. The first pillar of protection resembles those found in international instruments such as article 12 of the UNCHR and Article 17 of the ICCPR; with somewhat wider scope and more elaborate. Reading from Articles 38 to 42, the Constitution guarantees the right to privacy to personal identity, (including personal images) good name, honour, reputation in a civil capacity and in a family life.[466] The protection extends to protection against arbitrary entry into one's home without legal justification.[467] Article 41 guarantees confidentiality of correspondence and communications. The Constitution goes further under Article 42 prohibiting anonymous or secret recording (using technological devices) and processing of personal data, either for political, philosophical or ideological or religious/faith reasons. Prohibition is also made against an unauthorized access and processing of computer files, records or database. This provision is similar to Article 71 of the Mozambican Constitution.[468]

The second pillar is *habeas data. Habeas data* is provided under article 43 of the Cape Verdean Constitution. The provision states as follows;

---

[465] Mike Campbell (Pvt) LTD & others v. Republic of Zimbabwe; SADC (T) 2/07, 13 December 2007.

[466] Cape Verdean Constitution, Article 38.

[467] Ibid, Article 40.

[468] Article 71 of Mozambique Constitution on the Use of Computerised Data states;

> *'1. The use of computerised means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives, shall be prohibited.*
>
> *The law shall regulate the protection of personal data kept on computerized records, the conditions of access to data banks, and the creation and use of such data banks and information stored on computerised media by public authorities and private entities.*
>
> *3. Access to data bases or to computerised archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerised file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision.*
>
> *4. All persons shall be entitled to have access to collected data that relates to them and to have such data rectified'.*

'43. (1). *Tous les citoyens ont droit à l'habeas data leur permettant de prendre connaissance des renseignements figurant dans les fichiers, les archives ou les registres informatiques les intéressant, d'être informés des fins auxquelles elles sont destinées, et d'exiger que ces données soient rectifiées ou mises à jour.*

(2). La procédure d'habeas data est réglementée par la loi'.

The provision gives all citizens the right to *habeas data,* allowing them to review the information contained in the files, archives, or computer records; to be informed of the purpose for which their personal data are intended for, and to require that the data be corrected or updated. In Cape Verde, *habeas data* is a procedure regulated by law.

However, the Cape Verdean Constitutional provision on privacy right and that of *habeas data* have a limited application. They apply only to Cape Verde citizens. This limitation is similar to one imposed in the Nigerian Constitution of 2011. Article 37 of the Nigeria Constitution states;

'37. The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'.

Surprisingly, all other fundamental rights provided under part IV in the Nigeria Constitution are guaranteed to *'every person'* except the right to privacy which is guaranteed to only to *'citizen'*. It is even more surprising that the previous version of the Constitution, the Nigerian Constitution of 1960 had the right to privacy under article 22 in the following terms;

'22. (1) Every person shall be entitled to respect for 'his private and family life, his home and his correspondence'.

It would seem that the constitutional right to privacy in Nigeria deteriorated with the Constitutional development rather than improving; with regards to the right to privacy.

The other African States with Constitutional right to privacy structures the right in similar terms to international instruments. The right to privacy is provided as the basic protection to '*every person',* against arbitrary searches in one's dwelling houses or properties, collection and processing of information relating to their family and private affairs including privacy of their communications.[469]

[469] See article 31 of the Kenya Constitution 2010; Article 14 of South African Constitution 1996; Article 27 of Uganda Constitution 1995; Articles 13 and 15 of Senegal Constitution; Article 57 of Egypt Constitution; Articles 10 and 11 of Lesotho Constitution; Article 32 of Angola Constitution; Article 9 of Botswana Constitution; Articles 20 and 21 of Benin Constitution; Article 16 of Tanzania Constitution (New constitution article 27); article 21 Malawi Constitution; Article 22 Rwanda Constitution; article 28 of Burundi Constitution; Article 9 of Mauritius Constitution; Article 28 of Togo Constitution; Article 6 of Burkina Faso Constitution; Article 24 of Tunisia Constitution; Articles 39 and 40 Algeria; Article 37 of the interim Constitution of Sudan of 2005 (the previous Constitution of 1973 article 29); article 22 of South Sudan Constitution; article 26 of the Ethiopian Constitution; article 24 of the Morocco Constitution as published in the bulletin official; articles 11,12 and 13 of the Libya Constitution; article 6 of Mali Constitution; article 12 and 13 of Djibouti Constitution; article 42 and 45 of Chad Constitution; article 5,6 and 12 of Gabon Constitution; article 12 of Guinea Constitution; article 23 of Gambia Constitution; article 27 and 29 of Niger constitution; article 32 of Zambia constitution.; article29 and 31 of the Constitution of Democratic Republic of Congo; article 13 of Namibia Constitution; article 13 of Madagascar Constitution and article 15 of the Constitution of People's Republic of Zanzibar and article 57 of the Republic of Zimbabwe of 2013.

Mauritanian Constitution is silent on privacy rights; Somali, Swaziland and Ivory Coast's Constitutional privacy rights are limited to unauthorized entry and surveillance of dwelling houses. Cameroonian Constitution has the right to privacy provided in the preamble; normally not enforceable. However, Article 12 of the Cameroonian Constitution states, that, Cameroon *'shall recognize and protect traditional values that conform to democratic principles, human rights and the law'*. The similar pattern is seen in Comoros, where the right to privacy is provided in the preamble. However, in the case of Comoro, the right to privacy, like Somali, Swaziland and Ivory Coast are only guaranteed against unauthorized searches and surveillance of the dwelling houses.

Some African States have adopted comprehensive privacy protection laws/data privacy laws;[470] other with draft bills.[471] These laws enforce the Constitutional right to privacy in a more achievable manner. They impose privacy protection obligations and principles in securing and regulating storage, usage and processing of personal information. These reforms, as reported by Cynthia Rich, 'are still in their formative stages, in large part because the regulators are not yet in place; however, in some of the countries with a more established privacy regimes, the regulators have been stepping up their enforcement efforts'.[472] The best example to illustrate Cynthia's observation is Cape Verde; Cape Verde was the first African country to adopt a comprehensive data protection law in 2001. To-date, the country has yet to establish a DPA. Another example is Seychelles, the second country to adopt comprehensive data protection law in Africa in 2003; to-date, Seychelles has not yet publicized the law. Hence, the law remains unimplemented. Most of these laws contain the traditional data privacy principles and obligations.

Although these principles are similar to the domestic laws, there is varying degrees of the strictness of rules, practice and procedures in dealing with personal data as well as regimes for trans-border data flow. In some countries, there are also (on top of or without the comprehensive data protection laws) sector-specific laws. These laws have privacy specific rule/principles based on activities within a relevant sector. Most of such laws are found in the communication sector, health sector, National security laws, and employment sector.

4.3 Conclusion

Data protection regulations and institutions in Africa are still developing. Privacy is protected both in the human rights instruments and specific data privacy laws. The majority of the human rights instruments and data privacy laws/instruments are soft law hence do not offer compelling force for the enactment of data protection legislation at national levels. Although these laws are similar, in a sense that they contain basic data protection principles, and require the establishment of supervisory authorities, they are at the same time dissimilar for having different scopes.

[470] E.g., Angola (2011), Benin (2009), Burkina Faso (2004), Cape Verde (2001), Mauritius (2004), Morocco (2009), Senegal (2008), Tunisia (2004).
[471] E.g., Ghana (since 2010); Kenya (since 2009), Tanzania (Since 2013), Uganda (2010), Rwanda (since 2013).
[472] Rich, C., 'Privacy laws in Africa and Middle East', Privacy and Security Law Report, 2014.

The record on the domestic enforcement of the constitutional right to privacy is disappointing. As a Region, Africa neglected or refused to recognize the right to privacy under the Regional Instrument. It is therefore not surprising that even at Sub-Regional level; the right to privacy has never been adjudicated. The enforcement of other human rights violations has also been stalling. In fact, Sub-Regions such as the SADC had decided explicitly to revoke its Tribunal's power to enforce human right violations. This reveals the lack of political will to enforce individual rights in Africa; regardless of the promise and guarantees provided in the preambles of the Regional and Sub-Regional human rights instruments.

5. Data Protection Reforms in Africa: Civil and Common Law Legal Culture

5.1 Introduction

African States' legal systems are relatively complex and diverse owing to colonization. The majority of the systems are an interface of imported colonial rules and customary laws. Others add Islamic law to the mix. Senegal is a former colony of France hence 'inherited' the Civil Code legal system. In addition to this system, Senegal has a customary and Islamic law system. Like Senegal, Tanzania has a system of customary law, Islamic law (invoked mostly in matters relating to personal law) and of course Common Law legal system, an inheritance from the British. Although the focus of this chapter is not to assess the legal cultures or the systems of the two countries, it is necessary to identify the attributes of the two legal systems and their relevance (if any) in legal reforms. This is important because both systems have, during and in the post-colonial era, responded and been influenced differently by an introduction of what Jacques Frémont refers to as 'the official legal system'.[473] Also, is the fact that, in the sphere of human right (especially the right to privacy) acceptance and legitimization of such rules or legal frameworks may create complex questions on concepts and cultural interaction as already discussed in chapter three. Another consideration is the fact that, African states accommodate more than one legal culture in parallel. In total, the chapter assesses to what extent is this classification relevant in relation to legal reforms.

The chapter also makes a comparative mirror analysis of the two countries data reform process and the established data protection regimes. The essence of the analysis is to see how, and if so to what extent these reforms reflects the nature of the African pluralistic legal systems. Also, the chapter navigates through different attempts to harmonize legal frameworks in Africa as an attempt to predict the prospects for the harmonization of data protection regimes in Africa.

5.2 Demystifying Legal Cultures: The Relevance of the Civil and Common Law Systems in Legal reforms

Civil or Common Law legal system is the difference resulting from the variation in legal standing. While Civil Code system relies on the legal text, the Common Law system relies on judicial opinion and traditions (precedents). It means a civil law judge would rely entirely on the legal text to derive to a decision; while a common law judge has much more autonomy to decide beyond the legal text by applying judicial reasoning and invocation of precedents. Contemporary scholars discourage a discussion on the differences between the two systems as they consider having no substantial role in legal reforms. Salvatore Mancuso illustrates this with reference to the traditional understanding where the distinction came from, regarding the role of Courts applying abstracts and general rules to get to a legal standing. Explaining the scenario saying;

> 'Civil Law legal systems are characterized by the presence of codes and other statutes containing an extensive number of legal provisions forming the entire corpus of laws to be applied by the courts. Such a system is assumed to be self-sufficient; encompassing all

[473] Frémont (n 369), p. 150.

> the rules suited for all possible cases without any need for "external" contributions, leaving the courts without any space to move beyond the application of the prearranged substantive rules. On the other hand, the English legal system was conceived as a system with a limited number of statutes and legislative acts, creating wide autonomy for the courts to determine the rule of law applicable to a specific case which would later serve as precedent for future courts.'[474]

The author believes the reliance in codes and statutes by the Civil Law systems is vanishing. To him, the practitioners and scholars from Civil Law legal traditions are becoming more similar to the Common Law legal tradition by going beyond the codes and statute and applying case laws. He explains in length, and to avoid derogation and distortion in what he meant to say, I prefer to bring in his words;

> 'Modem courts tend to make their decisions conform to the principles of law contained in the rules set forth in the codes and statutes, as well as to how other courts, especially the high courts, have interpreted and applied the codes and statutes. Journals and commentaries related to case law have been established in both case law generally and to specific areas of law specifically. Academic teaching is constantly moving from the simple use of doctrinal handbooks, to a more integrated approach - teaching by using case law and incorporating practical classes where the analysis of foreign legal systems is now considered essential to better one's knowledge of a specific legal issue.'

In the area of law-making, the trend is to move to the adoption of codes characterized by 'open' rules. Thus, the courts are left to decide between further developments of the single rules (this is the case of the Dutch Civil Code of 1992 where even the traditional hierarchy among the different sources of law has been abandoned); the adoption of rules that are the result of principles elaborated both in the civil law and the common law legal traditions (this is the case of the UNIDROIT Principles of the International Commercial Contracts or the CISG which greatly influenced the drafting of the rules on contracts in several countries); or the codification of legal institutions elaborated by the Common Law tradition (like in the adoption of trust law in China).'[475]

The author also notes that the Common Law legal tradition is taking steps towards the use of codified rules. He gives an example of England's on going law making activities and the 1998 adoption of a civil code fashioned in civil law style. He gives other examples of a mixed legal system as such as the USA which seems to be moving towards codification of legal rules and reliance on written statutes, bringing it closer to Civil Law legal system. The trend, he says, have converged the two systems, something that is not only seen in practice but also in legal concepts, rules and fundamental categories, terminology as well as sharing of common legal and democratic values,[476] which he attributes to the ongoing legal harmonization in Europe.

As with Europe, Africa is moving towards legal harmonization. Although the harmonization has been very slow; an important point of departure is that the convergence of the Civil and Common Law legal systems in Africa cannot be surmised as a convergence of legal culture in

---

[474] Mancuso, S., 'The New African Law: Beyond the Difference Between Common Law and Civil Law', Annual Survey of International & Comparative Law, 2008, Vol. 14, No. 1, pp. 39-60, at p.. 43.
[475] Mancuso(n 476), p. 44.
[476] Ibid, p. 45.

general terms as well. One needs to be mindful of the factual differences; more so when there is an introduction (or the need to introduce) of a new legal framework. The first aspect is the structure of the African legal systems with makes it different from the rest of the world. Salvatore Mancuso explain this phenomenon in terms of the mixture of legal systems in African system; he says, the imported Western legal system which gives each African country a specific legal imprint differentiates it with the other African States and gave rise to a sub-classification of an African legal system rooted in the structure and tradition of a former parent country.[477]

Mancuso continues to explain that, although African legal systems can be assimilated with that of the respective colonizing country, one should not assume that the legal rules are the same with the Western country from which they received their legal system. There have been several legal developments both in Europe and Africa; on one hand, African States have not adopted the new development of their former colonies and on the other, African States had their own legal development 'involving the revaluation of customary law, development of their own case law and transplant from other non-European legislations. The key role played by customary law, the influence of religious law (Islam) give rise to a hybrid, modern African legal system cannot found anywhere else in the world.'[478]

There is also a role of the Sub-Regional economic community bringing the Member States with different legal culture and colonial backgrounds such as the East African Community. Initially, the EAC comprised of Tanzania (former Germany and later British colony) which, after independent adopted a socialist approach, Kenya and Uganda (former British colonies) and currently joined by Rwanda and Burundi (former French colonies). Regardless their history, the then and the renewed Treaty for the establishment of the EAC[479] calls for the Member States to harmonize their national legal frameworks to foster for trade and development within Members. South Africa for example, has a mix of Civil and Common law but with a major influence from a Roman-Dutch system; characterized by the application of 'customary' laws in absence of professional judges.[480] Today, South African legal system may be characterized as more of a Common Law system, although stare decisis is given less weight as other Common Law systems. In South Africa, customary law is more powerful that Civil and Common Law. The South African Constitution explicitly requires judges, when interpreting Bill of Rights, to consider the local Customary Law and International Law.[481] In fact, Courts have a constitutional obligation to develop customary law in order to align it with constitutional dictates.[482]

Another example is the Monarchy of Morocco, with a more complex history and legal culture. Morocco has three tier legal systems functioning parallel; the Islamic Law, Civil Law and Customary Law. In balancing the requirement of all the systems, Morocco had to establish a peculiar Court system, better narrated by Chris Nwachukwu Okeke quoting Emory, L., that, 'Morocco has a four-level Court or Judicial setup. It has twenty-seven Sadad Courts, thirty

[477] Mancuso (n. 474), p. 46.
[478] Ibid.
[479] See Article 126 of the EAC Treaty and Article 47 of the EAC Common Market Protocol. This led to drafting of the Bill of Rights for the EAC and establishment of the EAC Frameworks for Cyber Laws 2008/2011.
[480] De Cruz, P., Comparative Law in a Changing World, Cavendish Publishing Limited, London/Sydney, 2nd ed., 1999, p.47.
[481] Constitution of South Africa 1996, Article 31.
[482] *Gumede v. President [2008] ZACC 23 at p. 29.*

Regional Courts, nine Courts of Appeal and a Supreme Court in Rabat. Sadad and Regional Courts are divided into four sections: shari'a; rabbinical; civil, commercial and administrative; and penal sections. Sadad Courts are Courts of the first instance for Muslim and Jewish personal law. Shari'a sections of Regional Courts also hear personal status cases on appeal.'[483]

Upon her independence, Morocco established a legislative body, *Mudawwana* and started codification of legal rules, including traditional customary rules and Islamic rules. Presently, Morocco has a well-established system of religious and customary law with precedents forming binding law.[484] The legal system implemented today in Morocco is no longer Civil Law system; it is a localized legal system devised to express the need, wish and definition of justice for the Moroccan people. The legal system in Morocco cannot be considered to resemble any of the categories of the Western legal systems or that of the colonial masters or any other African state. Therefore, the classification of African States based on the legal system transplanted or adopted from the ex-colonial powers bears no or very little significance today in determining new legal reforms. This is contrary to the assumptions made at the beginning of this research. Hence, in this research, the two systems are not considered as whole separate systems, but, as proposed by Mancuso, two possible aspects of Western legal systems as they are no longer taken to have substantive significance in legal reforms in the African context.

Perhaps an important aspect when dealing with African legal reforms is the role of African customary law and or practices. Again, a startling and an insightful discovery made in the course of this research. While the distinction between Civil and Common Law systems seems to be vanishing and of less relevance in reform processes in Africa; the role and influence of African customary laws in legal reforms and legal harmonization are remarkable and cannot be ignored. Instead of looking at the traditional Civil and Common law differences (which are in fact diminishing and may lead to false conclusions) in determining legal cultures in Africa, as a Region and in individual States, three dimensions are proposed. Mancuso in affirming Gbenga Bamodu[485] proposition, suggests a three dimension examination, 'diversity within each country, diversity among the African countries and diversity between African and non-African countries.'

Mauro Bussani and Anthony Allott suggests an interdisciplinary study involving researchers from other fields such as sociologists, anthropologists, linguists, economists, historian to search for the 'common core' of an African law to extract common features from different traditions. While the proposal is valid, its implementation may be far-fetched. Africa has 54 countries; each country has a number of customs and traditional rules; as a result, Africa has more applicable laws (through customary) than other Continents and Countries.[486] The diversity of customary law practices and traditions within a single country makes its nearly impossible to invoke such a study; at least in the present context with limited time, human resource and funds. For example, taking one of the case studies, Tanzania has 128 tribes, each with its peculiar customary law practices, traditions and own tribal language. In Big countries like Nigeria, there are 250 ethnic

[483] Okeke, C.N., 'African Law in Comparative Law: Does Comparativism Have Worth?', Roger Williams University Law Review, 2011, Vol. 16, No. 1, pp.1-50.
[484] Ibid.
[485] Bamodu, G., 'Transnational Law, Unification and Harmonization of International Commercial Law in Africa', Journal of African Law, 1994, Vol.38, No.2, pp.125-143.
[486] Okeke (n 483), p.2.

groups each with its customary laws, traditions and ethnic languages.[487] These systems of tribal law are as diverse and innovative as the legal system of any State.[488]

Studying the traditional or tribal laws of African States, summons a major difficulty. Most of these systems are not incorporated into written texts. Cultural anthropologists in Africa have recorded some systems through studies, but very few have been formally codified as part of the laws of the African States. Moreover, the vast majority of these systems would require a scholar studying the systems, a journey to the Region and speak with people about how their system of traditional law functions. The full understanding of the traditional system would also require a greater knowledge of the way the culture and social relations are conducted in the Region and with individual State and down to each ethnic group. As such, a simple textual and situational analysis of these systems would not suffice. They require far more effort than studying a series of Constitutions or Codes for effective analysis. For these reasons, this research opted to focus on comparing various layers within each case study (Senegal and Tanzania), the political and legal background as well as the history and or motivations pertaining to the drafting and reforming of the data protection regimes; and whether or not the reforms reveal any considerations to the existing legal systems apart from the 'formal legal' system.

5.3 Legal Harmonization and/or Unification: Is Africa in Divide?

The discussion in this section is imperative for the reasons that, this research seeks to examine African legal environment with regards to harmonization of data protection regulation. Although Senegal and Tanzania were selected as case studies, whatever route the two countries undertook have been stimulated and or have bearing within the bigger picture; specifically, Regional and Sub-regional responses, trends and practices with regards to data protection and in particular legal reforms and legal harmonization in general. Therefore, it is necessary to have a glimpse of what is happening on the Continent regarding law reforms and legal harmonization.

The legal harmonization initiatives in Africa reveal a pattern of partition. The divide manifests between the Francophone and Anglophone countries. This, although not formally declared can be observed from the approaches, patterns and initiatives towards specific legal reforms and collective efforts in legal harmonization. For purposes of clarity, it is important to note that the partition is neither related nor influenced by denominations to a Civil Or Common Law legal culture. The partition is based on the States' official languages, i.e. English or French.

5.3.1 The OHADA Framework for Harmonization of African Business Laws

The Organization for the Harmonization of African Business Laws (Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA) is an organization established in

[487] Okeke (n 483), p.2
[488] Ibid, p. 7.

1995[489] with the aim to modernize and harmonize business laws in Africa and to promote investment and economic growth. Although the organization and its objectives refer to 'Africa', its activities are focused on the Francophone African countries. The organization has created a framework for the implementation of the harmonized business laws in the francophone countries through the adoption of Uniform Acts. The Uniform Acts are published in French (with no official English translation) which automatically excludes the English speaking countries from making good of the Acts. This is in compliance with Article 42 of the OHADA Treaty which despite a lack of an official translation of the Acts and other legal documents completely disregards the English-speaking countries, by imposing a language requirement to the Member States signing the Treaty. The Treaty provides that a country signing the Treaty agrees that the working language shall be French. Consequently, all legal documents relating to OHADA and its activities, including case laws are published in French.

Furthermore, the Uniform Acts have a direct domestic application. The effect of the Uniform Act is to annul all conflicting domestic laws.[490]This is a strategy adopted by OHADA to avoid discrepancies and adoption of conflicting laws. Consequently, this rejects the English-speaking countries from adopting the Acts. The Uniform Acts are made and adopted by the Council of Minister under OHADA on behalf of the Member States. Law making bodies in specific countries are excluded in the process, although the governments are consulted in the process. The Common Court of Justice and Arbitration is involved in providing expert advice, while the law making mandate remains with the Council. In effect, this creates another obstacle for the English-speaking countries to form membership, as the language of the law is unfamiliar not only to the people but also to the law enforcers. It also closes any possibility of the English-speaking countries to access the Court (CCJA) for lacking comprehension of the working language. Indeed, the English-speaking countries are technically excluded from forming part of this initiative in harmonization of business laws in Africa. Nevertheless, Article 53 of the OHADA Treaty opens doors to all African countries, members of the African Union (AU) to assent.

5.3.2 ARIPO and OAPI

The African Regional Intellectual Property Organization (ARIPO)[491] and *Organisation Africaine de la Propriété Intellectuelle* (OAPI)[492] are organizations formed to coordinate and harmonize industrial systems in Africa. ARIPO was created by the 1976 Lusaka Agreement and it caters for the English-speaking African Member States. OAPI was created by the 1977 Bangai Agreement. It presupposes of the 61 French-speaking African States. However, unlike the UNIDROIT, OAPI provides for an official English translation for its legal and working documents. The two

[489] The stablishing Treaty was signed in Port Louis, Mauritius in October 1995 and came into force in July 1995.
[490] OHADA Treaty states, Article 10.
[491] Established under Article 1 of the Lusaka Agreement of the creation of the African Intellectual Property Organization, 1976 as amended on August 13 2004.
[492] Established under Article 1 of the Bangui Agreement relating to the Creation of the African Intellectual Property Organization, Consists of the revisions of the Agreement Relating to the creation of an African and Malagasy office of Industrial Property (Bangui (Central Africa Republic) March 2 1977.

organizations coordinate in issues relating to intellectual properties in Africa and both are partners with WIPO through the Quadripartite Agreement.

In 2006 the African Union made an effort to unite ARIPO and OAPI by creating PAIPO as an overall African intellectual property organization. Up until the time of writing this thesis, the organization has not yet come into existence. The Draft PAIPO Statute is still under review by the specialized technical committee on justice and legal affairs of the African Union.

5.3.3 Harmonization of Data Protection Legal Frameworks

5.3.3.1 The Francophone

For the purpose of clarity, Francophone Africa is an economic zone comprised of the former French colonies in the central and West Africa.[493] The Francophone Africa was created by the French in 1945, after the WWII with the hope to assure a continued relation and assimilation with the colonies and sustaining the exchange rate of the CFA against the dollar.[494] [495] This was after realizing that the zone was comparatively underdeveloped and economically behind.

In relation to data protection legal reforms, the Association of Francophone Data Protection Authorities (*Association francophone des autorités de protection des données personnelles* - AFAPDP) has been playing a crucial role in harmonization of privacy and data protection legal and regulatory frameworks in the Francophone Africa. The AFAPDP was founded in 2007 and has its headquarters with the French data protection authority in Paris (CNIL). The AFAPDP has an objective to promote cooperation and training initiatives between the French-speaking countries specifically on issues relating to data protection.[496] It offers expertise to countries without 'proper' legal framework for data protection and brings together data protection authorities to discuss and resolute on issues relating to data protection in specific countries.[497] This is done through yearly organized meeting where all members participate. Apart from the meetings, they also organize summits for members to discuss and exchange priorities and challenges in regulation of data protection. Trainings are also conducted to impart the new authorities with the

[493] Including the West African countries of Equatorial Guinea, Guinea-Bissau and Cameroon not colonies of the French but members of the Francophone Africa.
[494] Zafar, A and Kubota, K., 'Regional integration in central Africa: key issues', World Bank African Region Working Paper Series No. 52, June 2003,World Bank, p. 2.
[495] The 14 Francophone African countries have a common currency, the Communaut financiere africaine (CFA) franc, which is tied to the French franc since 1948. 65 per cent of these countries' external reserves continue to be kept in an account held by the French Treasury issued only by two central banks, for western and equatorial Africa, respectively. While the French treasury guarantees the convertibility of the CFA franc and provides 'practically unlimited overdrafts' to the central banks. This system has been helpful to African countries in that it enables those with balance-of-payments problems to draw on foreign exchange reserves created by those in surplus. See Irving, J., For better or for worse: the euro and the CFA franc, United Nations Department of Public Information Vol. 12 No. 4 April 1999, PP. 24-29 at p. 24.
[496] Statute of AFAPDP, Section 5.
[497] Ibid.

proper knowledge to implement the law and raise awareness to its members on new legal instruments adopted by the organization for their proper implementation.[498]

Furthermore, the AFAPDP participates in dialogue with other Regional data protection institutions such as the EU and the APEC. So far, the AFAPDP has been granted an observer status in the work of the Consultative Committee of the Convention for the Protection of Individual with regards to Automatic Processing of Personal Data of the Council of Europe.

The AFAPDP has made revolutionary changes in the regulation of data protection in the Francophone Africa, although much of their work has largely escaped publicity.[499] Floriane Leclercq, the Data Protection Project Manager at the AFAPDP, had reported that, as of June 2013, seven out of 16 French-speaking African countries had an authority tasked with the protection of personal data and bills are being drafted in six French-speaking African countries.[500] This makes the Francophone African countries ahead of the Anglophone African countries in data protection legal reforms.

According to Leclercq, the objective of the AFAPDP is to ensure maximum adoption of data protection laws and their enforcements. The AFAPDP is inspired by the EU Model notably the Convention 108, although she says, one of its key approaches it considers is the adoption of a law that respects the needs and traditions of each country. Leclercq adds that 'the AFAPDP offers assistance to States and local authorities to develop an expertise in the protection of personal data, based on the experience of members of its network authorities.'[501]

The AFAPDP have adopted several instruments that place Francophone African countries more secured and in the global data protection map than the Anglophone African countries. In 2013 a Protocol for Cooperation was adopted to allow the AFAPDP members to exchange information in the discharge of the data protection authorities duties in light of their national law and the duty of confidentiality.[502] According to the president of the AFAPDP, the Francophones are determined to establish a framework which can facilitate cooperation mechanism to regulate international transfer within the francophone space in the absence of international regulation on international data transfer.[503] Other instruments adopted by the organization in protection of personal data includes, Madrid Declaration on protection of personal data,[504] Protocol on

---

[498] In July 2014 the organization organized training for data protection authorities on the use of BCR which were adopted in 2013 in Marrakech. In addition to this, the organization published on its website an FAQ for the multinational companies in several countries French to acquaint themselves with the procedure.

[499] ESOMAR, French-speaking African countries are adopting data protection regulation at lightning pace, Published Online 31 January 2014, at https://www.esomar.org/newsandmultimedia/news.php?idnews=133; accessed on 09/02/2016.

[500] Leclercq, F., 'A francophone BCR model to boost African data protection', Data Protection Law & Policy September 2013, p.7.

[501] Ibid.

[502] CNIL., 'Transferts de données personnelles de l'espace francophone : les autorités adoptent les règles contraignantes d'entreprise (RCE)', 26 December 2013, http://www.cnil.fr/nc/linstitution/actualite/article/article/transferts-de-donnees-personnelles-danslespace-francophone-les-autorites-adoptent-les-regles/.

[503] Data Guidance: International: AFAPDP - Francophone Summit should prioritise data protection http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2416

[504] Déclaration conjointe sur la protection des données personnelles Madrid, le 3 novembre 2009; available at http://www.afapdp.org/wp-content/uploads/2013/09/D%C3%A9claration-conjointe-RIPD-AFAPDP_Madrid_20092.pdf.

Cooperation between Francophone countries,[505]Resolution on Mass Surveillance,[506] Resolution on Ethics in Processing Health and Generic Data,[507] Resolution on Transparency of Governments in Processing Personal Data,[508] Resolution to Promote Digital Education,[509] Resolution for Sensitization of Society on Data Protection,[510] Resolution on Independence of Data Protection Authorities,[511] Resolution on the Use of French Language in Official and Non-Official Activities by the Member States,[512] this supplements a 2010 Resolution where members agreed to use French in official activities of the AFAPDP and international conferences.[513]

In 2014, the AFAPDP adopted Company Binding Rules (CRB) to allow transfer of data by companies within the francophone space and possibly with the EU members. The rules are said to have been modelled based on the same rules from the EU, but also took consideration of the developments in EU.[514] The Organization is working on creating a global framework on data protection, and have adopted the 'Strategy of the Digital Francophone: 2020' with a goal to impart an extensive knowledge on data protection within and among the Francophone.

---

[505] Protocole de coopération entre autorités francophones de protection des données à caractère personnel, Résolution 7 ème Assemblée générale de l'AFAPDP du 22 novembre 2013 à Marrakech; available at http://www.afapdp.org/wp-content/uploads/2013/09/PROTOCOLE-COOP-modifi%C3%A9-2014.pdf.

[506] Résolution sur la surveillance de masse Adoptée par la 9ème Assemblée générale de l'AFAPDP le 25 juin 2015 à Bruxelles, available at http://www.afapdp.org/wp-content/uploads/2015/07/PR_Surveillance-de-masse-26.pdf.

[507] Résolution pour la prise en compte des principes éthiques dans les traitements de données à caractère personnel dans le domaine de la santé et de la génétique Adoptée par la 9ème Assemblée générale de l'AFAPDP le 26 juin 2015 à Bruxelles, available at http://www.afapdp.org/wp-content/uploads/2015/07/PR_Ethique-sant%C3%A9-26.pdf.

[508] Résolution visant à une plus grande transparence des pratiques de collecte de données à caractère personnel par les gouvernements, 7ème Assemblée générale de l'AFAPDP, Marrakech, le 22 novembre 2013, available at http://www.afapdp.org/wp-content/uploads/2013/12/AFAPDP2013_TransparencePratiquesGouvernements_finale.pdf.

[509] Résolution pour promouvoir une éducation au numérique pour tous, 7ème Assemblée générale de l'AFAPDP, Marrakech, le 22 novembre 2013, available at http://www.afapdp.org/wp-content/uploads/2013/12/AFAPDP2013_Education_finale.pdf.

[510] Résolution pour une sensibilisation efficace de la société à la protection des données personnelles, Adoptée par l'Assemblée générale de l'AFAPDP le 31 octobre 2011 à Mexico (Mexique), available at http://www.afapdp.org/wp-content/uploads/2012/01/AG-2011_R%C3%A9solution-sensibilisation1.pdf

[511] Résolution relative à la nécessaire indépendance des autorités de protection des données personnelles, Adoptée par l'assemblée générale de l'AFAPDP le 31 octobre 2011 à Mexico (Mexique), available at http://www.afapdp.org/wp-content/uploads/2012/01/AG-2011_R%C3%A9solution-sur-ind%C3%A9pendance1.pdf.

[512] Résolution sur l'utilisation de la langue française à la Conférence internationale des commissaires à la protection des données personnelles et de la vie privée Adoptée par l'assemblée générale de l'AFAPDP le 31 octobre 2011 à Mexico (Mexique), available at http://www.afapdp.org/wp-content/uploads/2012/01/AG-2011_R%C3%A9solution-sur-utilisation-langue-fran%C3%A7aise1.pdf.

[513] Résolution de l'Association francophone des autorités de protection des données personnelles (AFAPDP) pour la promotion de l'usage de la langue française au sein des organisations et conférences internationals, Assemblée générale du 30 novembre 2010, available at http://democratie.francophonie.org/IMG/pdf/Resolution_usage_francais-2.pdf.

[514] Résolution relative à la procédure d'encadrement des transferts de données personnelles de l'espace francophone au moyen de règles contraignantes d'entreprise (RCE),7ème Assemblée générale de l'AFAPDP du 22 novembre 2013 à Marrakech, available at http://www.afapdp.org/wp-content/uploads/2013/09/RCE-modifi%C3%A9e-2014.pdf.

5.3.3.2 The EUROMED Partnership

The Euro-Mediterranean partnership came about in 1995 after the European Community adopted the Barcelona Declaration.[515] The Declaration was aimed at economic integration between the European Community and the Arab Mediterranean countries. EU being the major trade partner of the Arab-Maghreb, [516]needed to protect its markets, after its own integration in 1992 through the Maastricht Treaty. In doing so, it was inevitable to ensure the stability of her neighbors on the assumption that, without security in the Mediterranean, there can be no security in Europe,[517] hence the Euro-Mediterranean partnership.

Attempts to establish EUROMED partnership were seen as early as in the 1960s when the European Community signed a Special Association and Trade Agreement with the Mediterranean countries. In the 1970s, the European Community launched a Global Mediterranean Policy declaring the countries around the Mediterranean Sea as belonging to a single region, the Mediterranean.[518] On the African side, the Mediterranean includes Morocco, Algeria, Tunisia, Egypt and the Kingdom of Jordan.

The Barcelona Declaration enforced the previous efforts by making the EUROMED a multilateral framework with set of objectives. Together with the Declaration, the European Community introduced the European Neighborhood policy.[519] The reason for the policy is to strengthen her relation with each country individually. The ENP introduces a new aspect of legal approximation and compatibility of rules. The aim is to prepare the Mediterranean to participate in the European internal market, information society, research, innovation, social policy, people to people contracts any many other aspects.[520] In the same year, 2004, Euro-Mediterranean Parliamentary Assembly was established as a body charged with following up on the Euro-Mediterranean association agreements and to adopt resolutions for the attention of the Ministerial Conference.[521]

The ENP, according to Postolache, is different from the previous policies as the declaration is focused on issues of democracy and human rights.[522] The focus of the ENP on democracy and human right were further compounded by the adoption of Partnership for Democracy and Shared Prosperity with the Southern Mediterranean in 2011. With the two documents, the European Community shifted approach, making democracy and promotion of human right

---

[515] European Community, Barcelona Declaration adopted at the Euro-Mediterranean Conference, Brussels.
[516] For details see Maamri, N., Free Trade Areas, Euro-Mediterranean Partnership and Prospects of South-South Integration in The Mediterranean, p. 174, http://emo.pspa.uoa.gr/data/papers/7_paper.pdf accessed 26/07/2016.
[517] Adamo, K and Garonna, P., Euro Mediterranean Integration and Cooperation: Prospects and Challenges, p.75, http://www.unece.org/fileadmin/DAM/oes/nutshell/2009/9_EuroMediterranean.pdf accessed 26/07/2016.
[518] Bicchi, F., 'The European Origin of Euro-Mediterranean Practices', Working Paper No. 12, 2004, California, p.2.
[519] Before the ENP, the partnership had three aspects, (i) Political and security partnership, (ii) Economic partnership, and (iii) Social and cultural partnership. The social and cultural partnership emphasizes on, among other issues, the respect for the fundamental rights. However, this aspect was largely ignored and efforts were directed to the other two categories. See further Postolache, A., New Challenges in the Relation between the European Union and the Mediterranean, p. 5, http://www.analyticalmk.com/files/2012/01/02.pdf accessed 26/07/2016..
[520] European Community, European Neighborhood Policy Strategy Paper, Brussels, May 2004, p. 3.
[521] Adamo and Garonna (n 517), p.75.
[522] Postolache (n 519), p. 8.

priority. The objectives include support to the democratic and constitutional reforms, judicial reforms and establishment of an appropriate legal framework.

The four Mediterranean countries, have, between themselves adopted the Agadir Declaration.[523] This declaration creates a free trade zone between the countries. Furthermore, Morocco, Israel and Tunisia have an observer status at the European Commissions for the Efficiency of Justice (CEPEJ). CEPEJ helps these countries to evaluate their legal systems and guide them through reforms. This is part of the EU and CoE programme on creating efficacy legal system in the zone; towards a common legal space between the Mediterranean and the EU. The idea behind CEPEJ within the Mediterranean zone is promotion of legal harmonization of the States' legislation to match with the European and international standards and to provide support to the development and the effective implementation of new legislation in accordance with the European and other international standards according to the needs.

5.3.3.3 The Sub-Regional Economic and Development Communities

Africa as a Region has about 14 Sub-regions. However, to avoid repetition to the previous section of chapter four on Sub-regional data protection instruments, this discussion focuses on the divide on the Sub-Regional instrument. The African Sub-Regions are 'competing' and in some cases create conflicts with regards to legal reforms. On the one hand, the Sub-Regional communities are competing - and in sometime conflicting - between the need of regionalization as an instrument for development in view of globalization, and the need for reform within their respective legal models.

Decolonization in Africa and the post-independence challenges such as the territorial disputes and lack of effective Regional organ to deal with insecurity issues made it vital for the creation of, what Julian Kitipov term as 'new regional security areas'.[524] Consequently in 1967, the first Regional Economic Community, the East African Community was established. This was followed by the ECOWAS in 1975 and the SADC in 1980. As a Region, Africa has 14 Sub-regions; today each Sub-region has its own economic community; of course majority with less visibility than the few.

These RECs embrace the idea of Regional identity with varied capacities and interests. This fact alone hinders the effectiveness of the overall objective of the African Union to unite Africa as one region. The result is the failure of the African Union to collectively address matters of common concern adequately. Furthermore, there emerge tendencies within Africa to restrict flow of data by States or Sub-regional groups which have adopted data protection instruments/laws.[525] African States' domestic laws on data protection have also inhere disparities

[523] Déclaration d'Agadir instituant la création d'une Zone de Libre Echange entre les Pays Arabes Méditerranéens, 8 Mai, 2001.
[524] Kitipov, J., 'African Local Integration and Multilateralism: The Regional Economic Communities and Their Relationship with the European Union', E-paper No. 16 November 2011, p. 9.
[525] For instance, the AU Cyber Convention has under Article II-41, restriction to cross-border data flow to non-members if the non-member does not provide adequate level of protection; the same is seen in sub-regional

which Makulilo attributes to diversity in legal culture and systems, lack of Regional data privacy regime, uncoordinated Sub-regional data privacy frameworks and countries' peculiar needs.[526]

5.4 Data Protection Legal Reforms in Africa: Senegal and Tanzania in Focus

As noted in the introduction part to this chapter, Senegal and Tanzania have mixed legal systems with Civil Code and Common Law as the 'official' or the dominant legal systems respectively. Both States adopted Constitutions based on their colonial legacy. This section explores the essential characteristics of each country (with no special attention to Civil or Common Law denomination), internal and external forces to reform and any consideration made to harmonize the process with customary and local norms.

These aspects are looked against the data protection law and draft bill (the actual texts) to see whether the adopted law considers peculiarities common within specific country. This is in a view of what Mancuso insists, that, in reforming laws in Africa, 'it is necessary to arrive at the creation of an 'African law', and to avoid a fracture among different legal actors causing this new epiphany of 'African' to become yet another example of inefficient law. The main essence is to avoid the conflict in order to avoid rejection'.[527]

Although it is necessary to have a localized law, 'Globalization of law' necessitates certain legal rules and or regimes/frameworks to conform to certain standards. This is the case with data protection regimes. Data protection reforms in Africa, which began in wake of 2000s, are highly influenced by the existing international data protection codes such as the Convention 108 and the DPD. Senegalese law is said to have been highly influenced by the Convention 108 while the Tanzanian draft protection of personal data by DPD. To suffice the research quest, a brief background on privacy protection, an overview on the internal and external motivations to reforms is provided as an overview. This is followed by textual analysis of the law and the draft bill. The analysis is made as a mirror comparison between the two texts in evaluating their strength in protection of personal data and individual privacy. The mirror comparison is also conducted to test the idea of harmonization of laws being pursued in Africa as a solution to eliminate obstacles to economic development caused by judicial differences.[528] Textual analysis is also made identify incorporation (or not) of the existing legal systems (mainly customary systems) that have bearing in privacy and data protection.

---

instruments such as ECOWAS under Article 36, SADC under Article 48 (1), and even in domestic laws restricting transfer to fellow African countries which do not provide adequate level of protection.

526 Makulilo (n 26), p. 470.

527 Mancuso (n 474).

528 Allot, A.N., 'Towards the Unification of Laws in Africa', International Comparative Law Quarterly, 1965, Vol. 14, No.2, pp. 366-389; Allot, A.N., 'The Unity of African Law', in Essays in African Law, London, Butterworths, 1960, pp. 69-71, and Mancuso (n 474).

5.4.1 Privacy Protection before the Data Protection Reforms in Senegal

Located in West Africa, Senegal got her independence from France in 1960. The country introduced a single party system in 1966 with dual-parliamentary system. In 1976, Senegal introduced a restricted multiparty system of government. However, in the late 1980's Senegal reverted into a democratic authoritarianism which led to limiting citizen's and civil societies' opportunity to exercise their constitutional rights in pretext of *order publique* (public order). The semi-presidential system of government in Senegal is based on the 5th French Republic and the French Constitution of 1958. In the late 1990s, with increased power outrage and protests for social justice, Senegal was labelled an autocratic government within Africa and at international level.[529]

As the capital of French West Africa during the colonial period, Senegal was France's most important African territory. The French had a real and central presence there than in other colonies, so its culture became particularly ingrained into Senegalese life. The two countries have maintained the close ties since political independence. Senegal has maintained a positive relationship with France, and many elements of French culture introduced during the colonial period remains an important part of Senegalese identity.[530]

The Constitution of Senegal contains provisions that protect and guarantees fundamental rights and individual freedoms. However, in practice, the state of human rights is affected by the Muslim brotherhood and their religious leaders; the Marabouts. The Marabouts exert authority in legitimizing a government in power. The Marabouts acts as intermediaries on policies and government actions and mobilize electorate activities; hence possesses considerable influence on the government. They are, in turn, an essential portion of the social and political stability in Senegal. Pitifully, the interests of the Marabouts are not always and not necessarily in harmony with human rights standards and advocates for human rights.

Senegal has had only two Constitutions (with several amendments) since its independence in 1960. The Independence Constitution had under Articles 10 and 13 the right to privacy as; Article 10,

> *'Le secret de la correspondance, des communications postales télégraphiques et téléphoniques est inviolable. Il ne peut être ordonné de restriction à cette inviolabilité qu'en application de la loi.'*

Translated as: The secrecy of correspondence and of postal, telegraphic, telephonic and electronic communications, is inviolable. Restriction of this inviolability may only be ordered in the application of the law.

Article 13 provides further for the right to privacy as follows:

---

[529] Adjolohoun, H.S., 'The ECOWAS Court as a Human Rights Promoter? Assessing Five Years' Impact of the Koraou Slavery Judgment', Netherlands Quarterly of Human Rights, 2013, No. 3.

[530] Bawa, A.B., 'From Imperialism to Diplomacy: A Historical Analysis of French and Senegal Cultural Relationship' a paper presented at the London Art as Cultural Diplomacy Conference 2013 on the theme: "Contemporary International Dialogue: Art-Based Developments and Culture shared between nations" held at The Portcullis House, British Parliament from 21st to 24th August 2013.

Le domicile est inviolable.

Il ne peut être ordonné de perquisition que par le juge ou par les autres autorités désignées par la loi. Les perquisitions ne peuvent être exécutées que dans les formes prescrites par celle-ci. Des mesures portant atteinte à l'inviolabilité du domicile ou la restreignant ne peuvent être prises que pour parer à un danger collectif ou protéger des personnes en péril de mort.

Ces mesures peuvent être également prises, en application de la loi, pour protéger, l'ordre public contre des menaces imminentes, singulièrement pour lutter contre les risques d'épidémie ou pour protéger la jeunesse en danger.

Translated as: The domicile is inviolable.

[A] search may only be ordered by the judge or by the other authorities designated by the law. Searches may only be executed in the forms prescribed by them. The measures infringing the inviolability of the domicile or restricting it may only be taken to evade a collective danger or to protect persons in peril of death.

These measures may be taken equally, in the application of the law, to protect the public order against imminent threats singularly to combat the risks of an epidemic or to protect youth in danger.

In 2001, Senegal introduced a new Constitution; retaining the semi-parliamentary system (with dual executive: Head of State and the head of government) although the President is 'the first and the last resort of all the institutions. He is the unquestionable head of the executive, and he supplants all the other powers. The President controls all the institutions, and even independent administrative bodies.....the president outweigh all the institutions. He dominates the legislature, overshadows the judiciary, and does not spare any sector of the nation's life. The presidential mandates are based on the powers of the President as provided by the Constitution under Articles 38, 42-52.

However, this situation may change when Senegal adopts a new Constitution as proposed by the Senegalese National Commission for Institutional Reforms. In 2013, this Commission reviewed the status and constitutional separation of power. Eventually, the Commission came up with *Avant Project De Constitution* (Draft Constitution) suggesting a new framework for separation of powers between the three organs of the State. The Draft, among other recommendations, suggests counter assignment of President powers by the Prime Minister.[531]

The Constitution in 2001 made changes to the judicial system; it removed the Supreme Court and introduced, in its place, the Supreme Court of Appeal, the Council of States, the Constitutional Council and the Accountability Court; the system which resembles the French system.

Of more relevance in the present context is the Constitutional Council. The Constitutional Council was created as an instrument for the protection of citizens' rights and freedom. The Constitutional Council is argued to have been set up in order to re-adjust the country's situation

[531] See more elaboration by Kamga, S.D., 'An Assessment of the Possibilities for Impact Litigation in Francophone African Countries', AHRLJ 2014, Vol. 14, 2014, pp. 449-473 at p. 458.

to meet international obligations and democratization of Senegal (among other things).[532] The composition of the Council requires 3 judges with at least 25 years working experience. They are presidential appointees from the list of six suggested judges by the Superior Council. One of the appointees must be a person recommended by human rights association who are required to submit a list of three nominations. The idea behind is to have a panel of judges from diverse sources for independence in decision making.

The 2001 Constitution maintained the right to privacy as was in the 1963 Constitution, word for word. The only change is that the right to privacy is now provided under Articles 13 and 16 instead of 10 and 13 respectively. The right to privacy in Senegalese Constitution (along with other rights and freedom in the Constitution) is argued to have been profoundly influenced by the French Civil Rights Code of 1883.[533] The right to privacy, as provided in the Constitution also reflects other international Covenants and Conventions which Senegal has acceded including Article 12 and 17 of the Universal Declaration of Human Rights and the Convention on Civil and Political Rights respectively.

It is prudent to note here that, in Senegal, international law takes precedence over domestic law. Hence on the right of privacy, Senegal would resort to provisions in the international Covenants and/or Conventions she has acceded to and approved, whenever they are in conflicts with domestic laws. This is according to Article 98 of the Constitution which states;

> *Les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie.*

Translated as:

Treaties or agreements duly ratified or approved shall, upon publication, an authority superior to that of laws, subject, for each agreement or treaty, to its application by the other party.

As mentioned previously the section's introduction, the 2011 Constitution also established a Constitutional Council (CC) for the enforcement and protection of citizens' constitutional rights and fundamental freedoms. The Constitutional Council is also mandated by Articles 74 and 75 to check the Constitutionality of all Bills before they are signed into laws by the president. The Council is to ensure that international obligations are adhered to. Through this power, all laws are required to be submitted to the CC for review before the second reading in the National Assembly to determine its constitutionality before any Bill is pronounced into a law. However, the president is empowered to seize the CC declaring a law unconstitutional six days after he has received the law passed by the National Assembly. The same powers are given to the National Assembly when such seization is by one-tenth of the members of the National Assembly.[534]

---

[532] Baldé, V.S., *Juge constitutionnel et transition démocratique. Etude de cas en Afrique subsaharienne francophone,* 2010. Available at http://www.etudier.com/dissertations/Tmp-3560-279828323162/73237300.html Accessed on 05.04.2017.

[533] Getz, R.T., Slavery and Reform in West Africa: Toward Emancipation in Nineteenth-Century Senegal and the Gold Coast, Ohio University Press, 2004.

[534] Article 74 of the Senegalese Constitution.

The Constitution also gives individual citizen the right to raise unconstitutionality of law. This can be done either incidental or *in conreto* during case hearing. A person may raise unconstitutionality of the law when s/he believes such law is in breach of the constitutional principles. Furthermore, it should be understood that, through Article 92 sub article 1 of 3 of the Constitution, citizens can make an application to the CC to enforce their constitutional rights and freedoms.

The CC has already made a number of decisions on political rights and electorate rights.[535] Unfortunately, until the final preparation of this thesis, there has been no case of the breach of the right to privacy or data protection concluded. Apart from the CC, infringement of the right to privacy in Senegal calls for criminal prosecution under the Senegalese Criminal Code which was also amended in 2008 to incorporate cybercrimes. The amendment creates a new Part III to the Criminal Code and introduces offences relating to Information and Communications Technology.

5.4.2 Privacy Protection in Tanzania

Tanzania is located in the Eastern of Africa along the Indian Ocean and within African Great Lakes region. Tanzania is the United Republic of two formerly sovereign States namely; the Republic of Tanganyika and the People's Republic of Zanzibar. This makes Tanzania a peculiar jurisdiction when it comes to law making and legal reforms.

Tanganyika got her independence on 9th of December 1961 and became Republic in 1962. Zanzibar got her independence on 10th of December 1963, and the People's Republic was established after the revolution of Zanzibar of 12th of January 1964. The union of the two States took place soon after the revolution of Zanzibar in 1964 and formed one State, the United Republic of Tanzania. The Union State has two governments, the United Republic Government and the Revolutionary Government of Zanzibar. However, the Union did not extinguish the sovereignty of Zanzibar, because, unlike Tanganyika, Zanzibar retains its own Constitution.

The Constitution of the Revolutionary government of Zanzibar provides for non-Union matters.[536] This means, the United Republic of Tanzania has two organs of government both with judicial, legislative and supervisory powers.[537] The Union government and its organs has power over the whole territory in all Union matters, while the judiciary of the Revolutionary government of Zanzibar and the House of Representative have power limited to non-Union matters in and for Zanzibar; within its Constitution. However, laws passed by the Union Parliament do not apply to Zanzibar without an express provision in that behalf[538] or unless the law relates to Union affairs and is in compliance with the provisions of the Union

535 Kanté., B., *Les Méthodes et techniques d'interprétation de la Constitution : l'exemple des pays francophones », in l'interprétation constitutionnelle, (Soucramanien)*, Paris, Dalloz, 2005, p.157 in Madior, F.I., *Evolution constitutionnelle du Sénégal - De la veille de l'Indépendance* aux elections de 2007, 2009. p.79

536 See Maina, C.P and Othman, H., Peter C M Othman H (eds.) Zanzibar and the Union Question, Zanzibar Legal Services Centre, 2006, p. 2.

537 These powers are provided by the Constitution of United Republic of Tanzania under article 4(1)(2) and articles of Union between United Republic of Tanzania and People's Republic of Zanzibar of 1964 article 111 (a).

538 Nchalla, B. M in Mbondenyi and Ojiende, (n 296), p. 15.

Constitution.[539] [540] Therefore, Zanzibar has her own laws passed by the House of Representative in Zanzibar.

In 1961, when Tanganyika got her independence from the British, the British did not (unlike with her other colonies) impose into Tanganyika the British Constitution model. Nevertheless, Tanganyika adopted the Constitution in a Westminster tradition with the government organs accountable to the National Assembly. The first Constitution, the Independence Constitution of 1961 excluded the bill of rights. This model of government lasted for one year when Tanganyika resorted to a presidential system through the Republic of Tanganyika Constitution (Constituent Assembly Act No. 1 of 1962). This was the second Constitution of the Republic of Tanganyika, also excluding the bill of rights as its predecessor. The Republican Constitution of 1962 created a Republic government. In 1964, with the Union of Tanganyika and Zanzibar, Republican Constitution was modified to cater for the Union government.

The then President, the late Julius Kambarage Nyerere passed an Interim Constitutional Decree, renaming the Constitution as an 'Interim Constitution of United Republic of Tanganyika and Zanzibar of 1964.[541] This was the third Constitution of Tanganyika and the first Constitution of the United Republic of Tanzania. In 1975, the Interim Constitution was amended.[542] The amendment did not consider an introduction of the bill of rights; rather, it introduced a single party political system (with party supremacy). Consequently, merging the two ruling parties (TANU in Tanganyika and ASP in Zanzibar) to form a single party. The merger gave rise to a new party, *Chama Cha Mapinduzi (CCM)* in 1977. In the same year, Tanzania adopted its fifth and permanent Constitution namely, the Constitution of United Republic of Tanzania of 1977.[543]

The 1977 Constitution included the bill of rights in the preamble. According to the common law tradition to which Tanzania is ascribed to, preambles have no legal force; hence, no one could enforce any right enshrined in the preamble.[544] This was a political move in response to mounting critics by the international society on Tanzania's failure in her obligations under the UNHRC. Jennifer Widner[545] explains, that the inclusion of the bill of rights was a way of Tanzania to illustrate her commitment to human rights since she used the umbrella of human rights to achieve her political goals such as the 'use of human rights language to galvanize international opinion against Idi Amin of Uganda (to help expel his forces from Tanzania). Yet is the fact that Tanzania was involved in development of African Charter on Human and People's Rights as such, it was essential for her to portray her commitment to the individual rights.

539 Articles 64(4) (a) 6 and (5) Constitution of United Republic of Tanzania, 1977 (as amended); Article 132 (1) (2) Constitution of Zanzibar Revolutionary Government, 1984 (as amended).

540 Union Constitution is the Acts of Union- The treaty which united Tanganyika and Zanzibar. This treaty was translated into domestic laws in Tanganyika the enacted law is the Union of Tanganyika and Zanzibar Act of 1964 (Act 22 of 1964) and for Zanzibar is the Union of Zanzibar and Tanganyika Law 1964. The two laws constitute Constitution of the Union.

541 This was through Act no. 43 of 1964.

542 Amendment was done through Interim Constitution of Tanzania (amendment) Act of 1975.

543 This is the current Constitution although several amendments have been made to it since its adoption to accommodate socio-political and economic changes.

544 Maina, C. P., Tanzania in Heyns, C., Human Rights Law in Africa 1997: Volume 2, Kluwer Law International: Netherlands, 1999. Pp. 282-288 at p. 284.

545 Widner, J., Building the Rule of Law: Francis Nyalali and the Road to Judicial Independence in Africa: NY-Norton, 2005.

In 1984, the Constitution was amended for the fifth time.[546] The Fifth Amendment gave bill of rights the force of law by introducing a new part III containing fundamental rights and individual duties. Sadly, its was suspended for three years, as Chris Peter Maina puts it, 'to allow the government put its house in order, repealing or amending laws which were likely to conflict with the bills of rights.[547] In March 1988, the bill of rights became operational, with the right to privacy among the guaranteed and protected rights. The same bill of rights was adopted in the Constitution of Revolutionary Government of Zanzibar in 1985. Accordingly, the right to privacy is provided under Article 16 (1) (2) of the United Republic of Tanzania Constitution; and Article 15 (1) (2) of the Revolutionary Government of Zanzibar Constitution in *pari materia* with the United Republic of Tanzania Constitution.

The constitutional right to privacy as provided is not an absolute right and its implementation depends on other pieces of legislation to provide for the substance of the right and enforcement mechanism. This is also clearly stated in a subsection 2 to articles 16 and 15 of the aforementioned Constitutions. The right is also limited by other provisions in the Constitution. These provisions further subject the enforcement of the right to the 'principle of proportionality'. Its enforceability is scaled with other constitutional rights and can be derogated in protection of national security and preservation of public safety.

Article 16 provides;

> 16.-(1) every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.
>
> (2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.[548]

The constitutional right to privacy is further limited by Article 30 of the Constitution. This section allows enactment of any other law in violation of the bill of rights for the interest of general of public (such as public safety, to maintain public morality, in the process of rural or urban planning or exploration of oilier interests), in execution of Judgment or Court order, protecting reputation, rights and freedom of others.

Precisely 10 years after the inclusion of bill of rights into the Constitution, the government enacted a law to enforce them. The Basic Rights and Duties Enforcement Act,[549] enacted in 1994 provides for mechanisms and procedure to enforce constitutional bill of rights. Section 1 (2) of this Act provides for the scope of application stating; 'this law applies to mainland Tanzania and Zanzibar in all suits relating to enforcement of constitutional basic rights, duties and related

546 This was through Act No. 15 of 1984.
547 Maina, C. P., Tanzania in Heyns, C., Human Rights Law in Africa 1997: Volume 2, Kluwer Law International: Netherlands, 1999. Pp. 282-288 at p. 282
548 See Article 16 (2) and 15 (2) of the Constitution of United Republic of Tanzania and Constitution of Revolutionary government of Zanzibar respectively.
549 Act No. 33 of 1995.

matters.[550] The Act is basically a procedural law, setting rules on composition of the judges, the majority rule in decision making,[551] and mode of instituting a complaint[552] as well as proper forum for redress.[553]

Surprisingly, the Act introduces a provision limiting the powers of the High Court to enforce bill of rights. The provision states, 'where the Court is satisfied that individual rights have been infringed by an action or law it should not pronounce such an act or law as being unconstitutional or invalid rather it should allow the Respondent or specific authority to rectify the infringement. If a law is in conflict with the Bill of Rights the Court should not declare such law as being invalid or unconstitutional. Such law will remain valid until the parliament amends or repeals it'.[554] The provision is in contradiction with another Constitutional provision; Article 65 (4) which empowers the High Court to declare any law unconstitutional or void.

Interesting is the fact that the Constitution was then amended, introducing Article 30(5) which is in *pari materia* with Section 13(2) of the Act. The article requires High Court not to declare any act or law void or unconstitutional even when its determination is to that effect. Instead, the Court is required to afford the infringing organ opportunity to rectify the infringement.

The judiciary resisted and declared the provisions as an obstacle in the pursuit of individual rights and freedom.[555] Consequently, in 2000, it was declared, through Article 65(4) of the Constitution, the judiciary has the final say on matters of determining rights and duties according to law and justice; however, Article 30 (5) was not deleted from the Constitution.

No substantive law on the rights and basic duties, (or right to privacy) has ever been enacted to provide context or substance of the rights. As a result, most people ends up airing their grievances, anger, dissatisfaction and concerns in blog discussions and other interactive social media. A few resort to newspapers.[556]

In 2002, the government of Tanzania once again amended her Constitution for the 13th time. Through this amendment, the Constitution established the Commission for Human Rights and Good Governance. The Commission was established as the national focal point for the promotion and protection of human rights, duties and good governance. According to Section 3,

---

550 Parallel to this provision, the Constitution of Revolutionary Government of Zanzibar provides, under article 25A, procedure for enforcement of the basic rights and duties in Zanzibar.

551 Section 10.

552 Section 5.

553 Section 4.

554 Section 13(2).

555 In 1998 the Court of Appeal of Tanzania, stated the section 13 (2) of the Basic Rights and Duties Enforcement Act seek to circumscribe the powers of the High Court in dealing with issues of fundamental rights and duties. The Court departed from section 13 (2), despite their duty to give effect to plain words, The Court opined that it would be meaningless for the Courts to refrain from declaring laws or actions that goes against human rights as void or unconstitutional. Further, enforcing of this provision is a contravention to article 170A (2) (b) of the Constitution of United Republic of Tanzania. See also *Adam Mwaibabila v. The Republic, High Court of Tanzania* at Dar es salaam, Miscellaneous Criminal Case No. 1 of 1997, unreported; see also *A.G v. Christopher Mtikila* [1995] T.L.R 3

556 One such instance was featured in Arusha Times with headline 'SIM card registration now viewed as spying move'. The Citizen also published a complaint letter from a reader titled, 'Airtel are bothering me with unwanted text messages'. The reader being annoyed by promotional text messages said the telecom company is invading his privacy urging the company to provide an 'opt in/opt-out' choice to avoid annoying their customers. Other publications on concerns over privacy breaches include 'the Big Brother is Watching You' in Daily news of 12th February 2009.

the Commission has mandate in both Tanzania mainland and Zanzibar.[557] Regrettably, the Commission brought no changes on the right to privacy as with the other rights.[558] Even in her submissions to the United Nations General Assembly, Tanzania's report did not include the right to privacy among the key national priorities, initiatives and commitments she undertook to improve.[559] More surprisingly is the fact that, the UN summary of recommendations on Tanzania report did not show any concern on the omission in relation to the right to privacy. This is despite the fact that the UN Recommendation report contains a specific section titled, 'Right to privacy, marriage and family life'. However, there is no mentioning of the right to privacy; neither the situational analysis nor recommendations for improvement.[560]

This indicates, as Makulilo asserts, 'privacy is less prominent a public issue in Tanzania'.[561] Although he agrees that there is a growing concern over privacy reflected from isolated cases; citing an example of the debates that emerged during introduction of compulsory SIM card registration in 2009. Perhaps Makulilo assertion indicates the outcome of the first ever case to reach the High Court. This was in 2004. It was a case where local Newspaper used images of a young lady, namely Siah Nyange. Miss Nyange participated in Miss Tanzania beauty pageantry. The Newspaper used her images for commercial advertisement without her knowledge or consent. Miss Nyange instituted a civil suit for violation of her right to privacy.[562] Many had hoped that the High Court would, for the first time, lay some basic principles or guidelines underlying the protection of privacy in Tanzania. Unfortunately, the Court did not adjudicate the case to its finality as the newspaper company requested to settle the matter out of Court and ended up compensating Miss Nyange.

The Media Council of Tanzania is so far the only forum which went a step further in asserting the right to privacy. This was in the Conciliation case of *Mkami Kasege and Ismail Msengi v. Risasi.*[563] In this matter, the Complainant approached the Council claiming violation of her right to privacy and damage to reputation caused by false and malevolent publication by a local Newspaper, namely, *Risasi.* The Newspaper published an article saying the Complainant is involved in extra

557 Section 3.

558 In the National Report on Tanzania Human Rights Institutions submitted to the Human Rights Council for Universal Periodic Review, the Commission is shown to have dealt mainly with maladministration issues than personal rights. [see UNGA., Individual Report of the Tanzania National Human Rights Institutions-Submission to the Human Rights Council: Universal Periodic Review, 12th Session 2011; Joint Stakeholders' (CSOs) Submission to the Human Rights Council- Universal Periodic Review Mechanism, 12th Session, 2011].

559 UNGA, National Report Submitted in according with para 15(a) of the Annex to the Human Rights Council Resolution 5/1- United Republic of Tanzania, Geneva, 3-14 October 2011, p.5.

560 UNGA, Summary Prepared by the Office of the High Commission for Human Rights in accordance with paragraph 15 (c) of the annex to Human Rights Council Resolution 5/1, Geneva, 3-14, 2011.

561 Makulilo (n 26), p. 534.

562 *Siah Dominic Nyange v. Mwananchi Communications Ltd*, Civil Case No. 155 of 2005; The Resident Magistrate Court of Dar es salaam at Kisutu (unreported).

563 Conciliation Case No. 1 of 2005, 1997-2007, MCT 111. A complainant instituted a claim against Risasi newspaper for publishing her semi-nude photographs. The article concerned alleged that the complainant was involved in an adulterous act against her husband. The complainant who is a University lecturer was concerned of the photographs which were published as being invasive of her privacy and damaging to her reputation. The Council conclusion was that the allegations were false and in violation of privacy and code of ethics for media professionals. The Council explained further that, even to public figures, it is only acceptable to intrude into ones privacy when it is absolutely necessary for public interest. The Council then ordered the editor of the newspaper to retract the story, apologize to the complainants and pay the costs of the case incurred by the complainants. Sadly, the council decision and orders were ignored. Perhaps because the Council is only a voluntary, self-regulatory body without powers to issue legal binding decisions. It has only reconciliatory powers.

marital affairs and had been caught ready-handed. This article was followed by another publication by the same Newspaper claiming the Complainant to have tried to commit suicide out of shame. The publications were accompanied by semi-nude photos of the Complainant which devastated the Complainant and which she considers to be in violation of her personal privacy.

The Council summoned both parties for a hearing, but the representatives from the Media Company did not attend. This forced to Council to continue *ex-parte* with the Complainant. The Council decided for the Complainant based on the Code of Ethics for Media Professionals. The Newspaper was found in breach of Complainant's privacy. The Council ordered the Newspaper to issue an apology to the Complainant, retract the story and pay for costs incurred by the Complainant. Sadly, the Media Council of Tanzania being a voluntary, self-regulatory body can only reconcile parties; it has no powers to issue a binding legal decision. Hence, the Media Company ignored the order, and the matter ended with no reparation to the Complainant.

5.4.3 Motivation to Data Protection Reforms in Senegal and Tanzania

Greenleaf and Georges posit that the motivation behind the adoption of data protection laws in Africa is the growing use of computers in routine States' activities, increased use of biometric IDs and increased operations of private entities outsourcing activities from EU countries; giving an example of the Mediterranean countries.[564] The authors are not too far from the truth, although, the former, may not be an immediate motivation or rather not a primary concern. The Malabo Convention is repeatedly pronouncing in the preamble that its objective is to set forth rules essential for establishing a credible environment for electronic transactions and combating cybercrimes. Reference to the protection of human rights and fundamental freedom is made in association with 'facilitating trans-border commerce'. The same pattern is seen in the report from the UNCTAD ECOWAS conference in harmonization of cyber legislation in Africa in stating;

> 'While noting the dangers facing personal data with emerging technology and cloud computing, members unilaterally agreed that, there are different cultural approaches to privacy. However; the need to adopt data protection legislation is linked to the transnational nature of internet and the information economy. In order to benefit from the off shoring or business processing outsourcing involving data processing, countries need to have some form of data protection law'.[565]

Furthermore, the National ICT policies also advocate for reform in the present legal framework for privacy and data protection, cyber-crimes, e-commerce and e-contracts.[566] However; the motivation stated in these policies are merely economic reasons and not focused on individual rights and or freedoms. In Tanzania, for instance, the policy narrates that the reforms are important for economic development. In Senegal, the National ICT Policy and the National

[564] Greenleaf, G and Georges, M., African regional Privacy Instruments: their effects on harmonization, PL&BIR, December 2014, pp. 19-21 at p. 19.
[565] UNCTAD, Review of e-commerce legal harmonization in economic community of West African states, Switzerland, 2015., p. 77.
[566] URT, 2003; Paragraph 3.5.

Science and Technology Policy were both drafted as part of the poverty reduction strategy documents which were adopted in 2002.[567] The dominating objectives in both policies are the massive use of the ICTs for economic development. Therefore, legal reforms in privacy and data protection are considered as a means to an end, that is, to facilitate 'massive' use of the ICT for the economic development and modernization through trade beyond local borders.

Tanzania commence the reforms after resolving that the existing laws, including the Records and Archives Management Act[568] which provides the legal framework within which records and archives should be managed, needed to be reviewed, taking into account electronic record issues as well as access to information and data protection.[569] In essence, there was a need for a law to secure personal data and activities in the cyber space to allow electronic transactions and achieve economic growth.

At the Regional level, Tanzania is a member of the East African Community (EAC) and the South African Development Community (SADC). In 2006, the Council of Ministers of the EAC launched an eGovernment programme. The programme discussed strategies for legal reforms to secure online transaction. The Council suggested reforms of the Regional and national legal frameworks to ensure security in online transactions and interactions. This was part of the East African Development Strategy (2011/12 – 2015/16).

One of the key drivers in the realization of the EAC regional integration agenda is the creation of a strong legal framework to realize full potentials in regional eTransactions. Based on this, the Council created EAC Task Force in 2008 to implement Council resolutions. The Task Force developed two instruments; the Legal Framework for Cyber Crimes phase I and II of 2008 and 2010 respectively. Phase I suggested legal reforms on eTransaction, Cyber-Crimes, Consumer Protections, Data Protection and Privacy. Phase II suggested legal reforms on Intellectual Property Rights, Competition, Taxation.

On privacy and data protection, Phase I, on recommendation 19 states;

> 'The Task Force recognized the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area'.

Unlike the other Regional instruments, the EAC Frameworks do not provide any 'framework' or model law for the Member States to draw inspirations from. It merely urges the Member States to reform their data protection and privacy frameworks based on international best practice. On other legal topics, the Framework has attached, as annexes, some models as examples for the

567 Thiam, N. F. G., ICT in Senegal: Management, Public uses and Perspectives, GOVTECH Conference, 5-8 September 2010, Durban-South Africa.
568 Act No. 3 of 2002.
569 URT, Proposal for Enacting Cyber Laws in Tanzania, Dar es salaam, January 2013, p. 3; See also Report by IRMT, Fostering Trust and Transparency in Governance: Investigating and Addressing the Requirements for Building Integrity in Public Sector Information Systems in the ICT Environment the case study of Tanzania, January 2007.

best practice. However, for unexplained reasons, on privacy and data protection, the Framework neither suggested nor attached a specific sample model considered as 'international best practice'.

On the other hand, SADC adopted SADC Model Law on Data Protection in 2012. The primary objective of the Model Law as it can be inferred from the 'preamble' is harmonization of data protection law of Member States. The Model Law adopts a comprehensive framework for data protection, similar to that of the DPD and other international codes.

In 2013, Tanzania embarked on the legal reform process with the aim of transposing the SADC Model Law into a domestic law. The process was initiated by HIPSSA.[570] Through the HIPSSA project, and with financial, technical and expert support from the ITU, European Commission and the European Union,[571] Tanzania produced her first comprehensive data protection draft bill titled 'Draft Privacy and Data Protection Bill', which was in 2014 renamed to 'Draft Personal Data Protection Bill'.[572]The bill applies to Tanzania Mainland only.[573] The draft bill was drafted within the six identified areas that needed legal reforms; these includes computer security against unauthorized access or modification, data protection, guidelines for processing personal data, legal recognition of eTransations and eCommerce, framework for legal obligations for online suppliers, protection of online consumers and retention of electronic records[574]

Prudence dictates a little explanation on the route taken in drafting the draft bill. In Tanzania, all legal reforms are conducted by the Law Reform Commission. However, in an unusual manner, the reform process was overtaken by the Ministry of Communications, Science and Technology. Another surprising fact is non-involvement of the public. It is standard practice, by the Law Reform Commission to upload draft bills on their website for the public to view and participate in the process; a very important aspect that gives the public a feeling of ownership; hence, acceptance of the proposed regulatory changes. The Ministry did not follow this approach. Only a few selected 'stakeholders'[575] were selected as representatives of the public. Surprisingly, the Law Reform Commission was not involved or consulted as one of the stakeholders.

According to Ephraim Percy Kenyanito and Raman Jit Singh Chim[576] the HIPSSA projects for the harmonization of ICT laws, under the ITU were, first carried without public consultation and second they were adopted as Reference Framework for Harmonization of the telecommunication and ICT Policies and Regulation in Africa by Ministers of ICTs for the

[570] The Support for the Harmonisation of the ICT Policies in Sub-Saharan Africa project.
[571] ITU., 2013.
[572] This was after the review of the initial Draft by Local and International consultants, including those coming from the ITU.
[573] Zanzibar is yet to embark into Data Protection Legal Reforms.
[574] Ministry of Communications, Science and Technology, 2013.
[575] The selected stakeholders includes the President's Office – Planning Commission, the Ministry of Constitutional Affairs and Justice, the Ministry of Finance-Mainland, the Ministry of Finance Zanzibar, the Ministry of Science and Technology, the Ministry of Communication and Transportation, the Ministry of East African Community Cooperation, the Tanzania Bankers Associations (TBA), Commercial Banks, Mobile Network Operators (Vodacom, Airtel, Tigo, Zantel), Savings and Credit Cooperatives Union League of Tanzania (SCULLT), Tanzania Association of Micro Finance Institutions (TAMFI), The Fair Competition Commission (FCC), Tanzania Consumer Advocacy Society, Tanzania Revenue Authority (TRA), Tanzania Communication Regulatory Authority (TCRA), and the Financial Intelligence Unit. See the Ministry of Communications, Science and Technology Report.
[576] Kenyanito, E. P., and Singh, J. R., Chim Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa, December 2016, Access Now.

respective Sub-Saharan States.[577] Consequently, the Ministers undertook to implement this 'project' as Ministerial projects rather than handing over the task to the law reform authorities.

In Tanzania, the whole process was conducted in confidential; no person, apart from the selected stakeholders' had access to the text. It took extra effort to acquire the text for the analysis in preparation for this project. However, in 2016, the Ministry, for undisclosed reasons, handed over the draft bill and all the process to the Law Reform Commissioner. The Commissioner, for the first time, published the draft bill on their website and local Newspaper, seeking public consultation.[578]

Senegal enacted a comprehensive data protection law in 2008, although its implementation was 'suspended' to 2011 for lack of funds. According to Professor Abdoullah Cissé, the process in construction of the data protection legal framework was participatory and inclusive. The approach was ideally to align the new framework with political institutions, economic, social structures and local mentality. This was necessary to overcome potential resistance to the framework. Cissé explains further that, the process was also constructed keeping in mind the existing tension between economy and human rights.[579] Accordingly, the involvement of international organization such as the AFAPDP had in mind a framework that supports not only the compliance to human rights in the processing of personal data, but also the acknowledgement and preservation of principle social values;[580] a fact also affirmed by the AFAPDP manager Mmde Leclercq.[581]

According to Cissé, the created framework for data protection in Senegal insisted on the law that gives judges a room for interpretation of the principles in the protection of personal privacy rights in data while keeping in mind the pluralistic nature of the legal system.[582] This is surprising, considering Senegal conventionally follows a Civil Code Legal culture.

The law and the draft bill both apply to the processing of personal data in both public and private sector whether or not processed by automated or by manual means.[583] While the draft bill applies to personal data regardless of format or media,[584] the law is quite on its applicability regarding data formats or processing media.

Scope and Purpose Both the Senegalese law and the Tanzanian draft bill have the aim to stop a breach of privacy that may occasion through collection, processing, transmission and use or re-

[577] Adopted in Cairo in the year 2008 during the 2nd Conference of African Ministers in charge of Communication and Information Technologies (CITMC-2).
[578] See http://www.lrct.go.tz/ and The Daily News of 15 August 2016.
[579] Cissé, A., Séminaire Informatique et liberté Quel cadre juridique pour le Sénégal ? Éléments de synthèse, Séminaire Informatique et liberté Quel cadre juridique pour le Sénégal ? Éléments de synthèse.
[580] Ibid.
[581] Leclercq, F., A francophone BCR model to boost African data protection, Data Protection Law & Policy September 2013, p.7.
[582] Ibid.
583 Article 2 of the law and Section 5 (4) of the draft bill.
[584] Section 2 of the draft bill "applies to data notwithstanding format or media, and whether printed, taped, filmed, by electronic means or otherwise. According to the draft bill, data can be in form of a map, diagram, photograph, film, microfilm, videotape, sound recording or machine readable record."

use of personal data.[585] The Senegalese law, unlike the draft bill, goes further stipulating the essence of the law, that is, to ensure the processing of personal data and ICT do not affect fundamental rights and freedoms of natural persons including the right to private life and the rights of the communities.[586] As such, the law calls for the treatment of personal data in accordance with the rights, freedoms and individual dignity keeping in mind the proportionality principle.[587]

Personal data The law considers as personal data, any information which can enable identification of a natural person either directly or indirectly. Article 4 of the law describes personal data as any data that can allow identification of a person, direct or indirect, either by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, mental, cultural, social or economic identity.[588]Similarly, the draft bill has, under Section 4 defined personal data as any data which can be used to identify a person, direct or indirect, 'in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity'. The draft bill provides that, to determine whether a person is identifiable, one should look at 'all the means reasonably likely to be used either by the controller or by any other person to identify the said person.'

Sensitive data Data concerning philosophical, political opinions, religious activities, sexual life, race, health, criminal records and prosecution and administrative sanctions is considered to be sensitive data under the law.[589]Under the draft bill sensitive data contains similar contents as the law but extends the list to includes genetic and biometric data, data related to children, data on security measures and any data if its processing would reveal ethnic origin, affiliation to trade union membership, gender and any personal data otherwise considered by Tanzanian laws as presenting a major risk to the rights and interests of the data subjects, in particular, leading to unlawful or arbitrary discrimination. Accordingly, the draft bill prohibits processing of sensitive data.[590] Sensitive data can only be processed when it is necessary to undertake legal obligation (for instance, under employment laws or in promotion of human rights), or when data subject has given consent to the processing or when such data has been made public by a data subject.[591] However, depending on the nature and extent of sensitivity of the data, the Commissioner may still prohibit the processing of such sensitive data regardless of the consent to process given by the data subject. Similar restrictions are found in the law under Articles 40 and 21 (4).

One thing the law is clear on is the fact that its application is limited to natural persons. On the other hand, the draft bill definition of a person lacks clarity. It is unclear as to who the data subject is, and whether or not it applies to juristic persons. Personal data is defined as, 'data

585 Article 2 Senegal Law and section 3 Tanzania of the draft bill.
586 Article 1.
587 Section 1.
588 Article 4 (6).
589 Article 4 (8)
590 Section 4 of the draft bill provides categorizes sensitive data into two categories; first category includes genetic data, data related to children, data related to offences, criminal sentences or security measure, biometric data as well as, if they are processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life. The second category comprises of any personal data otherwise considered by Tanzanian law as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.
591 Section 16 (2).

about an identifiable person that is recorded in any form'.[592] The use of the term 'identifiable person'[593] makes it difficult to ascertain whether it extends to juristic persons or even dead persons. The definition of data subject does not offer much assistance either; it refers to data subject as, 'an individual who is subject to the processing of personal data and who is identified or an identifiable person'.[594]

The law defines data controller as any person, legal or natural, public or private body who alone or jointly engages in the processing of personal data and determine its purposes. The draft bill provides for similar definition, except, it excludes from the list 'private bodies'.[595] Whether or not the omission in the draft bill is intentional, the implication is that, when a private body processes personal data, the application of the proposed law is ousted. It simply means, private bodies are given a free pass to process personal data in disregard of the law. Looking further on the definition of a data processor, the draft bill makes the same omission. It defines a data processor as any natural, legal or public body processing personal data for and on behalf of the controller, under controller's instructions, except for persons who, under direct authority of the controller are authorised to process the data.[596] The law does not have the term 'data processor'; instead, it has used a different connotation, 'subcontractor'.

The law defines a filling system as a structured set of data accessible according to specific criteria, whether centralized, decentralized or dispersed based on function or location.[597]The draft bill neither mentions nor defines filling systems.

Jurisdiction of the laws The draft bill applies to processing activities by a controller *domiciled* in Tanzania or a controller, though not *domiciled* in Tanzania has processing activities in Tanzania. The later applies only when the processing activities are not for purposes of a mere transit through Tanzania. The draft bill also applies to processing activities in any State that Tanzanian law applies by virtue of international law.[598] The law applies whenever processing of personal data is done by controller whether or not *established* in Senegal, as long as the *means of processing* is located in Senegalese territory. It also applies to any place where Senegalese law applies by virtue of international law. The law does not apply to processing of personal data by means located in Senegal, if the processing is solely for purpose of mere transit. However, in this case the law requires the controller to designate a representative established in Senegal.

Third Countries The law considers all countries other than Senegal as third countries. It does not matter whether or not such country is within African region or ECOWAS Sub-Region where Senegal is a member.[599] The Draft Bill is quite on who are considered as third countries.

---

592 Section 4.

593 Section 4 defines identifiable person as, 'identifiable person" is an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person'.

594 Section 4.

595 See article 4 of the law and section 4 (15) of the draft bill.

596 Section 4 of the draft bill.

597 Article 4 (10) of the law.

598 Section 5 (4) (b) (c).

599 Article 4 (2).

Conditions for Lawful Processing Processing activities in both the law and draft bill are categorized into two; general and sensitive personal data processing. The condition for processing of general data under the draft bill requires that the collection of personal data to be lawful. Section 6 states;

> '6. (1) A data controller shall not collect personal data unless:-
>
> (a)the personal data is collected for a lawful purpose directly related to a function or activity of the data controller; and
>
> (b) the collection of the data is necessary or incidental for, or directly related to, that purpose.'

It follows therefore, as long as personal data is considered to have been lawfully collected, processing activities can proceed without any further requirements such as consent or fairness. Although with regards to fairness, it may be argued that, the fact that the draft bill requires personal data be collected direct from the data subject or data subject to be informed of any collection of his/her personal data as soon as practicable to have fulfilled this aspect.[600] This as seen in chapter two, may be interpreted to mean 'fairness' in collection as the case with the UK DPA and subsequent clarifications by the ICO even when the word is not explicitly provided. The only instance data subject's consent is required under the draft bill is when data controller wishes to process the data for purposes beyond the initial communicated purposes.[601] This omission exists notwithstanding the fact that the draft bill is basically modelled after the SADC Model which drew inspiration from the international code on data protection, specifically the DPD, which emphasizes the importance of data subject's consent as the main condition for lawful processing of personal data.[602]

The law requires the collection of personal data to be lawful, fair and not fraudulent. However, the processing of such data can only be legitimate if the data subject gives consent to process.[603] Under the law, data subject's consent forms a central condition for processing of personal data, without which, processing activities are in breach of the law.

Purpose limitation Both the law and the draft bill requires data to be collected for specific, explicit and legitimate purposes and any subsequently processing to be compatible with the orignal purposes for its collection.[604] The law adds the requirement that the collection must ensure that the data is adequate, relevant and not excessive in relation to the purposes for which they were collected and further processed. By necessary implication, this provision enacts what is popularly known as data minimization. This aspect is not enacted either expressly or implicitly under the draft bill.

Data quality To maintain the quality of data, the law requires personal data to be accurate and, where necessary, kept up to date. The draft bill adds an obligation to ensure that the data is

---

600 Section 7 (1) (2) of the draft bill.

601 Section 9.

602 Article 7 of the Directive states, *'Member States shall provide that personal data may be processed only if:*
(a) the data subject has unambiguously given his consent….'. Again Recital 30 to the Directive states, 'Whereas*, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject*….'

603 Save for exceptional circumstance when processing activities can take place without data subject consent as provided under article 33 (1-4)

604 Sections 9, 10, 11 and Article 35.

relevant and not misleading.[605]However, unlike the law, the draft bill does not oblige data controllers to take reasonable measures in implementing this provision by ensuring inaccurate or incomplete data (with regards to the purpose of processing) are erased or rectified.[606]

In the same vein, both the law and draft bill tasks data controllers to ensure reasonable security measures are in place for the security of personal data in their custody. The draft bill requires security measures to focus on safeguarding the data against loss, unauthorized access, use, modification or disclosure, and against other misuses, unauthorized use or disclosure.[607]The law, on the other hand, emphasizes on the security of data by dedicating the whole section II of Chapter V the law on security measures. The Section is titled "*Obligation de Securite;"* it obliges data controllers to take due precautions with respect the nature of the data and, in particular, to prevent it from being deformed, damaged, and from unauthorized access and dissemination. The section gives special attention to automated data processing systems, and restricts its access within the country.[608] Furthermore, the law requires data controller to establish mechanisms to identify and verify third parties who have access to personal data; [609]prevent unauthorized access to computer systems and computer data, unauthorized introduction of any data in the system and unauthorized inspection, reading, copying, modifying, destroying or erasure of recorded data by unauthorized persons;[610] prevent unauthorized persons using transmission facilities to access personal data processing systems and safeguard data by creating backup copies, cooling and when necessary convert personal data to a permanent storage.[611]

Exempted activities Certain activities are exempted from the application of the law and the draft bill. These include the processing of personal data solely for personal and for household activities; as long as such processing is not intended for systematic communication, dissemination to third parties or for broadcasting.[612] Surprisingly and contrary to the usual practise, the draft bill has not exempted individual processing of data for purely personal, family or domestic purposes. This means activities such as creating a phone book in a mobile phone, keeping a diary containing a reference to friends, partners and workmates or domestic grocery lists are subjected to legal regulation. Consequently, data protection Commissioner are involved in issues arising in private processing of personal data for own personal, family for domestic purposes.

The law does not apply to personal data in temporary copies; such as data processed for technical activities in transmission or provision of access to a digital network to allow data subject access quality services.[613] The law also does not apply to processing of personal data for sole purpose of record keeping in a register sanctioned by laws or regulations,[614] or data processed by charitable non-profit organizations and religious organizations, philosophical,

[605] Section 8 of the draft bill.
[606] Article 36 of the law.
[607] Section 12 (a) (b)
[608] Article 71 (1)
[609] Article 71 (2) (3)
[610] Article 71 (4) (5)(6)(7)
[611] Article 71 (7) (8) (9) (10)
[612] Article 3 (1) of the Law
[613] Article 3 (2)
[614] Article 17 (2)

political or trade union relating to a member and for purposes of the organization as long as the data is not disclosed to a third party.[615] The draft bill has no corresponding provisions.

Furthermore, journalistic, research, artistic and literary expressions are also exempted in both the law and draft bill. However, in this respect, the exemption applies only when such activities are conducted as professional activities and in compliance with professional rules and codes of ethics.[616] In the law, it is further stated that this exemption does not preclude application of the provision of other laws relating to press, broadcasting or the penal code which provides for codes of conduct or penalizes offences against privacy and individual reputation from applying.[617]

Other activities exempted from the application of the law and the draft bill are those in the preservation of national security, public safety, criminal prevention, investigation and prosecution.[618] In the draft bill, activities in violation of the code of conduct in the case of the legal profession are also exempted.[619] In the law, population census, personal data revealing directly or indirectly, racial, ethnic or regional origins, parentage, political, philosophical or religious or membership to associations, or which relate to the health or sex life of the data subjects (as long as they do not form part of linking with other processing) the treatment of wages, pensions, taxes and other liquidations are also exempted.[620]

Notification and Authorization Regime The law, places an obligation upon data controllers to give notification or seek commissioner's authorization before any processing activity can take place. Commissioner's approval signifies that the processing satisfies the legal requirements.[621] Notification must be given to the general processing of personal data which is not likely to invade into personal privacy[622] while authorization must be sought in data considered delicate and sensitive.[623]

In seeking Commissioner's authorization, a data controller must give detailed information on his identity and location (address) as well as the purpose for processing, interconnection and linking of data, involved recipient(s) and security measures taken against potential privacy breaches. In cases where the controller is not established in Senegal, the Commissioner requires information of a duly authorized representative in Senegal. A data controller must also inform the Commissioner of any sub-contracts involved in the process and the shelf life of the processed data.

In additional to Commissioner's authorization, health data can only be processed if/when data subject has given consent to specific processing activities or when such data has been made public by the data subject or when it is necessary to protect vital interest of data subject and in

615 Article 17 (3)
616 Article 45 and Section 17 (1) (e).
617 Article 46.
618 Article 21 (1) (2) and Section 17 (1) (a-d)
619 Section 17 (1) (c)
620 Article 21 (3-5)
621 Article 18
622 However, to simplify the processing activities, Section 19 allows the Commissioner to issue Regulation on the standards in processing to exonerate the reporting obligation.
623 Article 20 and 21 of the law.

activities sanctioned by law. Furthermore, any processing concerning personal health must be done under the supervision of a health care professional who is subjected to professional secrecy. Additionally, access to medical records can only be given to a patient himself or a designated physician. If the patient is dead, the access can be granted only to his non-separated spouse, children, and parents.[624]

In all processing activities that need commissioner's authorization, it is upon the Commissioner to issue the authorization within two months of application. If authorization is not issued within two months, the concerned data controller is allowed to proceed with processing activities, as the authorization is deemed favorable upon expiration of the two months if the Commissioner no communication against the application.

The draft bill does not establish a 'notice of process' or 'authorization' regime. It is also silent on the proposed idea of data controller's obligation to file annual summaries of all personal data processes as proposed by the DPD.[625] Instead, it requires the Commissioner to maintain a register of data controllers and persons maintaining data bureau and any persons providing services concerning personal data. The essence of this requirement is to keep record of all persons processing personal data, description of data held, purpose(s) of collection and processes (as notified to the data subject), sources of collection and description of intended direct and indirect transfers of data to countries outside Tanzania, other than countries notified to data subject.[626] This means unregistered persons cannot process personal data or offer data bureau services in Tanzania.

Interconnection of Data/Files and Databases The law establishes a regime to deal specifically with the interconnection of files and databases. Accordingly, an interconnection of files is allowed only when it involves data controllers who are running public services for the public interest, or when implemented by the State to support the administration of remote services within a framework of e-government.[627] On the other hand, the interconnection of a database may only be performed to achieve statutory objectives or legitimate interests of a data controller. In this case, a warrant to process is only granted if processing cannot lead to discrimination or infringement of rights and freedoms and safeguards of data subjects concerned. However, the interconnection must take into account the principles of data relevance.[628]

Before interconnection is made, an application must be lodged to the Commissioner before the processing activity. The application must provide information on the nature of interconnection; illustrate the purpose which makes the interconnection necessary; duration of the interconnection and measure taken to ensure protection and preservation of data subject rights.[629] All authorizations for interconnection are required to be registered in the Commissioner's directory.[630] The draft bill has no corresponding provisions.

---

[624] Article 43
625 Articles 18-19 EU Directive
626 Section 30 (3).
[627] Article 53.
[628] Section 54.
[629] Section 55.
[630] Section 16.

Automatic Processing The law prohibits automatic processing of data when such processing deals with decision making bearing legal effect to a person. However, when processing is done by the State in accordance with the laws and regulations, the processing can take place with the approval of the Commissioner.[631] The law names the type of activities to which automated processing is allowed with Commissioner's approval to include matters of national security, defense and matters relating to a criminal investigation, detection, and execution of sentence. Others are matters of wages, pensions, taxes and other liquidation. However, when the processing leads to evaluation on personality or certain aspects of personality or defines person's profile, such evaluation is not to form a basis for a decision on an individual neither in a Court of law or any institution; public or private.[632]

In the same vein, the draft bill prohibits personal evaluation based on processing of personal data by automated means. Accordingly, the data subject has a right to prevent data controller from making any such decision based on processing by automatic means. If such decision is made, the data subject has a right, by notice in writing, to request from the data controller to reconsider the decision or defer the decision on that basis. Upon such notice, the data controller must, within 21, days give data subject a written notice specifying actions taken to comply with data subject's request.[633]

Direct Marketing or Advertisement The law and the draft bill forbids data controllers from carrying out direct marketing by any means or form of communication unless data subject has given a prior consent to receiving such promotions and/or advertisements.[634] This includes mobile-marketing usually done by telecom companies to advertise their products and promotions, or by emails or other electronic means.[635] Data controllers are further prohibited from using personal data to advertise or promote their businesses or transfer to third party for that purpose. The only instance personal data can be used for marketing purposes is when data subject has consented to their data to be used or shared, to promote business or for commercial advertising. In the draft bill, if the controller wishes to do so, he must inform the data subject of the identity of the data controller and all necessary information on the product to allow data subjects make informed decision.

Apart from a mere prohibition, the draft bill does not establish a concrete regime on the processing for purpose of direct marketing, other laws and regulations erects such regime to supplement the draft bill. The Consumer Protection Regulation 2011 made under the Electronic and Postal Communications Act of 2010 provides for that regime. The Regulation requires the collection of personal data for direct market to adhere to the usual data protection principles.[636] In addition, data controller must identify himself to data subject, and give breakdown of the total costs of the product or services that is the subject of the communication.[637] The essence is to allow data subject to make a decision of whether or not to opt-in or opt-out. Another complementing regulation is the Electronic Transaction and Electronic Contract Bill 2014. The

631 Article 21.
632 Article 48.
633 See section 4 (1) (2) and schedule II.
634 Article 47 and Section 3 (1) and Schedule I.
635 Section 3 (1) and Schedule I.
636 Regulation 6 (2)
637 Regulation 7 (4)

ETECB obliges service providers to establish an opt-in and opt-out registers. The ETECB fills in the gap left by the Regulation and the draft bill, as both have failed to impose a requirement for establishing opt-in and opt-out facilities for this purpose.

Rights and Duties The draft bill provides for data subjects' right and data controllers' duties in the implementation of the proposed law. Data controller has a duty and is accountable for adherence and enforcement of the data protection principles.[638] S/he is also accountable for the integrity and strict rules of confidentiality on personal data. Section 10 and 11 of the draft bill and Article 70 of the law requires data controllers to enter into written contracts with people having access to personal data and ensure they have the technical and legal knowledge to uphold the requirements of the law. This duty extends to third parties processing personal data for or on behalf of the data controller and whoever has knowledge of processing activities.[639]

On the other hand, data subjects have the right to access their information held. This right gives data subjects a subsequent right to their personal data including the right to inspect the data and (if desired) request correction or amendment of inaccurate, misleading or false data and erasure of irrelevant data. Data subjects have the right to be informed by the data controller of the identity of the data controller, his agents and any third parties to whom data may be transferred to. Data subjects have the right to object to any processing of their personal data on legitimate grounds.[640] Furthermore, data subjects have the right to be informed of their access rights and data retention period.[641] In the draft bill, the access right is limited to information about the purpose of collection or the fact that the collection is for purposes authorised by law and gives identities of intended recipients.

In relation to the right to erasure and amendment of personal data, the draft bill has introduced an unusual clause. The clause requires data controllers, when making amendments of personal data upon request, not to delete the records of the document as it existed before the amendment.[642] The intention of this clause is unclear; however, it derogates the overall essence of data subject's right to participate in the protection of his/her data and privacy. What then is the aim of allowing data subject to rectify or delete irrelevant or misleading data if the copy as it originally existed remains with the data controller? The draft bill is silent on the treatment of the retained data and gives no obligation to the controller to inform the data subject of the fact that the original copy of the deleted data remains in controller's database.

Furthermore, the definition of processing under the draft bill includes storage. It follows then, when data controller deletes data (upon data subject request) but retains a copy, s/he is in breach of data subject's rights under the proposed law. Bygrave clarifies such situations in clearer terms saying, contravention of one's right to privacy occasions when 'the data in question reveal details about the data subject's personality are processed without the latter's knowledge or consent, and the processing potentially casts the data subject in a negative light or could result in a restriction of the data subject's freedom of choice. These principles would seem to apply regardless of

638 Section 15.
639 Article 70; Section 45.
640 Articles 58, 62, 68 and 69; Section 14 (1) (2) and Schedule II.
641 Article 58 (1-9); Section 7(2) (a-c).
642 Section 14 (3).

whether the information is processed automatically or manually'.[643] As long as legality in processing personal data under the draft bill is centred on subject's knowledge of the existence of his data in data controllers' database, this provision goes against the spirit of the draft bill. In this case, there is neither knowledge nor consent of the data subject to retain the data.[644] This Section, not only obliterates the security of personal data provided by the draft bill itself,but it also interferes with a sphere of a person's life in which he or she can freely choose his or her identity.

The Data Protection Authority The law and the draft bill establish Data Protection Authority (DPA) as an independent administrative office, tasked to oversee the implementation of these laws.[645] Independence of the DPA is emphasized under Article 14 of the law and Section 21 (2) of the draft bill. Both texts envisages a Commissioner with managerial autonomy and freedom from the influence of instructions by any other public or private entity. The law goes further in ensuring DPA's impartiality by imposing restrictions on the social interactions of the data protection Commissioner. The Commissioner is, under Article 15 prohibited from receiving gifts and grants from individuals, organizations or foreign States, unless the grant from the foreign State is given through a partnership with the government of Senegal. Furthermore, the Commissioner is expected to take all the appropriate measures to ensure independence and impartiality of the member staff of the DPA.[646] The Commissioner and all member staff must take a Court administered oath, promising to save the DPA confidently, faithfully, independently and impartially.[647] The in both texts the Commissioner's tenure is protected against unduly termination. S/he cannot be removed from the positions save for inability to discharge their functions under the law and proposed law, by resignation or for misconduct.[648] The law goes further by protecting the tenure of member staff of the authority. Accordingly, member staffs are irremovable save for misconduct, inability to perform or by resignation. The draft bill has no provisions protecting the tenure of the member staff of the Authority.

The DPA in both cases receives funds from the government. In the case of Senegal, the Commissioner enjoys the management autonomy as he is the one preparing the budget based on the needs of the Authority, in light of the rules of public accounting. However, the budget is subject to the approval of the Commission's Board.[649]In Tanzania, the parliament is the one determining and granting the Authority funds to run its activities.

The Commissioner's activities in both the law and draft bill includes raising public awareness of the individual rights and obligations, oversee that ICTs and its development do not threaten fundamental rights and freedoms in privacy protection,[650]and advice persons and organizations on dealing with personal data. The law grants the Commissioner powers to investigate breach of the law, *suo motto* or on application, and to resolve disputes arising out of the rights and duties established under the law. Parallel to these powers, the Commissioner can enter any premises to

643 Bygrave, L. A., (n 201), p. 253.
644 Boshe, P., (n 202), p. 4
645 Article 5; Section 20
646 Article 9
647 Article 11.
648 Article 8; Section 24.
649 Article 14.
650 Articles 5 and 16.

search and to seize any evidence.[651] The Commissioner can also issue sanctions to data controllers in breach of the law.[652] At this point, it is important to note that, in the draft bill, the Commissioner can only deal with dispute brought before the Commission by a complainant or third party on behalf of the complaint, s/he cannot initiate investigation *suo motto*. Furthermore Commissioner's power to enter premises for investigation is conditional. First, the Commissioner must inform the CEO of the data controller of the intention to carry out such investigation and the substance of the complaint.[653] Thereafter, the Commissioner must inform the prosecutor before exercising this power.

International Data Transfer The law prohibits transfer of personal data to third country unless such country provides for sufficient legal protection to privacy, freedoms and fundamental rights of individuals with regards to the processing of personal data.[654] In implementing this provision, the law considers any country, beyond Senegal as third countries;[655] by necessary implication this includes countries within ECOWAS to which Senegal is a Member State. In exceptional circumstances, trans-border data transfer can be permitted at the request of the data controller who must adduce evidence of adequate safeguards with respect to protection of privacy, freedoms and fundamental rights of the data subjects.[656] In such cases, the Commissioner is required by the law to assess the sufficiency of security offered by third country. The assessment on the security measure provided by a third country are measured against the required security measures provided by Senegalese law, nature of data, purpose of processing, duration, origin and destination of the personal data subject to the process. Upon satisfaction of the security measure provided by a third country, the Commissioner may issue an authorization to data transfer.

Personal data can be transferred in exception to the above rule when the data subject has expressly consented to the transfer either in the protection of data subject's life, to safe guard public interest, in an exercise of defense or a legal claim and in an execution of a contract between data controllers and a data subject.[657]

The draft bill also has a regime for international data transfer; similar to one found in Articles 25 and 26 of the DPD. Although the draft bill does not define a 'third country', Section 4 provides that, international data transfer 'refers to any international, cross-border flows of personal data by means of electronic transmission'. Consequently, international or cross-border transfer of personal data using any other means, (apart from electronic means) are not regulated under this regime.

The general rule under Section 54 allows transfer of data to countries with adequate data protection framework. However, this rule gives additional duty to the data recipient to establish that the data is necessary for a performance of a task carried out for public interest or pursuant

651 Sections 21 (1) (b) (p), 36 (1) (2) and 41.
652 Articles 19, 26 and 32; Sections 21 (1) (b) (p), 36 (1) (2) and 41.
653 Section 38.
654 Article 49.
655 Article 4 (12).
656 Article 51.
657 Article 50.

to lawful functions of the data controller, or that the transfer is necessary and there is no reason to assume that data subject's legitimate interests might be prejudiced. The necessity of transfer is to be determined by the data controller[658] who shall also make sure that the recipient processes such data only for purposes for which they were transferred.[659]

As an exception to the general rule, Section 55 (1) allows transfer of data to countries without adequate level of protection. Such transfers can only be made when the recipient country ensures adequate level of protection and the basis of processing is solely to permit processing for authorised activities to be taken by the data controller.[660] In this case, adequacy determination depends on the nature of data, purpose of the data process activities, duration of process and recipient country's overall legal framework.[661] Yet, apart from this condition, there are other instances where personal data can be transferred to countries without adequate level of protection. These are listed under section 55 (4) to include when the data subject has unambiguously given consent to the transfer; when transfer is necessary for the performance of a contract between data subject and controller or implementation of pre-contractual measure taken in response to data subject's request; when transfer is necessary or legally required on important public interest grounds; or for the establishment, exercise or defence of a legal claim; transfer is necessary in order to protect legitimate interests of the data subject or the transfer is made from a register which, according to Acts or Regulations, is intended to provide data to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

The Commissioner may also authorise transfer or set of transfers if s/he is assured by data controller and satisfied that the data controller can provide adequate safeguard with respect to the protection of privacy and fundamental rights and freedoms of the data subject concerned. This can be through adequate legal and security measures or contractual arrangements.[662]

Whistleblowing The draft bill establishes a system for the protection of whistle-blowers from retaliation. Whistle-blowers are considered to have an important role in enforcing data protection principles. Section 51 (2) provides for the security and protection of whistle-blowers in an endeavour to uphold the data protection principles. In the draft bill, whistle-blowing is also encouraged in relation to technical and organisation rules which may have an adverse effect on the provisions of the proposed law.

So far, the draft bill has not provided for the rules on authorisation for and governing the whistle-blowing system. However, once the law comes into force, the Commissioner is obliged to establish such rules under section 51 (1). The whistle-blowing can, if properly devised, allow persons to unearth institutional malpractices and act as a safety net to adverse actions which may not be easily detected by the public or the Commissioner.

658 Section 54 (3).
659 Section 54 (5).
660 Section 55 (2).
661 Section 55 (2)
662 Section 55 (5).

At this stage, it is not clear how the Commissioner is going to address the challenges surrounding whistle-blowing in relation to data protection. Reference is made to the Article 29 Working Party opinion[663] on the Application of whistle-blowing schemes in the field of accounting, internal accounting controls, audit matters, fight against bribery, banking and financial crime. In the opinion, the Working Party insists that any whistle-blowing scheme must be subjected to data protection principles. The schemes must adhere to the duties of data collectors and rights of data subjects. In this case, the wrongdoer should have the same rights in relation to the processing of personal data for the whistle-blowing arrangement to be lawful. Such rights include the right to know the data held and purposes for its processing as well as recipients of the data. The wrongdoer also has the right to object the processing of personal data on legitimate grounds.

5.5 Conclusion

Data protection reforms in Africa and particular Senegal and Tanzania have been highly influenced by international data privacy policies/codes notably the EU Data Protection Directive as well as the CoE Convention on privacy protection. In both cases, international Agencies, as well as individual European countries, have provided financial and or technical support towards reforms. While there is no problem in transplanting a foreign law into African States, the question may arise on the relevance and applicability of such transplants in African contexts. This is mainly to the fact that, in Africa, there is an existence of multiple legal cultures and systems; an element lacking in the Western hemisphere where the laws/regimes originate. This could affect the transposed contents as they are met with different species of a host. Inevitably, this calls for certain adjustments in both legal structure and legal content for a successful adoption.

In the two case studies, the reforms seem to have, at some point, considered the nature of the local systems. For example, the draft bill has, under Section 4 included data containing personal cultural and social identity as sensitive personal data. The draft bill prohibits the processing of personal data are if the processing would reveal the ethnic origin of the data subject. On the other hand, the law has as its objectives statements to protect personal data and individual privacy as well as 'community rights' to privacy. Sadly, the law has neither defined what the 'community rights' are nor established principles or authority to enforce the community rights. In fact, apart from the statement of objective, there is no other place within the law that the community rights are mentioned. The law also ousts its application to all processing activities involving personal data revealing, directly or indirectly, racial, ethnical, regional origins and parentage.

The established enforcement authorities do not exhibit considerations to the local legal system with multiple legal cultures. They are established with a view of a State with a single legal culture. There is no inclusion of customary or Islamic personnel or personnel with knowledge of the customary and or Islamic legal culture.

663 00195/06/EN Working Paper 117.

Conclusively, in both case studies, the texts do not illustrate substantial consideration of the existing legal structures (apart from the 'formal' legal system) The exemptions, mentioning and special categorization of certain data considered to have cultural significance as an accommodation of existing legal structures is insufficient. Furthermore, reforms in data protection being more than just a legislative activity call for an establishment of a unique enforcement authority. The established authorities in the case studies do not illustrate a nature of a State with multiple legal cultures. One would expect the establishment of the similar authority as established in the Western transposed frameworks but modified to include existing legal cultures.

6. Conclusions and Future of African Data Protection Regimes

6.1 Conclusion

The 'Western' notion of privacy is argued to have received resistance in Africa solely on the assumption that, this notion appraises the idea of individualism while Africa is identified with communalism. The evidence adduced to support unacceptability of privacy in the form of an individual right includes the fact that the right is excluded in the African Charter. Furthermore as illustrated in chapter three, more reasons includs lack of cultural legitimacy on the right to privacy among the communities who are to reap its benefits. As a result, Himonga[664] speaking from an assessment of studies on enforcing the right to privacy in Africa says, this perception leads to the rejection of the right solely on societal values, i.e. "western" and "African" individualism and communalism respectively.

The right, first adopted in the form of bill of rights was contested as reflecting Western values, giving primacy to individualism against the African traditional values favoring the community.[665]As a result, Abdullah An-Na'im believes that their application is a subject of a century-long trial and error,[666]as they lack the legitimacy of public consensus[667] and perpetuates colonial institutions,[668] culture and practice.[669]The result is non-enforcement of the right to privacy in almost all of the African States except two countries; Kenya and South Africa. The main problem most of the proponent of the African communalism status as explained by Shahadah[670] is the idea that they wish to find African culture stuck somewhere back in the nineteenth century and want to apply and rearrange it to the present context. They fail to realize that culture itself must reconstruct itself in a system in which it exists. As Shahada once argued, the African culture is always changing and evolving because the context in which Africans live changes and evolves. Hence, what makes an African culture is its operation in the interest of the Africans to advance the Africans.[671] The continued reliance on the 'communalism culture' argument does not; according to Anthony necessarily indicate a lack of its development rather a skilful survival-centred method of exploring sustainable legal arrangements.[672]

The peculiarity of African legal cultural development as compared to Europe is noted. To elaborate, the African approach has been for the legal culture to follow human development on

---

[664] Chuma Himonga (2013). The Right to Health in an African Cultural Context: The Role of Ubuntu in the Realization of the Right to Health with Special Reference to South Africa. Journal of African Law, 57, 2013, pp 165-195 at p. 165.

[665] Keith, C.K and A. Ogundele., Legal Systems and Constitutionalism in Sub-Saharan Africa: An Empirical Examination of Colonial Influences on Human Rights, Human Rights Quarterly, Volume 29, Number 4, November 2007, pp. 1065-1097 at p. 1067.

[666] An-na'im, A.A., African Constitutionalism and the Rule of Islam 171 (2006).

[667] Ibhawoh, B., Between Culture and Constitution: Evaluating the Cultural Legitimacy of Human Rights in the African State, 22 Hum. Rts. Q. 838 (2000), p. 846.

[668] Okoth-Ogendo, H.W.O., Constitutions without Constitutionalism: Reflections on an African Paradox, in Constitutionalism and Democracy: Transitions in the Contemporary World (Douglas Greenberg, et al. eds., 1993); supra note 2, at 69.

[669] Mutua, M., Justice under Siege: The Rule of Law and Judicial Subservience in Kenya, 23 Hum. Rts. Q. 96 (2001), p. 97

[670] Supra at p. 14.

[671] Shahadah (n 380) p. 21.

[672] Ibid.

the creation of a legal culture called 'customary law', usually without the intervention of the central power. Still, contrary to arguments, the African culture has an ability to both be created and can be changed very quickly. It has the ability to mutate, is fluid and flexible. To narrate this fact, Shahadah uses an example of urbanization. He says, urbanization in Africa most often leads to the formation of new customs; people abandon their traditions whenever they are ruled to be non-sensical in new modern situations. Eventually, the formation or acceptance of a new culture formally unrecognized or ignored by society or official powers.[673]

In the globalized markets, demand has and continues to play a significant role in shaping African cultures. Accordingly, cultures adapt, evolve and reply to reality without affecting the ethics which remains rooted in the foundational paradigm which fosters them.[674] Furthermore, culture becomes redundant when it fails to meet the needs of the people or solve their problems. It follows, therefore, the fact that Africa has been an unregulated continent in relation to data protection within tremendous technological development poses an imminent threat to personal privacy; and that forms a strong motivation for establishing a form of regulation to protect individual privacy and secure personal data regardless of underlying values and conceptual foundations. Globalization means interaction and cross-influence of legal systems and cultures; this precludes Africa from clinging on communalism to avoid alignment with the rest of the world in reforming or adopting on data protection regimes.

Data protection legal reforms in Africa, given the delicate state of the African legal culture, cognizance to specific local situation owe to be considered. The reforms must not be made in isolation of the local contexts. Spătaru-Negură says, 'legal transplantation is a massive engineering project; it is not simply transplanting a single law or institution, but also creating the circumstances and the legal framework to make sure that the transplanted law can perform successfully'.[675] Furthermore, attention is owed to the legal culture; as Spătaru-Negură once again explains, 'legal culture is usually based on social values, local customs and national feelings. A comprehensive understanding of not only the legal culture of the country of origin but also a scientific appraisal of the compatibility between transplanted laws and local legal culture, after making a rational choice is required.'[676]

However, it is very important that the African States should not overly localize the data protection legal frameworks. If overly localized, may bring challenges in understanding and in interpreting by the rest of the world. African culture being peculiar to Africa may pose this challenge as the rest of the world lack education on African anthropology especially in relation to law making and interpretation. On the other hand, Africans have gone through formal legal education, they can understand a 'formal' law and can be able to interpret concepts, content and context of their application and apply them in specific context to yield expected objectives.

The world is becoming a global community hence the need to follow some rules to co-exist. Consequently, developing worlds cannot avoid the effect of the developed world legal frameworks. However, given the development gap, cultural and ethical diversities, Kingsley

673 Shahada (n 380) p. 49.
674 Shahadah (n 380) pp. 63 and 90.
675 Spătaru-Negură, L., Exporting Law or the Use of Legal Transplants, Challenges of the Knowledge Society. 2012; No. 2, pp.812-819 p. 815
676 Ibid, p.816

proposes that, before a country can transplant any law, it has to look at three important aspects to ensure that the law can work in the local environment. The first one is the legal culture, which looks at the structure, nature, forces, traditions, strengths, and deficiencies of a legal system. All of which forms a nation's legal culture which impacts upon the interpretation and acceptance, or otherwise, of legal transplants. The second one is to establish core parameters in which the laws and possible deficiencies arising out of these laws are reviewed, with a focus on law reform efforts. In addition, the proposed reforms cannot merely be ambiguous "framework" statements utilizing vague propositions; rather, clear areas of reform need to be delineated in order to allow adequate review and preparation for detailed research. The third is the application of interdisciplinary research.[677]

Tabalujan suggests, to overcome rejection of foreign legal transplant, every law reform proposal to change some substantive law or legal institution should include an analysis of what aspects of the local legal culture would support or inhibit such change. Every law reform initiative should be accompanied by concrete steps designed to make the local legal culture more amenable to the proposed change. If this is not done and legal culture continues to remain a neglected aspect of law reform, then the risk of failure is high.[678]

In reality, the world has accepted the European framework for data protection as providing standard protection and to have universal applicability. This stance alone leaves no room for an African State to avoid reforming data protection regime in alignment. Furthermore, when one poses the question of cultural difference or cultural incompatibility, there is a vast of research confirming the non-static nature of cultures. Generally, as argued by Warren and Brandeis, culture would undergo continuing growth as society and culture develop entailing recognition of new rights to meet the demands of the society. More so, when societal changes are influenced by technologies as technology plays a large role in developing a new understanding of our rights. In their words, they said;

> 'The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasion upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury'.[679]

Although Gerety still insists on our intuition of what *ought* to be surpass what *is,*[680] in this case, technology, human interaction and globalization endorse the inevitable adoption of accepted standards of data protection regimes. As long as African continent does not have any concept relating to privacy; and the fact that the European framework is considered as a 'universal' code, African States existence is more displaced unless they adopt similar Regulations as one provided by the European Union.

677 Kingsley J J,(n 23), p.4.
678 Tabalujan B.S, Legal Development in Developing Countries: The Role of Legal Culture,Singapore, 2001, p. 42
679 Warren and Brandeis, supra, p. 77.
680 Gerety, T., 'Redefining Privacy', Harvard CR-CLL Rev, Issue 12 Vol 2, 1977, p. 233 at p. 242.

Africa has a serious lack of experts in the area. It needs more than just legal reform to be able to have a working law. Unlike other laws, data protection regimes are a framework which needs more than just a person with legal knowledge to interpret and apply the laws. It needs legal personnel with expertise in data protection laws to have it properly and objectively implemented. Africa is still very immature in this area, it requires more than just financial and consultative support, it needs more support on the substance and structural reforms, at least at the take-off phase. Training is also required to main sectors responsible for implementing the law is also necessary. The approach taken by the AFAPDP in reforming Senegal (and other Francophone African States) is recommended for Africa.

In Senegal, the AFAPDP has continued to assist with the implementation of the law after the actual reforms. The AFAPDP sets up follow-up mechanism, gives a continuous assessment of the adopted framework on its compliance with international standards. AFAPDP hold regular seminars, conferences and training to teach and update knowledge on data protection regulations and discuss challenges in implementing the data protection laws. AFAPDP together with the Francophone African States discusses new strategies and resolutions to resolve new challenges posed by the ICTs development to data security. Through these meetings, States have an opportunity to discuss issues underpinning protection of personal data, share good practices and give visibility to the actions and positions of the AFAPDP and its members.[681] The organization, knowing the lack of data protection expertise in Africa, also acts as a source of expertise for the Francophone African countries in regulating of data security. It is also the mouthpiece for these States in dialogue with international data protection institutions including the UN, EU and APEC.[682]

This approach encourages dialogue and international cooperation which would not only help newly reformed African States to implement the adopted frameworks but acquire the necessary and practical knowledge to address data security issues posed by new technology. In Tanzania, reform process was initiated by Multi-National organizations. The financial and technical assistance ended with the adoption of the draft bill. Thereafter, the Ministry took over and continued the process behind 'curtains' with no public consultations or awareness programmes. This is different from Senegal where the adoption of the law was preceded with substantial public awareness.

6.2 Future of Data Protection in Africa

Authors suggest African communalism naturally rejects the idea of individual privacy. These arguments often lead to a conclusion that privacy right having being based on an individualistic approach is bound to fail. These arguments are in forgetful of the fact that, human beings are animals, and it has been scientific researched and verified that the desire for privacy is deep rooted in animal origin;[683]as such, they device different mechanisms to claim their privacy. These

[681] http://www.afapdp.org/
[682] https://www.esomar.org/news-and-multimedia/news.php?idnews=133 last visited on 22.07.2016.
[683] Westin, (n 29), p.4.p.8.

mechanisms include territoriality against other animals. In this regards, we find the existence of rules of exclusion such as the tort of trespass, defamation which exists in African legal systems as evidence in that regard.

In groups, animals set personal, intimate and social distance within their social organization. Furthermore, there are human activities summoning intimacy or privacy, such as sexual intercourse. These activities regardless of the communal nature of the society can never be conducted in groups/social organization. Yilma elaborates that, all communities have rules for concealment of female genitals, and on time and manner of their exposure. Privacy is also seen in sexual relations. Within a society, 'there are rules limiting entry by non-residents and outsider's conducts once s/he enters. Also, there are norms limiting family conversations or acts performed in the presence of outsiders'.[684] Hence, the absence of the right to privacy in the African Charter and non-enforcement of the right by the Member States is nothing but lack of political will. It is incorrect to conclude from these acts as the absence of the need for the right to privacy within African communities and its people.

There is a reason, despite colonization, African traditional legal structure and law continues to exist. A comprehensive reform or integration has never been achieved in a single African country. Change of law or reform in any African legal system requires an understanding of the core norms which specific African societies are 'unwittingly' to forego. The African States are, unlike European and American, capable of hosting different types of legal systems and laws. These legal systems and laws have not only co-exists, but their co- existence is balanced to allow intended justice/outcome to prevail; a phenomenon unseen in the Western legal systems.

The nature of the African States legal systems allows and welcomes changes. Cultural laws are even more predisposed to change. The absence of written codes allows societies to be extremely dynamic. It means, what is law is imagined at a certain time and place as something with life; it changes on demand and societal agreement. A rule is acceptable as law as long as it supports and retains stability to core traditional norms. This is in line with of law as a social contract.

African cultural laws aim at upholding societal interests. Societal interests change with time. Today, technology has infiltrated even into the crudest of communities; government activities affect even those who refuse to use technology. The effect is an invasion of natural rights and liberties which human being sought to preserve, such as territorial rights or intimacy. The change of times, technology and governance have an impact on the traditional norms and open doors for improvement. African cultural law does not enforce rules which are redundant to the society but rather adapts to new social challenges. This means reforms in data protection are potentially welcome and acceptable as long as do not unreasonably disturbs the traditional norms.

It is crucial, in the African context, to consider local realities in any data protection reform programme. And as suggested by Stephen Toope,[685] ignoring the local environment and cultural values can lead to resistance, unsustainability and ultimate failure. Data protection laws are aimed at regulating acts and providing rights of the society; hence, to be of value, they must provide

[684] Yilma, p. 4.
[685] Toope, S., Legal and Judicial Reforms through Development Assistance: Some Lessons, McGill Law Journal, Vol 48, 2003, pp. 357-417 @ p. 357.

guiding principles that allows for regularity and rationality in a way in which disputes are settled and the way in which relationships are governed.[686] In other words, the law should not only govern relations, rights and duties but the society should be able to relate to it. After all, the value of any legal system is derived from specific cultural, social and political contexts. It follows, therefore, 'Naïve assumptions of congruence are often overthrown in the project implementation'.[687]

The nature of African States requires consideration of different layers within a particular legal structure. This allows for a determination of overarching societal goals, existing frameworks and their effectiveness. This determination informs the decisions on the measures required for a legal reform and answers important questions such as what aspects of the existing structure;

- complements the proposed reform,
- conflicts with the proposed reforms, or
- are the missing in either the existing structure, the proposed structure or both (in light of the objectives of the reforms)

A close examination of the existing structure is important in determining the type of enforcement authority to be established. In this case, whether the existing formal and informal authorities;

- can interact harmoniously, or
- have sufficient expertise to implement the proposed reforms

Data protection reform by transposition, as was done in Senegal and Tanzania requires transposition of legal expertise. In this case, knowing the law or being a lawyer is insufficient. This is because, unlike other branches of law, reforms in data protection are not a mere drafting process; rather an establishment of a legal framework.

Data protection reforms in Africa are deficient. Despite scholarly concerns and debate on what constitutes African privacy, none of the reforms, from domestic, Sub-Regional to Regional bothered to deal with this question. The process neither conceptualized nor contextualized the concept within an African context. It may seem like a trivia issue since privacy has already been defined in so many ways and by so many people. However, in the African context, it is necessary that privacy receives a formal baptismal. Whether it is by borrowing from existing meanings or through a construction of a brand new meaning, privacy needs its African meaning. Not only because privacy is 'still' a novel concept in African societies but because a lack of its understanding within local context sets any reforms to an inevitable collapse.

Like building a house, conceptualizing privacy is the foundation for data protection. People need to understand what the concept means to them, to their interactions and their institutions. Failure to conceptualize the core right that led to the reforms makes the reforms a mere reaction

[686] UK., ODA, Government and Institutions Department, Law, Good Governance and Development (Guidance Paper), January 1996@pp. 1 and 12.
[687] Toope, S., (n 685), pp. 390

to globalization on data protection. This will, in the long run fall short of expected results or collapse the process altogether.

Unfortunately, it is not the first time that Africa reacted and reforms its system blindly to align to global systems. In 1960's after independence, the African Head of States adopted socialism after the Soviet Union and China. Similar to the ongoing reforms on data protection, the adoption of socialism lacked definite ideology. According to Firedland and Roseberg,[688] the adoption of socialism was a political reaction which had no legs to stand on African soil for lack of ideology. As a result, African socialism collapsed with the fall of Berlin Wall and the Soviet Union.

Chapter one elaborated how the data protection reforms in Africa are a reaction to somewhat modest threat by the DPD. Authors such as Bygrave, Greenleaf, Birmack and Makulilo have, in different occasion elaborated how Articles 25 and 26 of the DPD led to reforms in Africa and other regions such as Asia. This, in itself, is not a menace. In fact, it stimulates legal harmonization and hence international trade, market integration and economic development. The problem lies in the failure to localize the reforms. To begin with is the failure to conceptualize privacy within specific contexts. This threatens the very existence and sustainability of the established regimes. As was the African socialism, data protection regimes remain to be 'mere reactions' to the DPD. Like the African socialism, data protection regimes may end up depending on the survival of the EU data protection frameworks for their validity and survival. In case the EU regime collapses, so is the African data protection regimes. Although the established regimes can stand and function independently, their survival and validity depend on the survival, validity and relevance of the EU regimes. African regimes remain valid as long as the replica is unchanged, if and when the replica changes, the African regimes lose their validity in the global sphere unless they adopt to change. Eventually, the EU data protection regime continues to determine the validity and the life of the African data protection regimes. African regimes continue to 'play catch' in the area of data protection. In fact, this is already happening; with the GDPR coming into force in May 2017, many aspects in the data protection laws in Africa are rendered redundant.

While African States and the African Union continue to 'implement' the 1995 DPD, the EU has undergone several developments to address challenges by technological development that came after the 1995 DPD. Most of African State laws do not reflect these developments; they are silent on issues such as breach notifications, data protection for minors, the status of IP addresses, cookies requirement, recognition of data transfer agreements, etc. It is not clear how African States will address new measures and requirements that come with the GDPR; because the 2014 Malabo Convention and the Sub-Regional data protection instruments are based on the soon to be replaced DPD.

The African Union as an African institution needs to have its initiatives towards data protection within and beyond Africa. The African Union is failing its Member States by remaining dormant and a blind receiver instead of an active participant in the global discussion and processes. Scholars such as Mayer[689] urge Europe should treat Africa as an equal and responsible partner on

[688] Firedland, W. H and Roseberg C. G Jr.,African Socialism, Stanford University Press, 1964, p. 2
[689] Mayer (n 125).

issues of global challenge, not as a dominant and overbearing.[690] An approach which Mayer suggests would look at 'global good'; first by defining global responsibility and then address the question, what Europe or Africa as whole and EU or AU, in particular, ought to act on global affairs with its unique set of opportunities and instruments.[691] Unfortunately, in this context, Africa does not seem to take up her position and act accordingly. Furthermore, despite the brilliance and parity in Mayer's suggestion, the idea may not be forthcoming because of two dimensions that continue to define EU-Africa relations. First is the increased marginalization of Europe as a driver in world affairs, and secondly is the tainted Africa perception on Europe influenced by a history of colonization and which bring the feeling of dependency towards Europe.[692] The nature of privacy, the discrepancy in its value and perception calls for an understanding of its value on the basis of 'global public good'. Perhaps, Africa should, as suggested by Mayer, shift her perspective from inward looking and dependent Africa to one that places the continent firmly within the global context,[693] and illustrate capabilities and contributions in the data protection reform agenda.

Data protection is a highly evolving and internationalized area of law. It requires commitment, cooperation, active participation and constant negotiations with other regions such as the EU, APEC, and ASEAN. It is only in such manner African Union can, on behalf of its Member States; establish an acceptable and sustainable data protection framework regardless of the vast cultural diversity of its Member States and different international legal values. The dynamics involving data protection regimes requires active participation because their trans-border rules are usually intrusive. These rules will force Africa to deal with a complex matrix in which various existing domestic and international legal principles interacts. Africa is soon to realize that, being dormant and 'playing catch' in the field of data protection is more costly economically, socially and even politically. That active participation, coordination and negotiations in data protection processes and development are inevitable; if not for individual rights, for socio-economic and political survival.

[690] Ibid, pp. 43-45
[691] Ibid, p. 447
[692] African and European countries and regional organizations have been forced to adapt to tectonic shifts in the post-Cold war order since 1990, with each continent individually and jointly adjusting to the newly enhanced partnership where economic rather than political power is decisive; see generally Mayer (n 125). For a different view see Makulilo, A.B., 'One size fits all": Does Europe impose its data protection regime on Africa?', Datenschutz und Datensicherheit (DuD), 2013, Vol. 37, No.7, pp. 447-451.
[693] Mayer (n 125), p. 457.

7. Bibliography

Adamo, K and Garonna, P., Euro Mediterranean Integration and Cooperation: Prospects and Challenges,
http://www.unece.org/fileadmin/DAM/oes/nutshell/2009/9_EuroMediterranean.pdf.

Adjolohoun, H.S., 'The ECOWAS Court as a Human Rights Promoter? Assessing Five Years' Impact of the Koraou Slavery Judgment', Netherlands Quarterly of Human Rights, 2013, No. 3.

Akokpari, J., 'Human Rights Actors and Institutions in Africa in Africa's Human Rights Architecture', Akokpari, J and Zimbler, D.S(Eds), Cape Town, 2008.

Alan, F.W., Privacy and Freedoms, Atheneum, New York, 1967, p. 7.

Allot, A.N., 'The Unity of African Law', in Essays in African Law, London, Butterworths, 1960, pp. 69-71.

--- 'Towards the Unification of Laws in Africa', International Comparative Law Quarterly, 1965, Vol. 14, No.2, pp. 366-389.

Altman, I., 'Privacy Regulation: Culturally Universal or Culturally Specific?', Journal of Social Issues, 1977, Vol. 33, No. 3, pp 66-84.

--- The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Monterey, CA.: Brooks/Cole, 1975.

Analysis and Impact Study on the Implementation of Directive 95/46/EC in Member States, 2003.

Ankumah, E. L., La Commission africaine des droits de l'homme et des peuples. Pratiques et procédures, Londres, SADIC, 1995.

Arieff, A. et al., 'The Global Economy Crisis: Impact on Sub-Saharan Africa and Global Policy Responses', CRS Report for Congress, 2010.

Article 19., 'Kenya: Draft Data Protection Bill critically limited',

http://www.article19.org/resources.php/resource/2825/en/kenya

Article 19., 'Nigeria: Personal Information and Data Protection Bill',

http://www.article19.org/resources.php/resource/3683/en/nigeria.

Article 29 Working Party, 'Opinion 5/2001 on the European Ombudsman Special Report to the European Parliament following the draft recommendation on the European Commission in Complaint 713/98/IJH' , (WP 44, May 2001).

Article 29 Working Party, Opinion 03/2013 on purpose limitation as set out in Article 6(1)(b) of the Data Protection Directive 95/46/EC, (WP 203) April 2, 2013.

Article 29 Working Party, Opinion 2/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.

Article 29 Working Party's Opinion 4/2007 on the concept of personal data (WP 136).

Bakibinga, E.M., 'Managing Electronic Privacy in the Telecommunications Sub-sector: The Uganda Perspective', Africa Electronic Privacy and Public Voice Symposium 2004.

Baldelli, F., 'Legal Origins, Legal Institutions and Poverty in Sub-Saharan Africa', Master's Degree Thesis,LUISS Guido Carli University, 2009/2010.

Bamodu, G., 'Transnational Law, Unification and Harmonization of International Commercial Law in Africa', Journal of African Law, 1994, Vol.38, No.2, pp.125-143.

Banisar, D., 'Privacy and Data Protection Around the World', Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13th September 1999, pp.1-5, at p.1, http://www.pcpd.org.hk/english/infocentre/conference.html.

Barker, W. B., 'Expanding the Study of Comparative Tax Law to Promote Democratic Policy: The Example of the Move to Capital Gains Taxation in Post-Apartheid South Africa', Pennsylvania State Law Review, 2005, Vol. 109, pp.101-125.

Bawa, A.B., 'From Imperialism to Diplomacy: A Historical Analysis of French and Senegal Cultural Relationship' a paper presented at the London Art as Cultural Diplomacy Conference 2013 on the theme: "Contemporary International Dialogue: Art-Based Developments and Culture shared between nations" held at The Portcullis House, British Parliament from 21st to 24th August 2013.

Bennett, C and Raab. C., The Governance of Privacy: Policy Instruments in Global Perspective, 2006, MIT Press, pp. 12-13.

Bennett, C.J., 'Information Policy and Information Privacy: International Arenas for Governance' Journal of Law, Technology and Policy, 2002, pp 385-406.

---Regulating Privacy: Data Protection and Public Policy in Europe and United States, Cornell University Press, Ithaca/London 1992.

Bicchi, F., 'The European Origin of Euro-Mediterranean Practices', Working Paper No. 12, California, 2004.

Birnhack M. D., 'The EU Data Protection Directive: An Engine of a Global Regime' Computer & Security Review, 2008, Vol.24, No.6, pp. 508-520.

Borena, B et al., 'Information Privacy Protection Practices in Africa: A Review Through the Lens of Critical Social Theory', 48th Hawaii International Conference on System Sciences, 2015, pp.3490-3497.

Boshe, P., 'Evaluation of the Data Protection Bill in Tanzania', Privacy Laws & Business International Report, 2014, No. 127, pp. 25-26.

---'Interception of communications and the right to privacy: commentary on Zitto Zuberi Kabwe's political saga', Open University Law Journal, 2013, Vol.4, No.2, pp.1-5.

Boukongou, J. D., 'The Appeal of the African System for Protecting Human Rights, AHRLJ, 2006 Vol. 6, pp. 268-298.

Bygrave, L. A., 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol. 6, pp. 247–284.

---'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, 2010, Vol. 56, pp. 165-200.

---'Privacy Protection in a Global Context: A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, pp. 319-348.

---Data Privacy Law: An International Perspective, Oxford University Press, UK, 2014.

---Data Protection Law: Approaching its Rationale, Logic and Limit, Kluwer Law International, 2002.

Caruana, M. M. and Cannataci, J. A., 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States', Information & Communications Technology Law, Vol 6 No. 2, 2007, pp. 99-124.

Castells, M et al., Mobile Communication and Society: A global perspective. Cambridge, Mass.: MIT Press, 2007.

Chalton, S., 'The Court of Appeal's interpretation of "personal data" in Durant v FSA: a welcome clarification, or a cat amongst the data protection pigeons?', Computer Law and Security Report, 2004, Vol. 20 No. 3, pp. 175-181.

Church, J et al., Human Rights from a Comparative and International Law Perspective, UNISA Press, 2007.

Clarke, R., 'Information Technology and Datavaillance', Communications of ACM, 1988, Vol. 31, No. 5, pp.498-512.

Cohen, J.L., 'What Privacy Is For' , Harvard Law Review, 2013, Vol.126, pp. 1904-1933.

CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Burkina Faso, 2010.

CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Mauritius, 2010.

CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Tunisia, 2010.

CRID, Analyse du Niveau d'Adequation du Systeme de Protection des Donees dans le Royaume du Maroc, 2010.

Cuijpers, C., 'A Private Law Approach to Privacy: Mandatory Law Obliged?', SCRIPTed, 2007, Vol.4, No.4, pp.304-318.

David, R and Brierley, J.E.C., Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law, (3rd ed), Stevens & Sons, London, 1985.

De Cruz, P., Comparative Law in a Changing World, Cavendish Publishing Limited, London/Sydney, 2nd ed., 1999.

De Hert P and Gutwirth S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., et al (Eds), Reinventing data protection?, Springer Science, Dordrecht, 2009, 3-44.

---'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., et al (Eds), Reinventing data protection?, Springer Science, Dordrecht, 2009, 3-44.

Der Datenschutz im grenzüberschreitende Datenverkehr: Eine rechtsvergleichende und kollisionsrechtliche Untersuchung,Baden-Baden: Nomos, p. 87.

Diamonds, L., 'Introduction to Democratization in Africa', in Liberalism' in Diamonds, L and Plattners, M.F (Eds), Democratization in Africa, John Hopkins University Press, 1999.

Dogbey, G. Y., 'Towards Strategic Vision for a Continent in Distress' in Adesida, O and Oteh, A (Eds), African Voices - African Visions, The Nordic African Institute, Stockholm, Sweden, 2001, pp. 37-38.

Donovan, K. P and Martin, A. K., 'The Rise of African SIM Registration: the Emerging Dynamics of Regulatory Change', First Monday, 2014, Vol. 19, No. 2-3, DOI: http://dx.doi.org/10.5210/fm.v19i2.4351.

Electronic Privacy Information Centre and Privacy International, 'Overview of Privacy' in Privacy and Human Rights Report, 2006.

EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final respectively.

EU Commission 'A comprehensive approach on personal data protection in the European Union' (Communication From the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions), Brussels, 4.11.2010, COM(2010) 609 final.

FFC, Report on the legal obligations for encryption of personal data in Europe and Asia, 2013.

Fleischer, P., 'The Need for Global Privacy Standards' UNESCO Conference, Ethics and Human Rights in Information Society, 13-14 September 2007, Strasbourg.

Freedman, L.M., 'Legal Culture and Social Development', Law & Society Review, 1969, Vol. 4, No. 1, pp. 29-44.

Frémont, J., 'Legal Pluralism, Customary Law and Human Rights in Francophone African Countries' Victoria University of Wellington Law Review, 2009, Vol.40, No.1, pp. 149-166.

Frowein, J.A. and Peukert W, Europaische Menscheurecht Konvention: EMPK-Kommentar, Kehl an Rhein: NP Engel, 1996.

Gavison, R., 'Privacy and the Limits of Law', Yale Law Journal, 1980, Vol.3, No.89, pp. 421-471.

Gentili, A. M., 'Party systems and Democratisation in Sub-saharan Africa', Paper presentation at the Sixth Global Forum on Reinventing Government, Seoul, Republic of Korea, 24-27 May 2005.

Gerety, T., 'Redefining Privacy', Harvard Civil Rights-Civil Liberties Law Review, 1977, Vol. 12, No. 2, pp. 233-296.

Golafshani, N., 'Understanding Reliability and Validity in Qualitative Research', The Qualitative Report Volume, 2003, Vol. 8, No. 4, pp. 597-607.

Greenleaf, G and Bygrave, L.A., 'Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection', Privacy Laws & Business International Report, 2011, No. 111, pp. 8-9.

Greenleaf, G and Georges, M., 'The African Union's data privacy Convention: A major step toward global consistency?, Privacy Laws & Business International Report, 2014, No. 131, pp. 18 - 21.

Greenleaf, G., 'APEC Privacy Principles: More Lite with every version', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 105-111.

---'APEC's Privacy Framework: A New Low Standard', Privacy Law & Policy Reporter, 2005, Vol. 11, pp.121-124.

---'Australia's APEC Privacy Initiative: The Pros and Cons of the "OECD Lite"', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 1-6.

---'The influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108', International Data Privacy Law, 2012, Volume 2, No. 2, pp. 68-92.

Gutwirth, S., Privacy and the Information Age, Lanham/Boulder/New York/Oxford/ Rowman & Littlefield Publ., 2002.

Gyima-Boadi, E., 'The re-birth of African Liberalism' in Diamonds, L and Plattners, M.F (Eds), Democratization in Africa, John Hopkins University Press, 1999.

Héritier, A.,(ed)., Common Goods: Reinventing European and International Governance, Rawman & Littlefield, Boulder/New York/ Oxford, 2002.

Hickford, M., 'A Conceptual Approach to Privacy', Miscellaneous Law Reform Commission Paper no. 19, Wellington, New Zealand, October 2007.

Himonga, C., 'The Right to Health in an African Cultural Context: The Role of Ubuntu in the Realization of the Right to Health with Special Reference to South Africa', Journal of African Law, 2013, Vo.57, pp 165-195.

Hoffmann, E., Lost in Translation, London, Minerva, 1991, pp. 272-275.

Hunt, D. L. C., 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for Development for Canada's Fledgling Privacy Tort', Queens Law Journal, 2011, Vol.1, No. 37, pp. 167- 219.

Ibhawoh, B., 'Between Culture and Constitution: Evaluating the Cultural Legitimacy of Human Rights in the African State', Human Rights Quarterly, 2000, Vol.22, No.2, pp. 838-860.

IRMT, Fostering Trust and Transparency in Governance: Investigating and Addressing the Requirements for Building Integrity in Public Sector Information Systems in the ICT Environment the case study of Tanzania, January 2007.

Irving, J., 'For better or for worse: the euro and the CFA franc', United Nations Department of Public Information, 1999, Vol. 12, No. 4 pp. 24-29.

ITU., 'The Missing Link', Report for the independent communications for World Wide Telecommunication Development, 1985.

Jagessar, U and Sedgwick, V., 'When is personal data not "personal data": The impact of Durant v FSA', Computer Law and Security Report, 2005, Vol. 21 No. 6, pp. 505-511.

Johnson, S. D., 'Will our research hold up under scrutiny?', Journal of Industrial Teacher Education, 1995, Vol. 32 No.3, pp. 3-6.

Kamga, S.D., 'An Assessment of the Possibilities for Impact Litigation in Francophone African Countries', AHRLJ 2014, Vol. 14, 2014, pp. 449-473.

Kearney, A. T., 'African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services'; GSM Association, http://www.gsma.com/spectrum/wp-content/uploads/2011/12/Africa-Mobile-Observatory-2011.pdf.

Keetharuth, S. B., 'Major African Legal Instruments', in Bösl, A and Diescho, J(Eds), Human Rights in Africa: Legal Perspectives on their Protection and Promotion, Macmillan Education, Namibia, Windhoek, 2009.

Keith, C.K and A. Ogundele., 'Legal Systems and Constitutionalism in Sub-Saharan Africa: An Empirical Examination of Colonial Influences on Human Rights', Human Rights Quarterly, 2007, Vol. 29, No. 4, pp. 1065-1097.

Keith, T.I., 'An examination of the commercial and noncommercial appropriation of persona within the United Kingdom, with a comparative analysis with common and civil law countries', LL.M thesis, Durham University, 2011.

Kirby, M., 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' International Privacy Law, 2011, Vol. 1, No. 1, pp. 6-14.

Kitipov, J., 'African Local Integration and Multilateralism: The Regional Economic Communities and Their Relationship with the European Union', E-paper No. 16 November 2011.

Koops, B., 'The trouble with European data protection law', International Data Privacy Law, 2014, Vol. 4, No. 4, pp. 250-261.

Korff, D (ed)., Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Case study Germany, 2010.

---Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Case study France, 2010.

---'Report on Implementation of the Data Protection Directive: Comparative Summary of National Laws', Cambridge-UK, September 2002.

---'Study on the Protection of the Rights and Interests of Legal Persons with Regards to the Processing of Personal Data relating to such Persons', Final Report to the EC Commission, October 1998.

Krygier, M., 'Is there Constitutionalism after Communism?: Institutional Optimism, Cultural pessimism, and the Rule of Law', International Journal of Sociology 1996-1997, Vol. 26, No. 4, pp.17-47.

Kuner, C., 'International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review, 2009, Vol.25, No.4, pp. 307-317.

Kuner, C., European Data Protection Law: Corporate Compliance and Regulation (2nd Edition), Oxford University Press, UK, 2007, pp. 34-35.

Lacey, N., A Life of H. L. A. Hart: The Nightmare and the Noble Dream, Oxford University Press, Oxford, 2006.

Leclercq, F., A francophone BCR model to boost African data protection, Data Protection Law & Policy September 2013.

Lee, D. J et al., 'Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection', MIS Quarterly, 2011, Vol. 35, No.2, pp. 423-444.

Legrand, P., 'What 'Legal Transplants'? in Nelken, D and Feest, J., (eds), Adapting Legal Cultures, HART Publishing, Oxford-Portland-Oregon, 2001, pp. 55-69.

Lober, S., 'Data Protection and Subject Access Requests', Industrial Law Journal, Vol. 33, No. 2, 2004, pp. 179-190.

Long, W.J and Quek, M.P., 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbor Compromises', Journal of European Public Policy, 2002, Vol.9, No. 3, pp. 325-344.

LRDP Kantor Ltd and Centre for Public Reform., Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Final Report, 20 January 2010, pp.27-42.

Maamri, N., Free Trade Areas, Euro-Mediterranean Partnership and Prospects of South-South Integration in The Mediterranean, http://emo.pspa.uoa.gr/data/papers/7_paper.pdf.

Maina, C.P and Othman, H., Peter C M Othman H (eds.) Zanzibar and the Union Question, Zanzibar Legal Services Centre, 2006.

Makulilo, A. B., 'The Right to Privacy Relating to Credit Reporting: A Critical Review of the Emerging Africa's Credit Reference Market#, Journal of Internet Law, 2016, Vol. 19, No. 9, pp. 3-17.

---'"One size fits all": Does Europe impose its data protection regime on Africa?', Datenschutz und Datensicherheit (DuD), 2013, Vol. 37, No.7, pp. 447-451.

---'Data protection and law reform in Africa: a systematic or flawed process?', International Journal of Technology, Policy and Law, 2016, Vol. 2, Nos. 2/3/4, pp. 228-241.

---'Data Protection Regimes in Africa: too far from the European 'adequacy' standard?', International Data Privacy Law, 2013, Vol. 3, No. 1, pp. 42-50.

---'Mauritius Data Protection Commission: an analysis of its early decisions', International Data Privacy Law, 2013, Vol.3, No.2, pp.131-139.

---'Myth and reality of harmonisation of data privacy policies in Africa', Computer Law & Security Review, 2015, Vol.31, No.1, pp.78-89.

---'Privacy and Data Protection in Africa: A State of the Art', International Data Privacy Law, 2012, Vol.2, No.3, pp. 163-178.

---'Protection of Personal Data in Sub-Sahara Africa', PhD thesis, Universität Bremen, 2012.

---'Data Protection Regimes in Africa: too far from European 'adequacy' standard?', International Data Privacy Law, 2013, Vol.3, No.1, pp.42-50.

Mancuso, S., 'The New African Law: Beyond the Difference Between Common Law and Civil Law', Annual Survey of International & Comparative Law, 2008, Vol. 14, No. 1, pp. 39-60.

Matondo, M.J., 'Cross-Cultural Values Comparison between Chinese and Sub-Saharan Africans', International Journal of Business and Social Science, 2012, Vol. 3, No. 11, pp. 38-45.

Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010.

Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004)

Mayer, H., 'Europe's Post-Colonial Role and Identity', in Adebayo, A. and Whiteman, K(eds), The EU and Africa: From Eurafrique to Afro-Europa, C. Hurts & Co Ltd, United Kingdom, 2012.

Mayer, J., 'Globalisation, Technology Transfer and Skill Accumulation in Low-Income Countries', United Nations Conference on Trade and Development, Geneva, August, 2000.

Mbaye, K., Les Droits de l'Homme en Afrique (Second Edition) Pedone, 2002, pp. 71-73.

Mbazira, C., 'Enforcing the economic, social and cultural rights in the African Charter on Human and Peoples' Rights: Twenty years of redundancy, progression and significant strides', African Human Rights Law Journal, 2006, Vol.6, N.2, pp. 333-357.

Mbondenyi, K. M and Ojienda, T., 'Introduction to and overview of constitutionalism and democratic governance in Africa' in Mbondenji, K.M and Ojienda, T (Eds)., Constitutionalism and Democratic Governance in Africa: Contemporary Perspectives from Sub-Saharan Africa, Pretoria University Law Press, 2013.

Moerel, L., 'Back to Basics: When does EU Data Protection Law apply?', International Data Privacy Law, 2011, Vol.1, No.2, pp. 92-110.

---'The long arm of EU Data Protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by website worldwide?', International Data Privacy Law, 2011, Vol.1, No.1, pp.28-46.

Moreham, N.A., 'Privacy in the Common Law: A Doctrinal and Theoretical Analysis', Law Quarterly Review, 2005, Vol. 4, No. 121, pp. 628-656.

Mutua, M., Justice under Siege: The Rule of Law and Judicial Subservience in Kenya, Human Rights Quarterly, 2001, Vol. 23, No.1, pp. 96-118.

Napier, B., 'International Data Protection Standards and British Experience',Informatica e diritto, 1992, Vol. 2, No.1 , 1992, pp. 83-85.

Neethling, J et al., Neethling's Law of Personality, Butterworth, Durban, 1996.

---'The Concept of Privacy in South African Law', The South African Law Journal, 2005, Vol.122, No.1, pp.18-28.

Nelken, D., 'Towards a Sociology of Legal Adaptation' in Nelken, D and Feest, J (eds), Adapting Legal Cultures, Hart Publishing, USA, 2001, pp. 25-26.

Nyerere, J.K., Freeedom and Development/Uhuru na maendeleo, Oxford University Press, 1973.

Okeke, C.N., 'African Law in Comparative Law: Does Comparativism Have Worth?', Roger Williams University Law Review, 2011, Vol. 16, No. 1, pp.1-50.

Okoth-Ogendo, H.W.O., Constitutions without Constitutionalism: Reflections on an African Paradox, in Constitutionalism and Democracy: Transitions in the Contemporary World (Douglas Greenberg, et al. eds., 1993).

Olaoba, O.B., African Traditional Methods of Conflict Resolution, NOUN, 2010.

Olasunkanmi, A., 'Liberalism Versus Communal Values in Africa: A Philosophical Duel', IOSR Journal of Humanities and Social Science, 2013, Vol.12, No.5, pp.78-81.

Olinger, H. N et al., 'Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol.39, No. 1, pp. 31-42.

Onipede, K.J and Phillips, O.F., Cultural Values: Index for Peace and Branding Africa, Ladoke Akintola University of Technology, Nigeria.

Onwubiko, O. A., African Thought, Religion & Culture, Enugu, SNAAP, 1991.

Onyango, P., African Customary Law: An Introduction, LawAfrica, Kenya, 2013.

Patton, M. Q., Qualitative Evaluation and Research Methods, (3rd ed.), Sage Publications, Thousand Oaks, CA, 2002.

Pityana, N. B., 'Reflections on the African Court on Human and Peoples' Rights', AHRLJ, 2004, Vol. 4, pp. 121-129.

Polcˇa´k, R., 'Getting European data protection off the ground', International Data Privacy Law, 2014, Vol. 4, No. 4, pp. 282-289.

Postolache, A., New Challenges in the Relation between the European Union and the Mediterranean, http://www.analyticalmk.com/files/2012/01/02.pdf.

Prempeh, H.K., 'Africa's "constitutionalism revival": False start or new dawn?', International Law Journal, Vo.l5, 2007, pp. 469-506.

Raab, C.D and Bennett, C.J., 'Protecting Privacy across Borders: European Policies and Prospects', European Policies and Prospects', Public Administration, 1994, Vol.72, pp.95-112.

Rauhofer, J., 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?', EDPL, Vol 1, 2015, pp. 5-15.

Reding, V., 'The European data protection framework for the twenty-first century', International Data Privacy Law, 2012, Vol. 2, No. 3, pp. 119-129.

---'The Upcoming Data protection Reform for the European Union', International Data Privacy Law, 2011, Vol 1, No. 1, pp. 3-5.

Rempell, S., 'Privacy, personal data and subject access rights in the European Data Directive and implementing UK statute: Durant v Financial services authority as a paradigm of data protection

nuances and emerging dilemmas', Florida Journal of International Law, 2006, Vol. 18, pp. 807-840..

Rich, C., 'Privacy laws in Africa and Middle East', Privacy & Security Law Report, Vol.14, 2014.

Roos, A., 'Data protection' in van der Merwe, D., Information Communication Technology Law, LexisNexis, South Africa, 2008.

---'Privacy in the Facebook Era: A South Africa Legal Perspective, South African Law Journal, 2012, Vol. 129, No. 2, pp. 375-402.

---'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', LL.D Thesis, UNISA, 2003.

---'Definition of the Problem: The Impossibility of Compliance with both European Union and United States', Transnational Law & Contemporary Problems, 2005, Vol. 14 No. 3, pp1137-1162.

Rotenberg M and Jacobs D., 'Updating the Law of Information Privacy: The New Framework of The European Union', Harvard Journal of Law & Public Policy, 2013, Vol. 36, No. 2, pp. 605-652.

Saad, A. R., 'Information Privacy and Data Protection: A Proposed Model for the Kingdom of Saudi Arabia', Abdul Raman Saad & Associates, Malaysia, 1981.

Saldana, J., The Coding Manual for Qualitative Researchers, SAGE Publications Ltd, 2009.

Schmidl, M and Krone, D., 'Germany DPAs Decide EU-U.S. Safe Harbor May Not Be Relied Upon Exclusively', http://www.bnai.com/GermanyDpas/default.aspx.

Schoeman, F.D., Privacy and Social Freedom, Cambridge University Press, USA, 1992.

Solove, D., 'A Taxonomy of Privacy', University of Pennsylvania Law Review 2006, Vol. 154, No.3, pp. 477-560.

South African Law Reform Commission, Issue Paper 24, Project 124, Privacy and Data Protection, http://www.justice.gov.za/salrc/ipapers/ip24_prj124_2003.pdf.

Stefano, K., 'Computer Diffusion in Black Africa: A Preliminary assessment' in Shubash, B and Bjorn-Anderson, N., (Eds), Information Technology in Developing Countries, Holland: Elsevier Science Publisher B.V, 1990.

Svantesson, D.J.B., 'A "Layered Approach" to the Extraterritoriality of Data Privacy Law', International Data Privacy Law, 2013, Vol. 3, No.3, pp. 278-286.

Tabalujan B.S, Legal Development in Developing Countries: The Role of Legal Culture, Singapore, 2001

Thiam, N. F. G., ICT in Senegal: Management, Public uses and Perspectives, GOVTECH Conference, 5-8 September 2010, Durban-South Africa.

Time, V.M,'Legal Pluralism and Harmonization of Law: An Examination of the Process of Reception and Adoption of Both Civil Law and Common Law in Cameroon and Their Coexistence with Indigenous Laws', International Journal of Comparative and Applied Criminal Justice, Spring 2000, Vol. 24, No. 1, pp. 19-29.

Treacy, B and Bapat, A., 'Purpose limitation – clarity at last?', Privacy & Data Protection Journal, 2013, Vol. 13 No. 6, pp. 11-13.

Umuzurike, U., The African Charter on Human and Peoples' Rights, 1997.

UNCTAD, Review of e-commerce legal harmonization in economic community of West African states, Switzerland, 2015.

UNGA, National Report Submitted in according with para 15(a) of the Annex to the Human Rights Council Resolution 5/1- United Republic of Tanzania, Geneva, 3-14 October 2011.

UNGA, Summary Prepared by the Office of the High Commission for Human Rights in accordance with paragraph 15 (c) of the annex to Human Rights Council Resolution 5/1, Geneva, 3-14, 2011.

UNGA., Individual Report of the Tanzania National Human Rights Institutions-Submission to the Human Rights Council: Universal Periodic Review, 12th Session 2011.

URT, Proposal for Enacting Cyber Laws in Tanzania, Dar es Salaam, January 2013.

Walden, I., 'East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework', Draft v.1.0, 2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008.

Warren, S.D and Brandeis, L.S., 'The Right to Privacy', Harvard Law Review, 1890, Vol. 4, No. 5, pp. 193-220.

Watson, A., Legal Transplant: An Approach to Comparative Law, 2nd Ed, London, The University of Georgian Press, 1993.

Wiley, J., 'The Globalisation of Technology to Developing Countries', Global Studies Student Papers, Paper No.3, http://digitalcommons.providence.edu/glbstudy_students/3.

Wilson, G., 'Comparative Legal Scholarship' in W.H Chui, and M. McConville, (eds), Research Methods for Law, Edinburg University Press, 2010, pp. 87-103.

Wolfgang, K., 'Germany' in Rule, J.B and Greenleaf, G (eds)., Global Privacy Protection: The first Generation, Edward Elgar, Cheltenham, Uk and Northampton, MA, US, 2008, pp.80-106.

Yonazi, E et al(Eds)., 'The Transformational Use of Information and Communication Technologies in Africa', eTransform Africa.

Zafar, A and Kubota, K., 'Regional integration in central Africa: key issues', World Bank African Region Working Paper Series No. 52, June 2003, World Bank.

Zurawski, N., 'Increasing Resilience in Surveillance Societies: Germany Country Reports' http://irissproject.eu/wp-content/uploads/2014/06/Germany-Composite-Reports-Final1.pdf.