ASSESSING THE RELEVANCE OF THE EXISITNG LEGAL REGIME IN TANZANIA FOR DATA PROTECTION

ELIZABETH ANDREW MAMBA

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE MASTER OF LAW DEGREE IN INFORMATION TECHNOLOGY AND TELECOMMUNICATION (LL. M IT & T) OF THE OPEN UNIVERSITY OF TANZANIA

2013

CERTIFICATION

The Undersigned certify that he have read and hereby recommend for examination a Dissertation entitled, **Assessing the Relevance of the Existing Legal Regime in Tanzania for Data Protection**; in partial fulfilment for the Award of Master of Law Degree of the Open University of Tanzania

…….

Prof. Ian J. Lloyd

(Supervisor)

Date: …….

DECLARATION

I, Elizabeth Andrew Mamba, declare that this Dissertation is my own original work and that it has not been presented and will not be presented to any other University for a similar or any other degree award.

…….

Signature

…….

Date

COPYRIGHT

DEDICATION

This dissertation is dedicated to my three loving kids, Gloria, Augustine and Leonard for their inspiration and brighter future.

My dedications go to my deceased parents Mr. Yuda Mtama and Mrs. Margaret Mtama who brought me to this world and up in the way I am today and my deceased guardian Mr. Andrew Mamba whose support throughout my schooling life saw me to all the success I have.

AKNOWLEDGEMENTS

I firstly acknowledge the blessings of the Almighty God who made this study succeed. I also express my sincere gratitude to my supervisor Professor Ian Lloyd, to whom I am much indebted for his great support and advice throughout the pursuit of this research.

I am also much indebted to my Course Coordinators at the Open University of Tanzania, Dr. Susan Kolimba and Mr. Gervas Yeyeye for their guidance and encouragement throughout the time of studying the entire program and finally this research.

Fourthly, I grateful for the immense support of all stakeholders in information security within and beyond the Government; Ministry of Higher Education, Science and Technology, for their support despite their busy schedules, the High Court of Tanzania (Commercial Division), the police Force of Tanzania, and private law firms.

Fifthly, also thank my close friend Mr. Innocent Mwaluki who offered his encouragement and moral support which is valuable to my work. Lastly, my colleagues, Tumaini Silaa, Bernadetha Mnkandya, Shukya Kiroga and His Lordship, Mr. Nyangarika, J. and all those who in one way or another played a role in making this work a reality but are not mentioned here, are highly appreciated.

ABSTRACT

Tanzania is among countries embarked upon the use of ICT for national development. One of the major challenges is cyber security, which if not dealt with; it results into undesirable adverse consequences. The research examines Tanzania's efforts in overcoming the challenges in a legal perspective and make necessary recommendations for drastic measures to be taken. Chapter one introduces the research work, giving the essence of personal data protection. The statement of the problem is that cyber security in Tanzania is poor to date despite the country indulging into the use of ICT as a fact of life. The background of the existing problem is identified as lack of relevant laws to match with e-crimes compelling law enforcers to use traditional laws. The government's hesitant behaviour is also a backdrop of the problem. The main objectives of the study are to critically examine the Tanzanian position on personal data protection and assessing the existing legal framework and the extent of cyber crime. The study is significant to point out the risks of failure to install a sound legal framework and recommend measures to be taken. Chapter two discusses personal data protection issues, nature of data, supply, processing, storage, its flow, control and its use. Chapter three covers research methodology which involved text books, statutes, journals, and other online materials plus personal interviews. Chapter four gives current status of cyber security in Tanzania resulting from the research. The status of cyber security in Tanzania is confirmed to be still poor for lack of the necessary legal framework. Personal data protection is absent putting privacy rights at a menace. Chapter six makes observations, recommendations and conclusions of the research work, recommending for radical measures for the Government to formulate a sound legal framework for information security and enact personal data protection law.

TABLE OF CONTENTS

LIST OF CASES

1. Case C-101/01 Bodil Lindqvist
2. Avnish Bajaj v. State 150 (2008) DLT 769: (2008) 105 DRJ 721
3. Foundation v. UPC Nederland (unreported, July 2006)
4. R v. Gold (1987) 3 All ER 680 affirmed by House of Lords in (1988) 2 All ER 186
5. Trust Bank Limited v. Le-Marsh Enterprises et al [2002]TLR 144
6. Tanzania Cotton Marketing Board v. Cogecot Cotton Company SA [1997] TLR 165 (CA)
7. High Court of Tanzania (Commercial Division) Commercial Case No. 42 of 2011 Dodsal Hydrocarbons & Power Limited et al v. Hasmukh Bhagwanji Masrani (Unreported)
8. High Court of Tanzania (Commercial Division) Commercial Case No.10 of 2008: Lazarus Mirisho Mafie et al v. Odilo Gasper Kilenga alias Moiso Gasper

(Unreported)

9. High Court of Tanzania (Commercial Division) Commercial Case No. 3 of 2010: Vodacom Tanzania Limited v. African Banking Corporation (unreported)
10. High Court of Tanzania (Commercial Division) Commercial Case No. 5 of 2006: Oyster-bay Hospital Limited v. University Computing Centre (unreported)
11. High Court of Tanzania (Commercial Division) Commercial Case No. 32 of 2005: Mark Foley v. Robert Thomson et al (unreported)
12. High Court of Tanzania (Commercial Division) Commercial Case No. 42 of 2004: Prismo University Italiana s.r.1 v. Termcotank (T) Limited (unreported)

LIST OF LEGISLATION

A. International Legislation

1. The Indian Penal Code, 1860,
2. The Indian Evidence Act, 1872,
3. The Bankers' Book Evidence Act, 1891 (of India)
4. The Reserve Bank of India Act, 1934
5. The Data Protection Act 1998 (of UK)
6. The European Directive on Data Protection
7. Statutory Instrument 2000 No. 417: the Data Protection (Processing of Sensitive Personal Data) Order 2000

B. Local Statutes

1. The Constitution of the United Republic of Tanzania, 1977 as amended in 1984
2. Sheria ya Mabadiliko ya Tano ya Katiba ya Nchi, ya Mwaka 1984, Act No. 15 of

1984 (The 5th Constitutional Amendment Act, No. 15 of 1984)

3. Criminal Procedure Act, Cap 20 R. E 2002,
4. Evidence Act of Tanzania Cap 6 R. E. 2002,
5. Penal Code Act, R. E. 2002 Cap 16,
6. Copyright and Neighbouring Rights Act Cap 33 R. E 2002
7. The bank of Tanzania Act, No. 4 2006
8. The Banking and Financial Institutions Act No. 5 of 2006,
9. The Business License Act Cap 273 R. E. 2002
10. The Capital Market and Securities Act Cap 79 R. E. 2002,
11. The Carriage of Goods by Sea Act Cap 164 R. E. 2002
12. The Electronic and Postal Communications Act No. 3 of 2010
13. The Universal Communications Services Access Act, No. 11 of 2006
14. The Written Laws (Miscellaneous Amendments) Act No. 15 of 2007
15. Statutory Instrument 2002 No. 2905: The Data Protection (Processing of Sensitive Personal Data) (Elected Representative) Order 2002
16. Information Commissioner's Office, The Guide to Data Protection,
17. The Information Technology Act, 2000 of India
18. Directive 95/46 of European Parliament and Council of 24 October, 1995 on Protection of Individuals with Regard To Processing Of Personal Data and Free Movement of Such Data.
19. Directive 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15th March 2006 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

ABBREVIATIONS

ATM	Automated teller Machine
BPO	Business Process Outsourcing
EA	East Africa
EU	European Union
ICT	Information and Communications Technology
OECD	Organization for Economic Cooperation and Development
SA	South Africa
SADC	Southern Africa Development Cooperation
TCRA	Tanzania Communications Regulatory Authority
UK	United Kingdom
USA	United States of America

CHAPTER ONE

1.0 INTRODUCTION

1.1 Overview

The importance of information communication technology (ICT) as a vehicle to development in the 21st Century cannot be underestimated. ICT has become such a reality and a fact of life in the modern world that one cannot do without. As ICT facilitates easy access to information and communications in both commercial and non commercial undertakings, infringement of personal information is likely to occur. For that reason this research will be confined to personal data aspect of ICT as an embryo for telecommunication.

The research has been prompted by the gap that exists between cyber space activities and the need for related laws for its regulation. ICT is a new creature of mankind employing cyber space to enhance ways of doing business and lifestyles to obtain far reaching benefits. For instance, payment of taxes has changed from the traditional paper based to electronic processes which ensure the Government maximum revenue collection. But this also means movement of personal data at the expense of privacy, as misuse of such data may cause far reaching damage to not only human dignity but also the development we are seeking.

In Tanzania, the Constitution provides for respect and protection to the privacy of an individual, family, matrimonial life, residence and private communications, making it necessary to enact laws that protect and guarantee the right to privacy[1].

[1] Article 16 (1) and (2) of the Constitution of the United Republic of Tanzania 1977, as amended by Act No. 15 of 1984 during which the Bill of Right was entrenched.

In Tanzania, therefore, privacy is a human right protected by the Constitution. However, to date, the Government has not enacted a law to this effect.

Inevitably, the country has joined the world of information technology, employing digital devices in everyday activities, allowing high flow of data electronically within and without. The laying of sea cables (SEACOM) that connects East Africa to other parts of the world has even enhanced performance in telecommunications to higher standards rendering the world as a global society, people engage in electronic business transactions daily. Unfortunately, the developments create legal insecurity as crimes against personal data follow suit. This necessitates creating conducive legal mechanism for personal data protection against all types of abuse which are an obvious occurrence in this 'information age' to encourage e-business. Regrettably, the legal framework in Tanzania does not adequately address all issues of cyber security, particularly personal data protection apart from the national policy on ICT. Countries worldwide continuously promote information technology without forgetting to address challenges attached to it. Data protection principles, regulations and legislation, are formulated to deal with electronic violations as one of the major challenges to information security.

It therefore becomes imperative for Tanzania to have a distinct legal framework for information security as a vital component of ICT development. Government efforts are needed to legally protect data subjects through a comprehensive legal framework to ensure that criminals are brought to the hands of justice[2]. The transition to ICT

[2] Cited from http://www.doingbusiness.org/data/exploreEconomies/tanzania/ visited on 25th March, 2013 at 7.30 am

driven economy should be supported by legislative changes to incorporate cyber security for obtaining the desired results.

This research explores the extent to which Tanzanian legal system safeguards personal data as an information security phenomenon, proposing improvements to any existing gaps so as to have an ideal legal framework for information security that provides data protection against cyber violations. The position of data protection in the United Kingdom, European Union (EU) and the United States, and the famous eight fundamental principles [3] will be examined in a bid to borrowing a leaf from them.

1.2 Background to the Problem

The advent of computers and information technology has promoted personal information processing and storage electronically; allowing data processors to access one's information supplied including sensitive personal information. In the process ICT has revealed itself as a vital tool for social, educational and economic developments to mention a few. However the use of ICT brings with it challenges that need drastic measures to keep pace with the technological developments and achieve the desired results. Illegal access to and misuse of personal data are some of the major legal challenges in Tanzania as enterprises turn to online investments. These can only be addressed by legal mechanisms.

Up to now, ICT users suffer grievances which courts find it difficult to remedy due to lack of the relevant legal framework within which to operate. Traditional evidence

[3] Ibid

and criminal laws are still in use, while they cannot cope with the new challenges posed by the technological advancements. In the case of *Trust Bank Limited Versus Le-Marsh Enterprises et al*[4] the court had to exercise a contemporary mind and decide to admit electronic evidence though not admissible under the existing laws, in a bid to give a remedy to the aggrieved party in pursuit of justice. This indicates the need for a comprehensive legal framework adequately covering personal data protection to make cyber space secure.

1.3 Statement of the Problem

From 1990s, Tanzania ventured into using computers for simplifying work, communication and business transactions. Individuals often supply their sensitive personal particulars to be stored electronically. The use of e-government, e-banking and e-health services puts privacy rights at risk as the computer devices used are targets of electronic violations. This has serious implications on the legal regime of the country. The research starts with the hypothesis that Tanzania misses the necessary legal framework for personal data protection and intends to establish how the processed personal data can be protected under the law to a secure level[5].

In this digital era, information is an asset capable of being possessed, owned, processed or transferred. But like any other asset, information can be stolen, misused or destroyed causing damages to the possessor and/or owner and this makes information protectable by law. We more often than not experience unsolicited phone calls and messages, money theft through automated teller machines (ATMs)

[4] [2002] TLR 144, High Court Commercial Division Civil Case No. 4 of 2000
[5] Cited from http://www.doingbusiness.org/data/exploreEconomies/tanzania/protecting-investors/

are a common occurrence. All facts point to the truth that cyber security in Tanzania is still poor. The legal fraternity should be enabled to cope with new challenges as they occur and keep pace with ICT developments. Owing to the ever-growing nature of information technology more and new violations are likely to be conceived, which are more sophisticated [6] than the legal regime can face. Thus the legal system needs to equally adapt to change for its sustainability in the digital era.

This study will assess Tanzanian legal position in protecting personal data and privacy rights as enshrined in the Constitution and propose ways to fill existing gaps. It will compare with the United Kingdom laws, United States status, European Union position as well as the OECED Model Law, looking into the aspects worth emulating to Tanzanian legal framework as far as personal data protection is concerned.

1.4 Objectives of the Study

This work is aimed at attaining the following objectives:

i. To examine the policy of personal data protection in Tanzania
ii. To examine the extent of personal data infringements in Tanzania
iii. To establish the role played by the law in combating personal data infringements in Tanzania.
iv. To critically examine sufficiency of the legal regime on ensuring personal data protection.

[6] Hacking, bots and botnets, key loggers, website defacement, malware-viruses, distributed denial-of-service (DdoS) attacks, phishing, vishing, pharming, phreaking, identity theft, spoofing, rootkits, mobile malwares. Described by Aparna Viswanathan, "CYBER LAW":Indian & International perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes, Butterworths Wadhwa 2012 at pages 14- 23

v. To establish the effect of international laws, principles and regulations relating to data protection to Tanzanian legal system.
vi. To establish extent of awareness of the legal profession and the public on personal data protection and role of various stakeholders on the same.
vii. To establish challenges facing law enforcers in combating personal data infringements.
viii. To discuss the issues of privacy rights and the right to information in relation to personal data protection.
ix. To give recommendations on whatever lacuna identified in the country's legal frameworks as far as personal data protection is concerned.

1.5 Significance of the Study

The ever changing character of information technology necessitates the law to evolve to promote technological progress while at the same time protecting the society against abuse. This study is needed for matching the legal system with the speedy advancements in ICT, particularly:

i. To add on the existing limited knowledge about personal data protection in Tanzania.
ii. Providing literature on personal data protection as a feature of fundamental right to privacy.
iii. Pointing out data protection issues in Tanzania, because individuals supply their personal information electronically in banking services, hospitals, various government institutions, business and other online services, without knowing the challenges facing cyber security in Tanzania.

iv. Offers a critical assessment on the existing legal regime pertinent to personal data protection in Tanzania and its effectiveness to the prevalent abuse to personal data.
v. To enable the Government achieve best results in ensuring fundamental privacy rights, cultivate harmonious fight against misuse of personal data with other ICT user countries.
vi. Addressing prevailing gaps in the existing laws and charting out the best personal data legal protection.

Ultimately, propose amendments or enactments of laws relating to personal data protection in Tanzania.

1.6 **Literature Review**

The Tanzanian ICT Policy 2003 was very promising on the review of the existing laws and regulations so as to create "conducive legal environment to the healthy growth of ICT"[7]. But up to the time of this research, Tanzania has no law for governing data protection in online transactions. If one is to measure the damage the country is suffering attributed to lack of the law the results would be breathtaking.

Taking for instance in financial services industry, most banks in Tanzania have installed ATMs for more convenience of both the banks and their customers in terms of time and charges, but in so doing exposing the customers' data at a risk of being viewed by a larger public. And as Mambi states, e-banking is growing explosively,

[7] Tanzania National Policy for ICT, 2003

while a legal framework that regulates personal data is lacking.[8] This poses legal issues of privacy rights since the use of electronic cards contain data protectable by law. Events of personal data infringements are being filed in court frequently and Judges are unsettled in what position to take since there is no guiding law on the subject. Some minds in the legal fraternity take a liberal position and extend interpretation of laws to cover new situations created by cyber activities as it happened in a case involving a CRDB bank branch manager who had to be charged with economic sabotage under the Economic and Organized Crimes Control Act for an e-crime due to lack of data protection law.[9]

The other side of the school of thought say that it is upon the legislature to change the laws and for law enforcers to apply them. It all brings up the point that a data protection law is particularly necessary. It is clear evidence that Tanzania needs to reform the legal framework to create an enabling legal environment to accommodate IT developments in relation to data protection which is very crucial for promotion of investment.

The existing law on electronic communications[10] does not give the requisite legal protection to data subjects despite compelling mobile phone subscribers to provide their personal information for registration of their sim cards.[11] It further empowers the Communications Regulatory Authority (TCRA) to keep a database of all subscribers' information for monitoring and supervision. The law marginalizes data

[8] Adam J. Mambi, ICT Law Book: A sourcebook for Information & Communication Technologies and Cyber law, Mkuki na Nyota DSM 2010, page 122
[9] Ibid Page 123
[10] The Electronic and Postal Communications Act No. 3 of 2010, Section 93
[11] Ibid Section 91

protection as it simply imposes a duty of confidentiality upon network operators regarding their customers' information.[12] In my view, the duty of confidentiality is not adequate coverage to issues of personal data protection to curb various possible infringements.

There are opposing views on the need for data protection law in various parts of the world. The first category represents state machineries of most countries which vies for cyber security law, which in essence is about having unrestricted legality to access personal data on grounds of national security and prevention of terrorism, the other category represents majority of the citizens who are the main data subjects, and this group cry for data protection. The unfortunate is obvious to happen since the state machineries have the upper hand being the law makers they might easily leave data protection in the peripheral.

In my view, marginalizing data protection is a grand error since both are important. As the government being not only one of the users and purchaser of ICT but also the regulator has the role of creating the necessary legal environment in which technology may grow through innovations and investments. The government should also ensure an effective and efficient delivery of information and services to the general public. This cannot be achieved without legal reforms to cope with ICT developments. Also having an adequate legal framework will pave way for enactment of laws which spell out specific requirements for regulation.

The inclination of the state machinery appears to lie on the criminal side of cyber

[12] Ibid Section 98

security. But based on Buckland's analysis of elements of e-crimes[13] it is more difficult to prove the accused guilty beyond reasonable doubt with five elements in e-crimes than it is in normal offences which have only two elements of *mens rea* and *actus reus.* This gives legal protection to data through civil laws a milestone as an alternative. Another factor worth considering is that cyber security as a concept is too broad to have a single regulating statute. It needs to be broken down into specific domains and have a distinct governing law for each. With that in mind the research is confined to personal data protection.

1.6.1 Regional Efforts

In 2012, SADC countries prepared a model law on data protection with the objective of combating misuse of personal data likely to arise from collecting, processing, transmission, storage and use of personal data[14] for each member country to adopt into their domestic laws in a harmonized way. This is intended to give guidance to member countries in formulating their domestic laws. The document has facilitated discussions in various forums[15] advocating for data protection. The SADC model data protection law is mindful of the need for cyber security thus provides in its guidelines for authorities to formulate legal procedures for preserving a person's right regarding the circumstances, manner and extent to which the right to privacy may be encroached upon legally.[16]

---

[13] Buckland, J. A. "Combating Crime: Prevention, Detection and Investigation" 1st Edition MacGraw – Hill, New York 1992 page 4. He mentions five elements namely; intent to commit a wrongful act, disguise of the intent, reliance on ignorance of the victim, voluntary victim action to assist the offender and concealment of the violation

[14] HIPSSA, Model Law on Data protection, ITU and EU 2012 at page 7

[15] Pria Chetty, (an International Legal Expert on Data Protection) and Baraka Kanyabuhinya, (a National Legal Expert on Data Protection) a Training on DATA PROTECTION LAW, HIPSSA Project, Support for Harmonization of the ICT Policies in Sub-Sahara Africa on 07th January 2013

[16] Ibid Article 16(2)

To achieve harmonization, Sub-Sahara African countries will need to spell out in their constitutions the need to enact laws that guarantee privacy rights including personal information. The Namibian ICT policy of 2009 conveys the country's position as being committed to promote information security and data protection and the protection of privacy, among others. The policy creates an obligation upon ICT telecommunication licensees to protect subscribers' privacy and comply with international standards.

1.6.2 Indian Position

India has been in continuous legal reforms to embrace information technology advancements since the start of this phenomenon. It has done a lot in terms of literature in the form of texts and statutes. The country enacted Information Technology Act, 2000 to allow growth of e-commerce[17] among others.

Apparently, keeping pace with the IT developments is an uphill task for the legal systems of all countries. As Justice Yatindra points out, the growth of information technology in this information age renders the law inadequate whenever dealing with new legal problems it poses in jurisprudence.[18] For instance, it is reported that the Information Technology Act, 2000 of India started to prove inefficient by failure to curb e-crimes that emerged from the use of digital facilities, in less than a decade. Several incidents of data identity theft of customers of international banks began to plague the Indian Business Process Outsourcing (BPO) industry.[19] This was

---

[17] Aparma Viswanathan Op. Cit page 25
[18] Justice Yatindra Singh, Ibid page 3
[19] ibid

facilitated by the fact that all filings with the registrar of companies since 2007, and all income tax returns since 2008 are made through e-filings.[20] This necessitated amending the IT Act, 2000 in 2008 and also in 2009. Other statutes are also said to have been amended by the Act in response to abuse of data[21] That is the situation where a legal framework is in place. What is the situation in Tanzania where there is none, is matter for the research.

1.6.3 South African Position

Deloitte[22] gives the situation in South Africa, on how the country gives importance to protection of personal information, through a bill on Personal Information, which will place them in line with the international data protection laws whereby personal data will be protected as they are processed by public and private organizations. South Africa recognizes that personal data protection addresses the challenges of individuals' privacy rights. Organizations are therefore required to comply with international principles on how to handle individuals' data by making relevant policies and procedures recognizing various forms of data protection as part of their business operations.

Deloitte elaborates that if information such as names, physical, postal or email addresses, identity numbers, employment history, health data pertaining to an individual, or if individuals' data is outsourced to third parties, the organizations are

[20] Ibid page 71

[21] Justice Yatindra Singh, "CYBER LAWS", 5th Edition, Universal Publishing Co. Ltd, 2012, refering to the Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 at page 4

[22] http://www.deloitte.com/view/en_ZA/za/marketsolutions/popi-act/index.htm#%3EUnderstanding%20the%20lmportance Visited on 25th March, 2013.

obliged to comply with principles on data protection. It is commonplace that all organizations have individuals' information concerning shareholders, employees, customers, suppliers and contractors. Therefore, protection of personal information affects every undertaking of their business. The South African Bill for processing individuals' information contains fourteen principles but the under listed are more relevant on protection of personal information.

i. Personal data must be collected directly from the data subject.
ii. A data subject has to consent before his/her personal information is processed.
iii. The information must be accurate and complete, which may necessitate updating to keep it as such.
iv. Trans-border data flow is restricted to contract purposes between the data subject and a trans-border firm, and consent has been sought and given in that regard.
v. Individuals have the right to request confirmation of their data from a company, and can make correction if they so wish.
vi. Data can only be collected for specific, explicit, and lawful purposes.
vii. The processing of personal data must be compatible with the stated purpose of collection.
viii. Personal information on sensitive data like health, ideology, race, politics, religion, or marital status has their own distinct rules under the Bill.
ix. Any further process of the individual's data than the initial purpose of collection, have to adhere to the above conditions as if processing for

the first time.

x. Individuals' information should be destroyed reasonably after the purpose for which they were processed is over, to keep the individual's integrity and privacy.

xi. The Bill also provides that companies should be responsible for not only the security but also the quality and integrity of data being processed and stored.

xii. The Bill also demands that security measures are to be kept in place in case a third party processes information on behalf of the company.

The essence of giving protection to data and specifically those relating to persons is that in the modern business world data is regarded as a valuable asset. Therefore, enterprises in South Africa are urged to adhere to law in safeguarding this asset. Social networking websites like MySpace, Face book, blogs, twitter and Friendster[23] are in the picture, where data subjects post sensitive personal data. Therefore the law should exist to be adhered to.

When a governing law exists non adherence to it has adverse repercussions which may include giving the business a negative impact. In September 2006, Face book introduced newsfeed feature which spurred additional privacy concerns from users. Almost over 700,000 users signed online petitions demanding the company to discontinue the feature on the basis that this compromised their privacy[24]. South Africa seems to be in the right track as the Bill covers a major part of data protection

[23] http://epic.org/privacy/socialnet/Visited on 25th March, 2013 at 11.00 a.m.
[24] Ibid

issues and might already have been passed into law by now.

1.6.4 International Position

Other parts of the world take collective measures to regulate ICT for giving guidance to individual countries in making their domestic laws to guarantee cyber security in relation to data transfer. The international community have done so much in ensuring that ICT is properly regulated and all developments are accordingly accommodated. Data protection has also been dealt with in breadth. The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data[25] provides on her preface that the development of automatic data processing, which enables huge quantities of data to be transmitted within seconds through national frontiers and across continents, has necessitated consideration on privacy protection pertinent to personal data.

The international community is mindful of the fact that data flow increases daily and is likely to grow further due to introduction of new versions of computers and advanced communication technologies, and take concern national legislation varies from one country to another. This is because they feel that these disparities can impede smooth flow of personal data across boundaries. They have justifiable fear that restrictions and prohibitions on the flow of data can cause serious disruptions in important sectors of the economy like banking, insurance and supply of goods and services.

That being the case, the OECD states considered it imperative to draw guidelines to

[25] http://www.oecd.org/ Visited on 26th March,2013

help them in harmonizing national privacy legislation upholding human rights but at the same time preventing interruptions in international data flows. The basic principle is drawn and taken as a benchmark to serve as a base for legislation in countries which have not yet arrived at this stage.

The Guidelines were developed in the form of recommendations by the Council of the OECD. The Council commissioned a group of experts which drew the Guidelines under the chairmanship of Hon. Mr. Justice M.D. Kirby; A Chairman of the Australian Law Reform Communication. These recommendations were adopted and become functional on 23rd September, 1980. The Guidelines provide on its part two *inter alia* for basic principles of national application namely;

i. The c*ollection Limitation Principle* which states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means; where appropriate with the knowledge or consent of the data subject.[26]

ii. The d*ata Quality Principle*. The data quality principle provides that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes. Data should be accurate, complete and kept up to date.[27]

iii. The p*urpose Specification Principle* which provides that the purposes for which personal data is collected should be specified not later than at the time of that collection and the subsequent use limited to the fulfilment of

[26] Section 7 of the Guidelines at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransboarderflowsofpersonaldata.htm#top. Visited on 26th March,2013.\

[27] Ibid Section 8

those purposes or such others as are not incompatible with those purposes and as specified on each occasion of change of purpose.[28]

iv. The *use limitation* principle demands that, personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph 9 save for: (a) with the consent of the data subject; or (b) by the authority of law.[29]

v. The s*ecurity safeguard* principle is another which states categorically that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.[30]

vi. The *openness principle* demands that there should be a general policy of openness about development, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[31]

vii. The *individual participation principle* which demands that an individual should have the right to;

viii. Obtain from a data controller or otherwise, confirmation of whether or not the data controller has data relating to him.

ix. To have communicated to him, data relating to him within a reasonable time at a change if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him.

[28] Ibid Section 9
[29] Ibid Section 10
[30] Ibid Section 11
[31] Ibid Section 12

x. To be given reasons if a request made under paragraphs (a) and (b) are denied, and to be able to challenge such denial.

xi. To challenge data relating to him and if the challenge is successful to have the data erased, rectified, completed or amended.[32]

xii. The *accountability* whereby a data controller is required to comply with measures which give effects to the above stated principles.[33]

These principles illustrate their importance in ensuring that member states adhere to the acceptable requirements on personal data protection. The work at hand will also assess whether Tanzania embeds such principles on personal data protection, or have anything of similar nature to ensure that personal information are legally protected. If not, the study may propose the same to be emulated to ensure that there is a well elaborated legislation on data protection in the country to get the economic benefits attainable from personal data protection including foreign investments to both public and private sectors.

The preamble to the guidelines however, states categorically that there are two contradicting but essential basic values involved in the phenomenon to wit protection of privacy rights against individual liberties and the advancement of free flows of personal data. The two values operate against one another, while accepting some restrictions to free trans-border flows of personal data they also seek to reduce the need for such restrictions and therefore strengthen the notion of free information

[32] Ibid Section 13
[33] Ibid Section 14

flows between countries.[34] The guidelines on their parts four and five contain principles which seek to ensure that there are effective national measures for the protection of privacy but at the same time allow individual liberties, avoiding practices of unfair discrimination between individuals, forming the basis for continued international cooperation and compatible procedures in any regulation of trans-border flows of personal data.[35]Undoubtedly, the principles are relevant and worth emulating to Tanzanian personal data protection legal regime.

On the part of the EU, the member countries have introduced relevant pieces of legislation on privacy protection (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden, and the United States) by enacting laws to that effect. The rest of the countries; Belgium, Iceland, Netherlands, Spain and Switzerland drafted Bills to curb violation of fundamental human rights including unlawful processing and/or storage of personal data, the storage of inaccurate personal data or unauthorized disclosure of such data.

Cornwall[36] discusses the legal framework of UK elucidating on how hard it is to protect data against abuse by traditional laws. This is evident that a separate legal regime is necessary for electronic data protection. This research will assess the Tanzanian legal regime consideration on privacy rights pertinent to personal data protection as necessitated by IT developments and usage, particularly whether users of ICT are protected, if so, to what extent.

---

[34] Ibid. in the Preamble
[35] Ibid Part iv & v
[36] Cornwall, H. "Data theft, Computer Fraud, Industrial Espionage and Information Crime" Heinemann Educational Books, London, 1987, page 321

1.6.5 Tanzania Position

As Tanzania already recognizes privacy rights in its Constitution, and since ICT has been integrated into our lifestyles and the way we do business, it goes without say that personal data needs legal protection, since the existing laws are rendered inadequate in dealing with the associated problems. In all the mobile phone networks operating in Tanzania we more often than not receive unsolicited emails and unwanted phone calls. And according to Chetty[37] loss of data, unauthorized intrusion to sim-cards and sim swapping are also common events. These are incidences of violation of right to privacy by misuse of personal information aggravated by lack of the proper legal mechanism to curb the situation.

The writer gives case studies, one of which is where subscribers of mobile phone companies in the country have complained of irritating unsolicited text messages and phone calls to their customers marketing their products, services, and offers without prior consent or subscription to those services by the mobile phone subscribers. This indeed is a violation to the right to privacy.[38]

The Government is mindful of the need for cyber security law stating in its national policy that any country that has inadequate cyber-law is essentially offering a safe haven for cyber criminals to act with impunity.[39] The foundation laid by the policy is for creating a legal framework for cyber security; this should also include having a distinct law to govern personal data dealings. The policy is exhaustive in its promises so it is upon the law makers to be focus on all promises given out under the

[37] Chetty
[38] http://www.africanliberty.org/content/tanzania-analogue-digital-new-era-tanzania-broadcasting; as cited from this author's paper.
[39] Section 3.5.1 of the National ICT Policy, 2003

policy.

Looking at every portion of the policy in comparison with the regulatory and legal frameworks, one expects to see all issues facing privacy rights being covered. But to the contrary, nothing is being done in regard to personal information. Tanzania needs to create and sustain a secure environment for online activities, before any significant new developments can emerge in ICT related services[40] as revealed by an ICT law expert. This is the issue at hand. For the policy objectives on ICT developments to be achieved an enabling legal framework aligned with Tanzania's constitutional provisions, consistent with regional and global best practices should be established. The policy has set a foundation for enacting laws that will ensure that Tanzania is free from abuse of personal data.

With the foregoing issues and challenges the government is tasked to review existing laws and regulations so as to have laws which provide a healthy environment for the ICT growth, and for the purpose of this research, data protection laws. This will ensure promotion of investment by ensuring that businesses involving electronic processes are conducted in a safe and secure environment as per the policy objectives.

Last but not least, the government is required to regularly carry out review of the policies and legislation so as not only to accommodate emergence of new services and technological innovations that will add value to the ICT enabled services providers and also to check optimum data protection.

[40] Adam Mambi Op. Cit page 12

The policy aims at enhancing the use of ICT and support development and installation of national e-health, e-tourism, e-education and e-commerce transactions.[41] All these put personal data to threat if not well safeguarded. The Policy indicates that the government is committed to ensure that ICT issues relating to electronic communications are well regulated particularly personal data protection. This shall be established in the succeeding chapters by verifying if there is any relevant piece of legislation.

ICT covers public services as well through establishment of e-government and other sectors respecting ICT reforms. Thus a firm legal regime on personal data protection is needed to ensure that individuals' privacies vis-à-vis right to information is addressed at length.[42] It is the role of this work to assess whether the legal regime pertaining personal data protection are aligned with the spirit of the National ICT Policy being promotion of ICT laws with the aim of promoting growth of the industry, but without undermining personal data protection.

1.7 Hypothesis

i. The current legal system in Tanzania does not have adequate personal data protection laws.
ii. Law enforcers in Tanzania still apply traditional laws in dealing with data protection issues.
iii. Privacy rights and personal data in Tanzania are at risk of being abused for lack of the relevant laws for their protection.

[41] Ibid Section 3.7.4
[42] Ibid Section 3.8.1

iv. There are too few law enforcers in Tanzania who are trained on privacy rights and data protection.

v. Public awareness on privacy rights and data protection issues is minimal.

1.8 Research Questions

Throughout this study the following research questions offered guidance in testing the hypothesis above:

i. What are the basic principles of personal data protection?

ii. Does the current legal system in Tanzania have adequate personal data protection laws?

iii. What are the applicable laws on data protection in Tanzania?

iv. To what extent is privacy and personal data protected against abuse?

v. Are you trained on data protection?

vi. Does the Government have any program for training law enforcers on data protection?

vii. What is the demarcating line between individual privacy rights and the right to information?

viii. How is the legal system dealing with the contrasting positions of individual privacy rights and the right to information?

ix. How does the police force observe privacy rights in the course of their job?

x. What are the challenges/limitations faced by the police force?

xi. What is the extent of awareness of the public in reporting personal data misuse?

xii. How much personal information is supplied and collected by banks? Mobile phone companies?

xiii. What are the guiding principles/policies in relation to data protection applied by the banks/mobile phone companies?

xiv. How are they processed? Stored?

xv. To what remedy is a data subject entitled to in case of infringement of personal data?

xvi. What action will a data subject take upon discovering personal information being processed without mandate? Misused?

xvii. What should the Government do to ensure personal data protection?

1.9 Research Methodology

The work at hand has adopted an analytical style because it looks into the legal regime of personal data critically and analytically, giving out observations and recommendations based on the findings. Chapter three illustrates the methodology employed by this study.

1.10 Data Collection Methods

1.10.1 Primary data

Information has been collected from a variety of individuals with diverse backgrounds who use ICT technologies in one way or another. Officials in the legal fraternity have been consulted and interviewed, court officials like magistrates, Judges and Advocates. Data subjects, processors, controllers and users were interviewed, including the police force.

1.10.2 Secondary Data

In order to come up with a successful study, secondary data have been used by the researcher by analyzing policies, Acts/legislations, reading text books on the subject, journals, development reports, papers on electronic data and surfing the internet. The data collected in this category are secondary from both electronic means and hard copies of books and statutes alike.

1.10.3 Data Sampling Design

The population involved in this study through sampling, involves normal individual users of emails, social forums, internet and ICT devices, on one hand. On the other hand court officials have been consulted to share their understanding on how ICT can pose problems in its usage especially through hacking, illegal access and other detrimental uses, and naming any legal remedy they know.

Data were collected and a coding and tiding process was employed to detect errors and omissions. Classification and tabulation of the collected data as per the nature and characteristics of data were employed. After processing data charts were used and tables to analyze them. This was done to relate their connection or differences, then the results were determined and conclusions established.

1.11 Scope of the Study

The study revolves around the need for protection of personal data as a legal phenomenon of privacy rights enshrined in the constitution. The collected facts and records encompass materials showing Tanzanian situation as lacking the legal

framework on data protection, compared to countries which embrace ICT but have such frameworks.

Geographically, this study has been conducted in Dar es Salaam city, the commercial city with a lot of central government offices, where individuals public and private engage or use electronic devices like mobile phones, go to internet cafés and supply their data online for various purposes. The respondents as already mentioned herein above were various individuals who access and use internet for various purposes. They include lawyers, ICT professionals, court officials, and business people who use online services. Research was limited between the months of March 2013 to August 2013.

1.12 Limitation of the Study

The researcher faced a number of setbacks, notwithstanding that she attained the goals set. A limited time she has due to work exigencies was big challenge. Power break outs in the country also impeded the researcher's efforts. Also, lack of readiness to some respondents and tight schedules of some others, compelled repeated visits to the offices of the respondents.

The researcher being an employee in a government agency with limited staff had a very tight schedule which could not be altered easily, necessitating the researcher to work late at night to meet the deadlines of the study at hand. Nevertheless, perseverance, persistent determination and commitment, coupled with good time management, facilitated overcoming the impediments and accomplishing the research work.

1.13 Conclusion

Chapter one is for introduction, statement of the problem, study objectives, significance of the study, illustrating the literature review and research methodology. As an introduction chapter, suffices it to say that much as ICT is an indispensable tool for development in the modern life, data protection is equally vital. As already seen from some authors some technical measures have already been devised to protect personal information like, physical restrictions, backups, encryptions and the use of soft ware[43], obviously a legal framework suitable for online transactions and communications, with regular reviews to keep pace with changes cannot be undermined, if ICT is to be secure. Just at a glance of a survey conducted in 1999 in UK, one can see how data can be affected by computer misuse, through viruses account for 41% pornography 40%, hacking 9% and fraud 10%.[44]

[43] Heathcote, P. M. 'As' Level ICT, Payne – Gallaway Publishers, Ipswich, page 50 - 53
[44] Bainbridge, D. "Introduction to Computer Law" 5t Edition , Pearson Education, London, 2004 page 36

CHAPTER TWO

2.0 PERSONAL DATA PROTECTION

2.1 Introduction

This chapter undertakes to define what in essence personal data protection is and discusses the issues pertinent thereto. The integration of technology with business has improved the business environment in Tanzania through enhanced flow of goods and services. A survey conducted Kamuzora among 106 small and medium enterprises (SMEs) in tourism industry shows that 100% of travel agents, 96% of tour operators and 92% of hospitality firms had internet access[45]. If such SMEs can engage so much on the use of internet in their daily operations, it is an indication that bigger enterprises and government institutions (as already seen) are taking the lead.

Every phenomenon has its pros and cons. While information technology hastens development through simplified work and communications, it strips naked individuals' privacy, rendering a data subject unrestrictedly accessible by data controllers. More intriguing is the fact that it is also employed as a surveillance device by state organs. It is said; the World Wide Web (www) is the major surveillance device[46] that enables tracing of any person in the world, provided one uses an electronic gadget. Having an e-communication tool with you is like having a spy in your pocket. There should be a demarcation line between right to privacy and right to information, so that data subjects may know when their information are examined legally and when not. This raises issues of data protection since when

[45] Kamuzora, F. "E-Commerce Journey of Tanzania SMEs: The case of Tourism Industry" A paper presented at the Tanzania Development Gateway Workshop on 'The use of ICT for SMEs Development: Opportunities and Challenges' Dar Es Salaam April 11, 2005

[46] Ian J. Lloyd "Information Technology Law" 6th Edition Oxford University Press 2011 at page 7

personal data is being scrutinized it infringes one's privacy. Telecommunication needs to be regulated in various ways as put by Lessig, through architecture, norm, markets and the law.[47] Law is what seem to be missing in many countries including Tanzania, and even where it exists, the pace of adapting to technological developments is too slow.

2.2 Data Protection

Data protection has been necessitated by the misuse of electronic gadgets causing privacy interference nuisances. If information technology is to grow without legal hurdles governments have to establish controls over the processing and use of personal data through legislation.

Personal data are produced daily and retained through online activities. How much data is stored and for how long is not known to the data subject. Switching on a mobile phone, allows internet to transmit signals in each minute. Presently phones can be tracked by the network operator within several hundred meters through relevant software. Through third generation (3G) mobile phones a person can be located within a range of 15metres. This location data is capable of being retained permanently and apparently governments wish that such data be retained for years for the eventuality that access may be sought in connection with criminal or national security investigations.[48] This deprives individuals of the right to determine the extent to which personal data may be accessible.

A demarcation line, though hard to draw is still necessary, which may be achieved

[47] Lawrence Lessig, "Code and Other Laws of Cyberspace, Basic Books" New York, 1999
[48] http://news.bbc.co.uk/1/hi.sci/tech/874419.stm. visited on 01st April 2013

through a legal framework for regulating online activities including safeguarding personal data for national security and business undertakings purposes. There are numerous Regulations[49] on telecommunications in Tanzania but none of them targets regulating personal data. This leaves a gap of a particular law to govern personal data used in e-health, e-government, e-education to mention a few which involve data processing. It is important to have enactments to protect personal data in the use of internet, e-banking, e-commerce and the likes where processing of sensitive personal information is indispensable.

2.3 Data Processor

A data processor in relation to personal data, is any person; other than the employee of through online activities who processes data on behalf of the data controller. A data processor does so basing on instructions of the data controller and the obligation is normally imposed on the data controller who has to enter into a written contract with the data processor.[50]

In Tanzania, data processing is governed by the Electronic and Postal

[49] Tanzania Communications (Consumer Protection) Regulations, 2005
Tanzania Communications (Quality of Services) Regulations, 2005
Tanzania Communications (Broadband Services) Regulations, 2005
Tanzania Communications (Content) Regulations, 2005
Tanzania Communications (Licensing) Regulations, 2005
Tanzania Communications (Importation and Distribution) Regulations, 2005
Tanzania Communications (Installation and Maintenance) Regulations, 2005
Tanzania Communications (Consumer Protection) Regulations, 2005
Tanzania Communications (Interconnection) Regulations, 2005
Tanzania Communications (Telecommunications Numbering and Electronic Address) Regulations, 2005
Tanzania Communications (Radio Communication and Frequency Spectrum) Regulations, 2005
Tanzania Communications (Tariffs) Regulations, 2005
Tanzania Communications (Type Approval of Electronic Communications Equipment) Regulations, 2005
Tanzania Communications (Access and Facilities) Regulations, 2005
Tanzania Postal Regulations, 2005

[50] http://news.bbc.co.uk/1/hi.sci/tech/874419.stm. visited on 01st April 2013

Communications Act[51] which is a general law for electronic and postal communications. The law vests custody and mandate to hold and monitor personal data processed by electronic communication networks into an Authority[52] (TCRA) established to regulate inter alia, telecommunications.[53] Going through the two statutes TCRA seems to be granted enormous powers in regulating electronic communications but unfortunately data protection is not covered. It is a risky situation to trade on in this digital era, as data flow is left unchecked. The Authority is even allowed to forebear[54] regulating a certain licensee in certain circumstances spelled out by the law. Such a provision should not be applicable to issues relating to personal data.

2.4 Data Controller

Sometimes referred to as the controller is any natural or legal person, or a public body designated as such by an Act, Decree or Ordinance, which alone or jointly with others determines the purpose and means of processing of personal information where the purpose and means are also determined by that Act, Decree, or Ordinance. [55] Furthermore; a data controller is the undertaking which controls the nature and extent of processing of personal data. The word control entails two elements; physical control of the data and equipment used for processing and the discretion as to the manner in which data is used, and the legal control of the nature of

[51] Act No. 3 of 2010
[52] The Tanzania Communications Regulatory Authority established under the Tanzania Communications Regulatory Authority Act No. 12 of 2003
[53]Ibid, long title
[54] Section 70 of the Electronic and Postal Communications Act Op cit
[55] Ibid

processing.[56]

In Tanzania, although the two leading Statutes do not define data or data controller, it can be inferred from their provisions that the data controller in Tanzania is TCRA. TCRA is mandated under a number of regulations mentioned under item 2.3 herein fore, to make Rules for regulation of electronic communications, numbering, maintain electronic address register, and formulate standards for proper regulation of electronic services. For clarity, the standards relate to technical and safety issues and there is no mention of data protection in any of he Regulations. So, TCRA only controls the processing; ensuring that all necessary data is obtained from the data subjects, duly processed by the processors and submitted to the Authority with monthly updates for monitoring and supervision.

It is common knowledge that governments wish to retain personal data for observing movements or activities of the data subjects especially for security purposes surveillance. The argument is however that privacy rights should not be undermined in the process. This is also because if left ungoverned, it creates loopholes for unauthorized access to personal data, which again is a violation of cyber security.

2.5 Data Subject

A data subject means an individual who is the theme of personal data, the person whose data is being processed.[57] As stated earlier, Tanzania is in full use of computer devices and mobile phones. This renders most of us data subjects in many

[56] The Data Protection Act ,1998 of UK, Article 2
[57] United Kingdom Data Protection Act 1998

aspects though it is always difficult to know to what extent is my personal information accessed without my consent or even knowledge, and for what purpose, justifiable or not and for how long it will be stored. Although such a situation calls for a regulative legal framework the Government is still silent on the subject.

Once a Director of ICT with the Ministry of Communication, Science and Technology warned that it was high time for Tanzania to create legal frameworks to govern the use of technology. These cries have to be heeded by the authorities, by putting in place the relevant legal framework to ensure data protection, since data subjects are the ticket to technology development, and promotion of investments. Also, a Director of Computer Science at the Institute of Finance Management in the country once stated that Tanzania needs a law on data protection to restrict intervention of communications through cell phones.[58]

One may imply that the silence is intentional with a bid to give room for accessing data without any judicial attention, which in my view only creates unhealthy environment for ICT growth. There have been public outcries worldwide by data subjects for data protection. A survey conducted in 2004, 2005 and 2006 indicate that 70%, 83% and 83% respectively were concerned about preserving personal information.[59] The doubts for the silence being intentional is inferred from the EU experience that in 1995, the EU passed a Data Protection Directive[60] which has over the years been regarded as harmonizing Data Protection rules throughout EU

[58] Emmanuel Onyango, reporting on a seminar conducted on the lack of laws to combat cyber crime, the Citizen newspaper, 27th July 2013
[59] Ian J. Lloyd, op cit page 10
[60] Directive 95/46 of European Parliament and of the Council, of 24 October, 1995 on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data

countries, and as the best practice model to the international community. However, in 2006 the EU adopted a Data Retention Directive[61] under which member countries are guided to make domestic laws allowing for data retention for periods of time ranging from six months to seven years. Some justifications for the retention were advanced mainly being for national security purposes.

It may also be argued that may be governments are not settled about the treatment of privacy rights vis-à-vis right to information, as indicative from the EU members' postponement of the application of the Directive on data retention for some time, presumably to compromise with their subjects on privacy issues which in most countries is a constitutional right. It would be better for the authorities to be bold and install the necessary legal framework and borrow a leaf from other countries which have laws for data protection and for cyber security, as the effects of ignoring data protection are cross cutting just as the sector itself is cross cutting when it comes to facilitation of improved business operations and service and information delivery.

2.6 Personal Data

Personal data means data or information which relate to a living individual who can be identified from those data or in collaboration with other information which is in the possession of the data controller and it includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[62] Personal data is said to be a very crucial element of identity in information security, thus its usage has to be regarded with

[61] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006
[62] United Kingdom Data Protect Act, 1998,

utmost care. This can only be achieved through installation of a legal framework for its control.

A draft Bill is said to exist that addresses cross cutting issues, such as; collection of information, use, disclosure and retention of personal information, limits on the use and disclosure of personal information storage and security for personal information, retention and disposal of personal information, to mention but a few. Issues relating to principles of data protection and consumer rights are also discussed. Likewise, powers of Ministers to make regulations are also discussed including establishment of the Office of Data Protection and Privacy Commissioner. All these issues are geared towards ensuring that there is a comprehensive legal frame work to govern data security to including protection of personal information and privacy rights in Tanzania. That is, if only it was enacted into law.

2.7 Data Processing

Processing in relation to information or data refers to obtaining, recording or holding the information or carrying out any operation or set of operations on the information including;

i. Organization, adaptation or alteration of the information or data.
ii. Retrieval, consultation or use of the information or data.
iii. Disclosure of the information or data transmission, dissemination or otherwise making available.
iv. Alignment, combination, blocking, erasure or distraction of the data;[63]

[63] Ibid

From the definition it is clear that data processing involves both creating data and erasing data. This means if there is no control; an irresponsible person may erase some very vital data occasioning immeasurable damage to the users and subjects of that data. If data can be so erased unrestrictedly even the national security is in danger. Therefore data protection is important not only for the data subject but also for national security.

2.8 Sensitive Personal Data

This means personal data consisting of information pertaining to racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether the data subject is a member of a trade union, philosophical beliefs, his physical or mental health or conditions, sexual life, the commission by him/her of any offence, or any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings[64]

In the Tanzanian perspective sensitive personal information refers to genetic data related to children, offences, criminal sentence or security measures, biometric data, as well as if they are processed for what they reveal, personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliations, trade union membership, gender and personal information concerning health or sex life of the individual, any personal information otherwise considered by Tanzanian law as presenting a major risk to the rights and interests of the data

[64] The European Directive on Data Protection, Article 8

subject, in particular unlawful or arbitrary discrimination.[65] Comparably, sensitive personal information under the European Directive on data protection is similar to that defined by the Tanzanian Bill said to exist. And since sensitive data is all about individuals, who are the data subjects anywhere in the world, it follows without say that sensitive personal data in Tanzania needs the same level of protection to guarantee privacy rights as in Europe.

2.9 Personal Information

Under the said Tanzanian draft Bill on Data Protection, personal information is about an identifiable individual that is recorded in any form including without restricting the generality of the foregoing:

i. information relating to race, national or ethnic origin, religion, age or marital status of the individual;
ii. information relating to the education or medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
iii. any identifying number, symbol or other particulars assigned to the individual;
iv. the address, fingerprints or blood type of the individual;
v. the name of the individual where it appears with other information relating to the individual or where disclosure of the name itself would reveal the information about the individual;
vi. correspondence sent to a data controller by the individual that is explicitly

[65] Chetty, P. Support for Harmonization of the ICT Policies in Sub-Sahara Africa, Training on Data protection Law, HIPSSA Project, Cited at

or implicitly of a private or confidential nature and replies to such correspondence that would reveal the contents of the original correspondence;

vii. The views or opinions of any other person about the individual.[66]

What this research has revealed is that in Africa, only Nigeria, South Africa, Namibia, Zambia and Swaziland have recently enacted laws on data protection so far. Tanzania should follow suit sooner and not later. Looking critically at the definitions assigned to personal information under the Tanzanian draft Bill, which is similar to the South African Law, the Data Protection Act, 1998 of UK and European Directive on data protection; they are all about protecting ones privacy rights and individuals' dignity. This creates an easy way for Tanzania to enact a law on data protection to create an environment to ICT growth similar to the rest of the world.

In the European Union (EU) protection of personal data and privacy are considered constitutional rights and not mere consumer protection issues. Privacy and the protection of personal data are fundamental rights enshrined in law and directly enforceable with the same status as other fundamental rights like freedom of expression and information. It is horizontal in scope and not confined to EU citizens or to consumers, therefore protects all natural persons in the jurisdiction. Sensitive personal data is assigned more stringent legal protection as illustrated in criminal

[66] Ibid

proceedings in the case against Bodil Lindqvist.[67] Mrs. Bodil Lindqvist, a catechist in a parish in Sweden, set up a website in her home computer and was the only person having access to it for uploading, manipulating and updating data. Her website contained sensitive personal information about herself and her colleagues from the parish, without their knowledge.

When her colleagues knew about it, they were unhappy that their personal details were posted in the website. Mrs. Bodil then removed their personal details from the website. Mrs. Bodil Lindqvist processed sensitive data by mentioning one of her colleagues that she had a broken leg. The last allegation was she transferred personal data to a third country with no authorization. The public prosecutor brought prosecution charges against Mrs. Bodil Lindqvist because she breached Swedish legislation on data protection and privacy rights as transposed into the national legislation from the Directive 95/46/EC.

Mrs. Bodil Lindqvist accepted the facts but denied being guilty of any offence. The District court fined her with 450EUR; She appealed to a higher Court but for purposes of this research, findings of the trial court offer the relevant point for discussion. The case indicates that individuals' data pertaining to their address, names, identity and health are sensitive thus should be protected. Mrs. Bodil Lindqvist was fined because she breached the law by processing sensitive data by posting them on her website without prior consent and no notification to the data subjects. This was a typical breach of privacy right not only data protection.

[67] Case C-101/01

2.11 Conditions for Processing

Processing personal data should be done fairly and lawfully, this requirement is set out in the first data protection principle and is one of the eight principles at the heart of data protection, whose aim is to protect interests of individuals whose personal data is being processed[68]

Processing personal data fairly and lawfully practically means you must have legitimate reasons for collecting and using an individual's data. Using data in unjustified adverse ways will affect the data subject. Appropriate private notices should be given when collecting personal data. People's personal data should only be handled in ways they would reasonably expect and make sure you do not do anything unlawful with the data.[69] Such a provision is very crucial not only in protecting personal data but also in preventing unauthorized access to data.

These conditions under the Data Protection Act, 1998 are set out in the second and third schedules of the Act where it is required that at least one of the conditions be met to ensure that data processing is done legally, [70] there must be consent from the data subject and a legal obligation for processing for the individual's benefit. This condition applies in instances of life or death, like where an individual's medical history being disclosed to a hospital medical treatment after a serious road accident, such data processing is necessary for life saving and is in accordance with the legitimate interests.[71]

---

[68] Cited at http://www.ico.org.uk/for.organisations/data-protection/theguide/exemptions
[69] Ibid
[70] Op. Cit, Data Protection Act
[71] Ibid.

All data processors and controllers have to adhere to conditions to ensure personal data are well protected because they go to the core of human dignity. One cannot discuss the right to have personal data protection without touching privacy rights. In an Indian case a data controller was held liable for failure to have adequate and automated filters to detect unauthorized data processing after another person managed to process and sale pornographic objects involving school children[72].

Processing of personal sensitive data is restrained because personal data are fragile; the UK Data protection Act provides for further conditions when processing sensitive personal data. Sensitive personal data may only be processed when there is a need to detect or prevent any unlawful act; or it is terribly needed for protecting the public against dishonesty or malpractice; or when publication is needed for public interest; when there is need for providing counselling, advice or any other services for carrying on insurance business when there is equal opportunity monitoring other than ethnic monitoring by political parties for legitimate political purposes; or it is in the form of disclosure to elected representatives.[73] The requirements for processing sensitive personal data make it more necessary for Tanzania to take drastic measures to install a legal mechanism for data protection because the consequences of infringements of such data are more adverse.

2.12 The Role of Information Commissioner's Office

The Commissioner under the Act is mandated to promote good practice in handling personal data and giving advice and guidance on data protection. She has also to

[72] Aparna Viswanathan, Op. Cit, page 78

[73] Statutory Instrument 2000 No. 417: the Data Protection (Processing of Sensitive Personal Data) Order 2000 and Statutory Instrument 2002 No. 2905: the Data Protection (Processing of Sensitive Personal Data) (Elected Representative)Order 2002

keep a register of organizations that are required to notify him about their information and processing activities. Nevertheless she also helps to resolve disputes by deciding whether it is likely or unlikely that an organization has complied with the Act when processing personal data.[74]

Besides the foregoing, the Office ensures that data protection is instilled in people's minds so that even when new policies are being formed and modalities worked out legislation and new initiatives have a policy friendly approach embedded in them from the beginning for promoting data protection aims and good practices actively covering businesses, government, parliamentarians and opinion formers; initiating and promoting research and engaging to consultations as it is initiated.[75]

In short the Commissioner's Office is charged with the regulation, governance and oversight of personal data protection in the United Kingdom. The role played by the Commissioner's Office in the UK can be replicated by the role of TCRA in Tanzania. Only that TCRA falls short of playing the protective role to personal data. This is so because there is no law that empowers TCRA to do so. With the necessary law in place TCRA can be better placed to oversee legal processing of data in general.

The Data Protection Act, 1998 and the European Directive on Data Protection 1995 demonstrate the best practices which are worth emulating by other countries that have not done much on data protection regime; Tanzania inclusive. The only drawback to EU approach to data protection is its connection with privacy issues.

[74] Data protection Act, Op. Cit
[75] Ibid

This does not appear to be the right approach on dealing with data protection. Privacy concept as stipulated in Article 8 of the European Convention on Human Rights refers mainly to the right to private correspondence while data protection needs a wider coverage beyond private communications, privacy being only part of it. Tanzania needs to take only what is felt fit for its circumstances, in which case data protection should be considered in its wider perspective.

2.13 Data Retention Directive

The EU is progressively taking action on every new technological advancement to ensure orderly safeguards to electronic communications. Having passed a Directive on data protection in 1995, it again passed another Directive on the processing of personal data in 2002 to narrow the safeguard to privacy rights so as to give room for exceptions on national security reasons. This enabled the member countries to enact laws for retention of data on grounds of national security. Subsequent to that, the EU felt a need for harmonizing the domestic laws and in 2006 a directive[76] on data retention was passed to allow access to the retained data by the national security forces as well as tax regimes. However data retention has been vigorously objected to on grounds that the measure does not give a proactive effect to the security threats rather it simply allows invasion to privacy.

2.14 A Review of the EU Data Protection Directive

The Information Commissioner's Office commissioned a review[77] of the Data

[76] Telecommunications data retention at http://en.wikipedia.org/wiki/Telecommunications_data_retention visited on 08/8/2013

[77] Neil Robinson, Hans graux, maarten Botterman and Lorenzo valeri "review of EU Data Protection Directive: Summary" prepared for the Information Commissioner's office, May 2009

Protection Directive of 1995. To establish whether it is still relevant after thirteen years since its inception, considering the increasing challenges of global data flow. The Commissioner admits to the findings which indicate that the Directive is outdated as it is failing in its scope, focus, and online surveillance contexts. He advocates for a better data protection which should reflect trust, confidence, transparency, governance and accountability.

Therefore, besides the report recommending for retaining the Directive, it also recommends for some improvements in areas like the adequacy rule, binding corporate rules, to mention a few. It is worth observing such developments in the EU closely to ensure a legal framework is formulated that is up to date in its perspective. The strengths, weaknesses and challenges pointed out from the application of the Directive, and the recommendations can be tested for customization into Tanzanian environment.

2.15 The General Data Protection Regulation

The General Data Protection Regulation[78]is a proposed new data protection regime in the EU. It is aimed at incorporating new developments like social networks and cloud computing and unifies data protection in the EU with a single law. It is an advanced step of privacy right developments which extends to foreign companies processing data of EU residents. Looking at its set of conditions for data processing they have been modified to have more strict effect to the extent of being impracticable for countries like Tanzania. But the measure can teach us one lesson

[78] http://en.wikipedia.org/wiki/Data_protection_Directive visited on 08/8/2013

that as a country, Tanzania has an obligation to protect its citizen against abuse of personal information.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This study has massively used electronic sources of information because the same has been efficient and easily accessible worldwide. Also in Tanzania where the study is done there is not much literature on personal data protection. Various writings on ideal legal regime for personal data protection are found online, save for statutes and a few text books which are paper based materials.

3.2 Online Libraries

Many online sources and websites have been visited by the author, obtaining substantial materials on ideal legal regime on personal data protection globally, though a few writings were obtained discussing on the ideal legal framework of data protection in Tanzania, as explained in this work.

3.3 Law Reports (Precedents)

Law reports have been accessed online and for Tanzania, case laws in hard copies have been perused. Landmark cases like that of Mrs. Bodil Lindquist have been analyzed in the work at hand.

3.4 Statutes

A number of statutes have been analyzed for facts home and abroad, to wit the Data protection Act, 1998 of the United Kingdom, the European union Directive on Data protection, 1995, the Tanzania National ICT Policies, of 2003, The Council of European Data Protection Convention, 108, The Data Protection Act 1984, the

OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. Information Technology Act, 2000 (of India), Indian Penal Code, the Tanzanian laws which are impacted by the ICT use like the Evidence Act, Banking and Financial Institutions Act, to mention but a few, were also perused.

3.5 Interviews with Various Stakeholders in Cyber Security

Various individuals; lawyers and other stakeholders in ICT usage and developments have been interviewed by the author of this work. The interviews went as reproduced hereunder:

3.5.1 An Advocate of the High Court who Preferred Anonymity

Question: Do you know anything about personal data protection as a lawyer?

Answer: No, I cannot tell exactly what really the thing is.

Question: Why can't you tell that?

Answer: You know the branch of law you are asking about is very new to many lawyers and the public at large.

Question: Haven't you read on anything concerning personal data supplied over the internet by users?

Answer: Yes, I have heard about it and things like cyber law and information security but cannot say more than the fact that it is all about technological advancements.

Question: Do you know what happens to your personal information when you conduct an online banking transaction? Or buy something through your MasterCard?

Answer: Well, once I buy goods using my MasterCard I understand that my

particulars are accessed and it is possible that they can be abused.

Question: Do you know anything about electronic misuse of data?

Answer: ooh yes, we see people known as hackers tampering with bank money i.e stealing through mobile banking and they are very difficult to be traced. There is also the issue of scams, individuals' money have been stolen through online banking, online frauds, etc whereby the perpetrators impersonate that they were having lotteries and the winners have to pay some money to redeem their prizes.

Question: As a lawyer, what is your opinion in making sure that electronic violations are curbed?

Answer: In my opinion the laws of the country should be revised to match with the technological pace of advancements.

By this interview you can note that at least the legal personnel/Advocates have some knowledge on the issue though a little. They cannot really tell much on the subject. If this is a lawyer and cannot say that much, think of a layman more so, rural dwellers.

3.5.2 A legal Practitioner, Mr. Mashaka Edgar Mfalla, an Advocate of the High Court

Question: Do you know anything about personal data protection as a lawyer?

Answer: Yes, I know what personal data protection is.

Question: Can you tell us what it means?

Answer: personal data protection is all about information security. The advent of technological developments has necessitated huge flow of

information from one person to another, country to country including supply of sensitive personal information to banks, hospitals, corporations companies and Governments. This being the case there is a need to have a very strong data protection laws in the country.

Question: Can you tell in brief what you think to be important or principles on data protection?

Answer: There are principles outlined by the European Directive on Data Protection which all Member states to the European Union are obliged to abide by when enacting their municipal laws on data protection. The United Kingdom has embedded the Principles in its Data protection Act, 1998. One of the Principles is that when processing an individual's personal information the process should be done fairly and lawfully. Another Principle states that the data should be processed for specific purposes and should be further processed in any manner incompatible with the purpose for which it was obtained. A further Principle states that the data should be accurate and where necessary be kept up to date but not to be kept longer that it is necessary. When processing personal data, rights of the data subject are paramount. For example the right to give consent to the data controller and/or her agent, processor such that if there is unauthorized or unlawful data processing appropriate measures need to be taken against that action. Lastly, the Act provides that data should not be transferred beyond EEA unless the recipient country attains an adequate level of protection.

Question: What is the adequate level of protection?

Answer: The adequate level of protection entails the presence of a sufficient legal framework that ensures that personal data are well protected.

Question: Does that principle apply to Tanzania?

Answer: The principle may be applied to give guidance on matters involving personal data but it is not binding. So far the legal framework for data protection in Tanzania has still much to be desired. There is so far no specific law on data protection.

Question: Do you know if there are any measures being taken to ensure personal data are protected?

Answer: Normally, we revert to EU Principles and the Data protection Act, 1998 for help.

The interview with Mashaka Edgar Mfalla sheds some light on the research that at least a few lawyers are aware of the information security and data protection, the lagging behind of the law notwithstanding.

3.5.3 A Magistrate with Kisutu Resident Magistrates' who Decided to Remain Anonymous

Question: Do you know anything about personal data protection?

Answer: Yes, personal data protection means the way personal information is protected under the law against breach of right of privacy.

Question: What is right to privacy?

Answer: Right to privacy in Tanzania is a right to respect of one's private life

and affair and his human dignity. The right is entrenched in the Constitution under Article 16(1).

Question: Have you ever handled any case in communications matters about breach of this right?

Answer: Personally I have never handled one.

Question: Can you tell us why?

Answer: The issue of breach of privacy rights in communications sector in the country is still not much elaborated and communicated to the public. A greater part of the public feels that it is not easy to trace the offender when the act is committed electronically. Moreover, the legal regime does not cover ICT crimes so, it lags behind technological advancements. The public does not know what to do or where to go when so offended.

Question: Apart from Tanzanian position, do you know of any case on privacy issues?

Answer: Yes, I know of the Durant case, an English case where Durant demanded from the data controller to access his privacy rights. Durant wanted to know what the data controller held against him and whether there was no infringement of data protection law of the country.

Question: Can you tell us whether the legal framework in Tanzania is adequate on its coverage of personal data protection?

Answer: In my opinion, the legal framework in Tanzania does not adequately cover personal data protection. Mainly, we borrow from the United Kingdom and the European Union because their coverage of the

personal data protection is much more advanced. Most of Tanzanian legislation does not incorporate information technology issues.

Question: What is your advice on data protection system in the country?

Answer: Since we already have a good policy on ICT the Government should strive to implement the same. This will give us up to date legislation addressing technological issues in the country because the entire world is going digital. Additionally, the Government should train more lawyers on information technology law because most transactions now whether public or private are done electronically. The legislature should also be asked to enact laws specifically on personal data protection to protect individuals' privacy and dignity.

3.5.4 A Senior State Attorney, Ms. Dorothy Massawe

Question: In your course of employment have you ever handled a case on electronic crimes?

Answer: Yes, but only once and was at a very initial stage of giving a legal opinion. However I could not proceed with the matter because I am not knowledgeable on issues related to electronic transactions.

Question: What was the case about?

Answer: The case was about a banker whom the bank claimed that he stole money from a customer's account through mobile banking.

Question: What did you advise the prosecution side over the issue?

Answer: As I said earlier, the file had to move to another attorney who was conversant with electronic issues and information security.

Question: After failing to opine over the matter, what do you advise the Ministry relevant to your work?

Answer: My advice is that the Government needs to invest a substantial amount of money to empower lawyers on information security and electronic issues to ensure efficiency in day to day work.

3.5.5 Mr. Phibe Komanya, an Advocate of the High Court who Works in a Hospital

Question: I understand that you work with hospital as a legal advisor, do you process personal data?

Answer: yes, we process and keep personal data of our patients.

Question: Do you know the law governing personal data processing in the country?

Answer: No, we normally take a patient's particulars and keep them electronically after the sick person has consented to it.

Question: Do you know the relevant principles when processing personal data?

Answer: Only one principle on the need to have consent of the individual whose data is being processed and the fact that we should keep them as confidential information.

Question: You said you normally process individuals' personal data after obtaining consent from the data subject, how do you get that consent?

Answer: Normally, the individual has to sign a form to show consent to the hospital.

Question: What happens in case a patient does not agree to give consent?

Answer: We normally do not force processing his data if he refuses.

Question: Are you trained in information technology law and information security?

Answer: No, I am not trained in that area of the law.

Question: How then, did you know about consent before processing personal information?

Answer: As administrators we learn ethics and values. Nevertheless, right to privacy is a constitutional right in our country under Article 16.

Question: Is the current legal system sufficient to cover personal data protection?

Answer: I cannot tell really because this area is not my specialization.

Question: Do you have any comment on this type of law?

Answer: Yes, I have a call to the Government, to train more lawyers in this field because of superimposed technological advancements in the country.

3.5.6 A Police Inspector of the Tanzanian Police Force at the Cyber Crimes Unit, Central Police, Dar es Salaam, Inspector Kennedy Msukwa

Question: Are you trained on cyber laws?

Answer: No, I am an IT expert dealing with investigations relating to cyber crimes.

Question: Does the Government have any program for training law enforcers on cyber crime?

Answer: Yes, but the problem is budgetary constraints, another problem is that

we are very few in this area since it is a new trend thus it is difficult to get the permission to go for studies, even on self sponsorship.

Question: What actions amount to cyber crimes?

Answer: illegal access to other people's electronic data, forgery and all other criminal acts committed through electronic devices.

Question: What are the applicable laws on data protection in Tanzania?

Answer: Tanzania has not yet enacted a specific law to govern cyber crimes. In our investigations, we rely on International guidelines and regulations. We also look at ICT policies of institutions involved and see if they have been contravened it gives us a basis for taking the culprits to court. Where an issue lands in a court law as a criminal offense we also rely on our traditional laws on criminal offenses and procedures.

Question: Does the current legal mechanism have adequate personal data protection laws to combat electronic crimes in the country?

Answer: I can say no. That is why we are still relying on international principles, institutional ICT policies and the old laws we have. We need to have such laws governing data protection and cyber crimes so as to secure personal data and hold data processors responsible for cyber security.

Question: What is the role of the law in combating electronic crimes in Tanzania?

Answer: The law has a great role to play in combating electronic crimes not only in Tanzania but worldwide. You know electronic flow allows

borderless communications therefore there is a need to have harmonized laws in recognizing and combating e-crimes, similarly in a borderless manner.

Question: To what extent is privacy and personal data protected against electronically committed criminal acts?

Answer: Although we lack the relevant laws in this area, the Police Force plays its role pro-actively. For instance, at our Unit we normally conduct online patrol, which have been very helpful in preventing occurrences of e-crimes. Once we managed to spot an online company at http://socialcompany.wapka.mobi/index.xhtml purported to be registered in the name of Social Credit Company, inviting people to apply for loans online at a fee. The company alleged to give loans without interest, and claiming to be linked with NBC Limited and National Microfinance Bank Limited, (These are credible banks in the country). Investigations revealed that this was a fake online company intended to steal money from unsuspecting individuals. We informed the named banks who in turn issued public notices, denying knowing the company, to caution people on the likely loss they would suffer if allured into applying for the loans on line by paying the 'fee'. In this way people are somehow protected against likely cyber theft.

Question: What is the demarcating line between individual privacy rights and the right to information?

Answer: As far as the Police Force is concerned, we are not restricted in obtaining personal data when at work.

Question: Can't a police officer be taken to court for accessing individual's personal information illegally?

Answer: Not quite, only if a police officer uses the information for illegal purposes in which case disciplinary measures may be taken.

Question: How does the police force investigate e-crimes without infringing privacy rights? i.e how do they access data related to commission of e-crimes?

Answer: As stated earlier, we have no limitation in accessing data. We are simply required to inform the data keeper that is the institution where an e-crime is suspected to have been committed, or in some cases we use forensic computer lab to access whatever data we need.

Question: How does the police force observe privacy rights in the course of their job?

Answer: In the police training college we take oath to protect the nation including observing privacy rights of citizens. Therefore, although we are not restricted in obtaining personal information, we are expected to use whatever personal data we access for lawful purposes.

Question: What are the challenges/limitations faced by the police force?

Answer: There are many challenges we face in investigating cyber crimes, such as lack of training, in this Unit we are only two my colleague has gone for studies I am all alone. Another challenge is the boundless nature of e-crimes; a person in Tanzania may commit an online crime here but the impact to be seen in another country which makes it costly or difficult to trace the culprits. Lack of the relevant laws on e-

crimes is also a challenge, a situation which gives room for network operators to escape from liability because there is no law obliging them to abide in protection of the customers personal data.

Question: What is the extent of awareness of the public in reporting e-crimes?

Answer: Public awareness is still very minimal. People may read criminal messages on blogs, websites but may not consider it as criminal unless the message has a damaging effect to a person that is where they report the incidence.

Question: What are the common online offences being committed in Tanzania?

Answer: Mostly, are online thefts relating to mobile money services rendered through M-pesa by Vodacom, tigo-pesa by tigo mobile company and airtel money by airtel mobile company. A few cases are reported related to ATM thefts. If not for monetary loss, personal data infringements are not reported presumably due to lack of awareness of privacy rights.

Question: What do you think should be done to enhance public awareness?

Answer: A joint effort is necessary by the Government, media and ICT experts. For instance the online patrol conducted by the Police Force is one such effort. The Government should oblige network providers to register sim cards immediately upon selling as opposed to the current practice where customers are given a grace period. This allows a person to buy a sim card use it in committing an offence and throw it away untraceably.

3.5.7 An Interview with a Celebrated Legal Expert in ICT Law in Tanzania

Mr. Adam Mambi

Question: What is the legal status of Tanzania as far as data protection is concerned?

Answer: So far, Tanzania is yet to have the required data protection law and even the legal framework does not cater for data protection besides the National ICT policy of 2003, although the Constitution provides for privacy rights.

Question: Has Tanzania signed to any of the international conventions or treaties or guidelines on data protection, which at least one can refer to?

Answer: No, referring to such positions lacks the legal basis, because we are not a party to any of them.

Question: What do you think is the future of data protection in the country, in the absence of such a legal framework?

Answer: of course, the future needs to be taken care of; right now we have a Model Law on Data Protection for SADC countries in which Tanzania is a member. I hope this will give a guidance to the member countries for enact domestic laws on data protection in a harmonized way. Currently, the government is attempting to draft a Bill on cyber security in which data protection issues will be covered bu is still at its preliminary stage.

Question: I have read somewhere that in 2006 a draft Law on Cyber Security was discussed in Kampala Uganda, since then it disappeared would

you know what happened to it?

Answer: That draft was prepared to cater for East African countries but then it was felt that it could not be proper to have a single statute for the EA region while the status of the East African Community is still under discussion. And taking it as Guidelines it would take time for all the EA member countries to ratify before it could be adopted into domestic laws. So it stopped there.

Question: Being an expert in ICT law what else can you share with me as a student in the same?

Answer: I can only commend you for taking interest in data protection.

3.5.8 An Interview with a Judge of the High Court of Tanzania (Commercial Division)

Question: Being a member of the Bench in Commercial division of the High Court how many cases are admitted relating to personal data infringements per annum?

Answer: Such cases occur very rarely, there may occur only one case in two or more years.

Question: Have you personally tried any case involving ICT activities?

Answer: yes, I have just delivered a judgment on a case that involved misuse of data through a cell phone.

Question: *What law did you apply in deciding the case?*

Answer: That is one of the challenges we still face in the court, Advocates and Judges alike. How do you decide on a cyber space matter while there

is no law for such events?

*Question**:*** I read a case where the Judge applied traditional laws to fit the circumstances of a cyber crime, what can you say about that?

Answer: yes, sometimes you are forced to take such an approach because you have to give a judgment for a matter placed before you. But it is a very difficult situation. There are even opposing views, some decisions trying to adapt to technological changes but others stick to the letter of the existing legislation.

CHAPTER FOUR

4.0 THE CURRENT STATUS OF DATA PROTECTION IN TANZANIA

4.1 Introduction

Information security entails the presence of a comprehensive legal framework to secure sensitive data and protect personal information. However, to date, the country still lacks such a comprehensive legislation to govern data protection. This is despite the fact that Tanzania has embarked on promoting ICT as one of the major tools of economic development through improved investments and services, and practically, it has reached a very advanced stage in terms of usage. The research has shown that through ICT Tanzania can achieve poverty alleviating as more people especially in the remote can access telecommunication and mobile money services, as it is already happening.

4.2 An attempt to Create a Cyber Security Law

A draft Bill on cyber security was prepared and discussed in the year 2006 at a Workshop on Cyber laws for East Africa, in Kampala Uganda, but this has vanished in thin air. The draft Bill however had lumped together data protection, privacy rights, contracts for licensing, assignment of copyright, creation of transfer in title deeds, wills and trusts created by wills negotiable instruments and bills of lading.[79] The Bill was also intended to apply to the East African countries whose operability would be difficult since it would entail each member country adjusting its domestic laws to conform to this law.

[79] Mambi, A., 'The Status of Cyber Laws in Tanzania'. A paper presented at Cyber Laws Work Shop for EAC, 24-28 April 2006, Kampala Uganda.

4.3 Status of the Legal Framework in Tanzania

Besides lacking a comprehensive law on personal data protection Tanzania has a few statutes on electronic communications which literally do not recognize personal data protection let alone distinguishing sensitive and non sensitive data. A statement by Prof. John S. Nkoma[80] in the preface to Adam Mambi's book[81] admits not only that a comprehensible legal frame work to govern data protection is lacking but also that the same is indispensable. He further states that in 2004, a computer law program was initiated at the University of Dar salaam sponsored by the World Bank, but when the sponsored period elapsed the program ended there, as there were no further steps by the government to sustain the program.

The government is impliedly reluctant to have personal information safeguarded by the law as the style and pace in which the legal reform is undertaken leaves much to be desired as evidenced by professor Nkoma's statement on the lack of a legal framework to assure users of ICT including investors, security to their personal data. This jeopardizes the future of ICT growth in this country. It is high time the Government takes drastic measures to rectify the situation in support ICT growth.

4.4 The Benefits of Data Protection Law

As already discussed in the preceding chapters of this work, a Data Protection law aims at promoting regulation of telecommunications in terms of protecting personal data processed by public and private bodies. The law will facilitate introducing information protection principles and set minimum requirements for the processing

[80] Director general to the Tanzania Communications regulatory Authority
[81] Adam Mambi, Op. Cit page x - xi

of personal information and also establish regulatory bodies to supervise data processing. ICT growth and investment require a legally safeguarded environment. As of now electronic communications are not adequately regulated, which leaves users unsecure.

The research has also realized that there are value added services rendered by telecommunication service providers such as mobile money services which also prove to have very positive impact to the economy. Such new developments give new challenges to the legal fraternity and widen the gap between the existing laws and the technological changes. Data protection law will cater for bridging the gap as it will provide answers to the questions of where and how should processing of data be regulated.

4.5 Processing of Personal Data in Tanzania and its Storage

It is surprising to find that neither the TCRA Act nor EPCA defines data, data processing, and data subject or data storage. This is a serious anomaly which can only be rectified by having a data protection law in which not only such important definitions shall be given but also proper governance of personal data will be ensured.

Under the abandoned draft Bill on cyber security for East Africa, processing of Personal data and its storage referred to any operations or set of operations performed upon personal information, whether or not by automated means, such as obtaining, recording or holding the data or carrying out any operation or set of operation on data, including:

i. Organization, adaptation or alteration of the data.

ii. Retrieval consultation or use of the data; or

iii. Alignment, combination, blocking, erasure or destruction of the data. [82]

Virtually, if the Bill is passed into law operating regulations shall be formulated which will put into consideration the right to privacy which is a fundamental right under Tanzania Constitution. [83]

It should also be noted that not all personal information was intended to be strictly controlled under the proposed Bill; it would all depend on what domain the data fell, to make it eligible for protection. Such types of communications that need to be strictly protected are such as lawyer-client relationships, doctor-patient relationships, child proceedings in courts of law (which needs to be in camera), bank – customer relationships, privacy between spouses, secrecy of correspondences, confidentiality and integrity especially on postal items, human DNA Regulations, prohibition of publication of identity by courts of law, National Security, Anti Money Laundering and Journalism. [84] Otherwise there would be a breach of secrecy.

Despite the fact that privacy and data protection is very important in Tanzanian digital era, and notwithstanding, the fact that privacy is taken to be a basic right as discussed herein above; the country still lacks an effective legal regime to address all the important issues on data protection. This being the case, subjects of data are exposed to massive threat of infringement of their personal information. Though the

[82] Chetty, P, 'Presentation on Data Protection Bill' Opera cit
[83] The Tanzanian Constitution, Op. Cit Article 16 as amended from time to time.
[84] Ibid

draft Bill sought to guarantee protection of personal information, its abandonment makes the political will shown previously through the ICT policy and other measures intended to support the grown of ICT, questionable.

It is not clear as to why the Government is hesitating to finalize and table the Bill before the legislature for passing it into law. The absence of the necessary legal framework to match with the ever-growing use of ICT makes the political will to enhance ICT meaningless.

4.6 E- Banking Privacy Rights

E-Banking is available everywhere and all the time as long as the systems are functional. E-Banking offers global reach, across cultural and national boundaries.[85] In Tanzania banking services are regulated by the Bank of Tanzania and the operating laws are the Bank of Tanzania Act, Foreign Exchange Act and the Banking and Financial Institutions Act.[86] Available records indicate that there were thirty-four (34) registered banks eighteen (18) financial institutions and two hundred and eleven (211) bureau de changes by 2012.[87]

Most of the banks and other financial institutions are computerized and have introduced Automated Teller Machines (ATM) cards and other related cards which are used to deposit and withdraw money, bringing cash services closer to the depositors without the need to visit the bank physically. Master cards are also employed to buy goods and other products online. All these put the customers to

[85] Loudon, K.C, 'E-Commerce business, technology, society, '2nd Edition.
[86] Act No. 4 of 2006, No. 2 of 1992, and No. 5 of 2006 respectively
[87] http://www.bot-tz.org/BankingSupervision/Registeredbanks.asp

risks of being accessed by third parties and that is where data protection questions come up. Nevertheless, the laws regulating the banking industry are not compliant to online money transactions. It also poses a challenge to the legal fraternity when called upon to find legal redress to personal data misuse.

Customers using credit or debit cards have to warn or ask themselves whether usage of credit/debit cards is safe and risk free under the current legal regime which leaves much to be desired. Banks and bank owners have also to warn themselves of the dangers posed by e-banking especially on the issues of data protection when personal details are supplied especially in the absence of a clear legal framework governing online banking.

The existing laws on banking issues fall short of provisions on electronic banking transactions, ATM's operations and online banking business generally. A legal administration of data protection in Tanzania is vital for regulating ATMs and other online banking facilities especially on security of sensitive data such as issues of pins, codes, and names etc which are at jeopardy if not well protected. In short e-Banking customers need be well protected through data protection laws, short of which they are at a risk of losing their savings to unauthorized access to data.

This process of entering into banking transactions using modern technology as already explained above, have enormous benefits to many business people. Banking as a sector plays a very important role in building and boosting the economy of a given country. That being the case, there is a need to ensure that the environment in

which banking transactions are done is not only easily accessible but also legally secure.

Online banking is said to be very convenient as it can be operated from home, on travel, offices and at any point provided you have computer access and internet connection. Online banking offers unlimited services, whereby a customer can access his account day and night, available seven days a week, and twenty four hours a day. Just at a click of a mouse everything happens. It is also stress free because no closure time like the traditional banking system which has a cut-off time.

Besides the above advantages, online banking is also easy to access using a personal computer where by various transactions can be carried out on one's personal financial matters. On top of that online banking ensures easy way and timely payments where due dates are set. Online banking is also smart and ubiquitous, the fact which will help you to trouble shoot any problem which may arise from the business. On the issue of interest, banking online attracts customers to get higher interest rates compared to traditional banking customers which range from 5% to 3.4% annually.[88]

Lastly but not the least; online banking is both efficient and effective. Through a well created and secure site all the customers' financial transaction are managed on orderly manner. [89] The only impediment to online banking is the absence of a data protection law which will cure the problem of security for on online banking transactions there will be control over information supplied over internet to protect

[88] Ibid
[89] Ibid

accounts from hackers and loss of funds. This is one of the grounds for data protection laws, to cater for online banking. Indisputably, internet banking has made life easier for customers and the banks alike, where a customer may access his account and get money from various cash points without the time consuming physical interaction with the bank. Legal data protection is therefore needed, to protect online banking customers and spell clear remedies for infringements.

4.7 Mobile Money Services

While the Banking and Financial Institutions Act regulates the banks and financial institutions, the Electronic and Postal Communications Act regulates postal and electronic communications. Here we have mobile money services rendered by telecommunication service providers, which service does not fall under either of the two Acts, thus unregulated. Worse still the service involves processing of personal information which is protectable by law but which is left unattended. According to the Five Year Development Plan, ICT is among the five strategic sectors earmarked as having a high potential for enhancing economic growth of the country. But in order for this to materialize, the challenges posed by technological developments should not only be addressed but also kept at pace with the technological changes.

4.8 Remedies for Illegal Access and Misuse of Personal Data

There is no shield that cannot be pierced no code for that matter cannot be breached and not a computer system that cannot be hacked.[90] That being the case, e-commerce and information technology will lose their relevance unless computer

[90] Yatindra Sigh, Op. Cit. page 16

systems are secure. In India preventive measures are undertaken under the Information Technology Act to ensure security to computer systems. Civil and criminal liabilities for the illegal actions are provided for in the said Act. The controller or any person authorized by him to access any computer and data, in case there is a reasonable cause to suspect, may access a computer system if the controller has a reasonable cause to suspect contravention of provisions of chapter VI of the Act. The power to intercept, monitor , decrypt of information through any computer system has now been instructed to the Central Government or the state government or any other officer authorized by them under section 69 of the Act.[91]

The Indian legislation tries to achieve information security by providing for civil and penal consequences for wrongful activities such as illegal disclosure of personal data, spam, spyware, phishing and cyber stalking, all of which always interfere with personal data if committed.[92]

A person is liable to pay damages to the person affected if he gets access or downloads information or data or introduces a virus, or causes any damage or disrupts or denies access to an authorized person to any computer system or computer network or changes services to the account of any other person destroys or deletes information or steals or alters any source code without permission of the owner.[93]

The Indian law on IT views personal data in a wide perspective considering that it is processed and stored in various ways, in credit cards, insurance records, banks,

---

[91] Ibid
[92] ibid
[93] The Information Technology Act, 2000 of India, Section 43

hospitals, schools, taxes, credit history, telephone calls; to mention but a few. All of which, if tampered with will occasion data abuse. [94] Bill Gates in his book "The Road Ahead at pages 302 and 303; on the Chapter titled 'critical issue' discusses the major worry on privacy where networks are concerned. As I hereby quote;

> *"The potential problem is not the mere existence of information it is the abuse that makes me worry. We now allow a life insurance company to examine our medical records, before it determines whether it wants to insure our mortality. An insurance company may also want to know whether we indulge in any dangerous pastimes, such as hang gliding, smoking or stock car racing. Should an insurer's computer be allowed to cruise the networks for records of our purchases to see whether there is any information that might indicate risky behaviour on our part. Should a prospective employer's computer be allowed to examine our communication or entertainment records to develop a psychological profile? How much should a federal, state, or city agency be allowed to see? What information should a potential land lord be able to learn about you? What information should a potential spouse have access to? We will need to define both, the legal and the practical limits of privacy.*[95] End of quote.

With the premises, one can see that with no proper legal regime for data protection in a given country, civil liability will not be taken care of although personal information are at risk of being interfered with. The legal regime needs to address both the practical and legal limits of data protection.

---

[94] ibid
[95] Bill Gates "The Road Ahead" pages 302 – 303 Yatindra Sigh, Op. Cit.

In the case of Torbay's Care of Trust Website in Torquay cited by Chetty, Torbay was fined sterling pounds 175,000 for publishing sensitive data of about 1,000 employees on the Trust's Website. Torbay Care Trust was held liable for putting sensitive information about their staff at the risk of scam.' Lesson learned here is that sensitive personal data if not well protected subjects the data subjects to infringement of the right to privacy.

Another case given is where Belfast Trust was fined for leaving thousands of patients' records in disused hospital. News were released that Belfast Health and Social Care (BHSC) Trust had been fined sterling pounds 225,000 following a serious breach of the Data Protection Act (DPA). The breach involved sensitive personal data of thousands of patients and staff including medical records, x-rays, scans and lab results, as well as staff records unopened pay-slips inclusive. There was lack of adherence to the provisions of the Data Protection Act by the hospital as a data processor and controller.

In yet another example, the closure of the best read Sunday newspaper is a stack illustration of the reputational and commercial damage that can result from privacy – intrusive practices carried out in the name of investigative journalism. While the law recognizes the right information, it should be balanced with the right to privacy so as to afford personal data protection.

The case of the News World demonstrates that data protection applies even in relation to the publication of materials in the media. In such cases, the issue to be considered at the first instance is whether public interest could be deemed to prevail

in the publication of the material. If it does; then the general requirements of the data protection are set aside. But if no public interest could legitimately be claimed; then the media must have due regard to their data protection obligation.

The cases stated hereinabove show how personal protection is crucial and how the breach of the underlying principles of data protection, attract heavy penalties. The work at hand looks into the ways Tanzanian legal regime will embed the fundamental principles on personal data protection and how they should be applied.

The global nature of the internet and its popular use creates new rights and obligations which necessitates for a matching legal and regulatory apparatus to put electronic transactions at a secure environment. Dishonest people worldwide persistently seek for loopholes through which to perform illicit businesses.

4.9 Conclusion

From the foregoing, one can safely say that the existing telecommunications legal framework does not give adequate legal safeguard to personal data therefore data protection needs to be addressed thoroughly under Tanzania data protection legal regime. And going though the draft Bill that has been dropped, some components were proposed. But the same is yet to become law. The illegal access and use of personal data both abuses and interferes with personal data protection. The law needs to address such issues to ensure that there is adequate data protection under Tanzania legal regime.

CHAPTER FIVE

4.0 SUITABLE DATA PROTECTION REGIME

4.1 Introduction

This chapter undertakes to address what legal regime or models are suitable to ensure that there is adequate data protection in Tanzania to operate against data infringements. The chapter also assesses the global trend on data protection and what system or trend should be adopted or emulated by the Tanzania government to ensure that there is adequate legal protection to personal data in the country. In short, this chapter undertakes to answer the following key questions or issues.

i. What is the internationally acceptable model on data protection?
ii. What is an ideal model legal regime on data protection to be adopted by Tanzania?

4.2 Internationally Acceptable Model on Data Protection

The purpose of data protection legal regime in any given country is to safeguard personal information processed online since it has impacts on the development of ICT through e-commercial and e-government activities. [96] Since a law is enacted to cure a certain mischief and misuse of information and unauthorized data access are increasing tremendously, there is an awful need for a comprehensive data protection legal regime. An internationally accepted model on data protection legal regime should therefore be adopted and emulating the United Kingdom model on data protection principles.

As already seen India, enacted the Information Technology Act, 2000 which initially

[96] Chetty, P, support for Harmonization of the ICT policies in sub Saharan Africa, Training/ Data Protection Law

missed data protection, but was amended in 2008 to redress the problem.[97] Tanzania may also start in the same way. Down here is the summary of the said basic principles which are considering. The data protection legislation should ensure that Personal data are processed fairly and lawfully and in particular the same should not be processed unless;

i. At least one of the specified list of pre-conditions is met (for instance the data subject has given his consent or the processing is necessary for the performance of a contract to which the data subject is a party, and
ii. In the case of sensitive personal data, at least one of an additional set of pre-condition is also met for instance the data subject has given his explicitly consent or processing should be lawfully consented.[98]
iii. Data should be processed only for specified lawful and compatible purposes.
iv. Data processing should be adequate, relevant and not excessive.
v. That the data processed need be accurate and update
vi. The data processed should not be kept longer than the necessary required time.
vii. Whatever is being processed, the data processor should always process the data in accordance with the rights of the data subjects as already discussed above.
viii. After processing, the data should be kept safe and secure.
ix. Transfer of the data so processed should be properly controlled to ensure

[97] Yatindra Sigh, op. Cit page 19
[98] Opera cit

adequate protection. [99]

These are the basic principles as enshrined in the Data Protection Act, 1998 of UK. In my opinion they are deemed to be acceptable and worth emulating in Tanzania.

4.3 An Ideal Model of Data Protection Legal Regime that can be Adopted by Tanzania

The aim of any data protection legislation is to protect data subjects and their personal rights at length. Data protection should always strive to ensure secure online communication environment as explained here in above. The legal regime also can consider encompassing the six basic tenets as stipulated in the European Union (EU) Data Protection Directive of 1995[100] since the world has become a global village in which case Tanzania is inclusive. The findings of a review conducted to the Directive should also be looked at for avoiding areas of weakness pointed out.

There are companies from US, EU and elsewhere in the world doing business or investing in Tanzania. If they are to exchange information they have to be assured of safety of their personal data thus a harmonized application of the principles enshrined in the European Union Directive on Data Protection should be considered. The Data Protection legal regime in Tanzania should emulate the best practice or principles as enshrined in the Directive so as to promote such foreign investment which is among the current Government policies. The Directive provides for the

[99] Wounds, J., A practical guide to the Data Protection Act, The Constitution Unit, 2004 cited at www ucl.ac.Uk /constitution,.

[100] Cited from www.gocsi.com visited on 15th may, 2013

following six basic principles:

i. Notice: an individual has the right to know that the collection of personal data will exist in that regard personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

ii. Choice: an individual has the right to choose not to have the personal data collected.

iii. Use**:** an individual has the right to know how personal data will be used and to restrict its use. Personal data may only be used for legitimate purposes as per the detailed description of the directive.

iv. Security: an individual has the right to know the extent to which personal data will be protected. Organizations must implement appropriate technical and organizational measures to protect personal data. The measures must be appropriate to the risks represented by the processing and the nature of the data to be protected.

v. Correction: an individual has the right to challenge the accuracy of the data and to provide corrected information. Personal data collected and maintained by organizations need be up to date and thus, reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected.

vi. Enforcement: an individual has the right to seek legal relief through appropriate channels to ensure that personal data are protected. [101]

[101] Directive 95/46 of European Parliament and Council of 24 October, 1995 on Protection of individual with regard to processing of personal data and free movement of such data.

Reading critically the provisions of the Directive and those of the Data Protection Act 1998 of the United Kingdom; it is apparent that personal data are afforded much protection and privacy rights are highly observed. If any legal regime emulates such principles, it will be acceptable as being reasonably adequate.

Emulating the data protection principles from the international forum will facilitate a harmonious operation of the laws on data protection considering that ICT has no geographical borders. A good example is when the 'ze utamu'[102] blog published obscene material intended to injure reputation of political leaders in the country. While one of the publishers resided in UK and other two in USA the Government could not press charges against them due to lack of law that governs cyber crime.

[102] http://www.bongoslang.blogspot.com the position was confirmed by the Head of cyber crime Unit at the Police headquarters in an interview held on 13th December 2010 by Abel Juma Mwiburi a student in LLM at the UDSM

CHAPTER SIX

6.0 OBSERVATIONS, RECOMMENDATIONS AND CONCLUSION

6.1 Introduction

Objectives of this study were enumerated earlier in Chapter one and a greater percentage of which has been achieved up to this point of the research. Throughout this work, some important issues pertinent to data protection have been exposed, as per observations below.

6.2 Observations

6.2.1 The Policy of Personal Data Protection in Tanzania

In examination of the way the National ICT Policy considers personal data protection in Tanzania the researcher has established that there was initially a political will within the Government in ensuring unhampered ICT growth. The Government acknowledges the fact that fostering ICT is necessary for not only improving governance and service delivery but also fostering economic development.

Most Government offices are installed with computers which facilitate electronic communications through emails and the web. Information systems are also a common place. Electronic data processing and storage are widespread in hospitals, banking services, government departments and ministries, agencies to mention but a few, almost all process and store personal information for a specific purpose. In doing business individuals provide their personal data on various websites. This makes it crucial to have data protection law to ensure that there is protection to

personal information.[103] It has been reported that the country needs a policy and legislation to provide a framework governing operations and enforcement of legally accepted cyber activities.[104] Various stakeholders in the seminar stressed the need for a data protection law and the importance of creating a legal framework to govern the use of ICT.[105]

It is a general rule that privacy is a basic right in Tanzania. But as people engage much on online transactions, where private and public, national and multinational bodies embrace digital operations, violations are doomed to occur jeopardizing cyber security in which case state organs may need to encroach privacy rights in search of personal data exchanged in illegal pursuits. This is one of the challenges which personal data protection law has to address, to lay a demarcation when and when not access to persona data is justifiable.

The absence of comprehensive data protection law exposes subjects to threats of illegal intrusion to their privacy, by misuse of information as personal data is not legally attended. Unscrupulous persons may intrude into an individual's personal information at the pretext of pursuing a legal duty of public interest while infringing privacy rights without proper remedy to the affected person. Therefore, government intervention is required by taking the necessary measures urgently to curb the situation. We should not wait any longer. Data protection law will deal with the

[103] Cited at http://www.ico.gov.uk/for-organisations/data-protection/the-guide/the-principles,aspx visited on 25th March, 2013 at 10.00 am

[104] The Guardian, 27th July 2013, reporting on a Seminar with regard to ICT for national development focusing on the use of mobile phones, internet and computers

[105] Ibid

impact of IT developments to privacy rights in commercial and e-government activities by giving proper responses to unlawful interference with data flows.

6.2.2 The Extent of Personal Data Infringement in Tanzania

The common online violations being committed in Tanzania are mostly, thefts relating to mobile money services rendered through M-pesa by Vodacom, tigo-pesa by tigo mobile company and airtel money by airtel mobile company. There are also reported cases on Automated Teller Machines (ATM) thefts. However, successful prosecution and proper remedy to aggrieved persons need the relevant legislation.

6.2.3 The Role Played by the Law in Combating Personal Data Misuse in Tanzania

Tanzania still lacks the relevant laws for combating misuse of personal data. The Government is in the process of reforming the legal framework to accommodate IT developments, but at a pace too slow to make sense. So far law enforcers are compelled to apply traditional laws on matters of data abuse and evidence. Much reliance is also placed on institutional policies, principles and guidelines governing online transactions, which are also inadequate.

However, as stated by Inspector Kennedy Msukwa in the interview with him, the laws have proved to be inadequate in dealing with problems brought about by information technology. The existing laws therefore are not suitable to ensure personal data protection in Tanzania. The legal framework as a whole does not allow legal administration of electronic transactions at all, particularly to data protection.

Some law enforcers resort to EU Directives on data protection for guidance due to lack of the guiding domestic law, although Tanzania has not signed to adhere to them, thus they are not binding.

6.2.4 Public Awareness on Data Protection

Personal data infringements are not commonly reported most likely due to lack of public awareness on personal data as being protectable by law. Education on ICT applications would reduce abuse of information and cyber crime occurrences. From the interview conducted, a very few legal professionals are conversant with personal data protection. The judiciary, the bar and even the Attorney General's Chambers, they do not seem to understand personal data protection as a legal phenomenon, except for a very few.

In the Judiciary, only a few cases have been tried so far indicating unawareness by the public to lodge complaints where their personal data are misused. At the Attorney General's Chambers they were of the view that data protection is something for the future as there is no law governing it so far.

6.2.5 Challenges Facing Personnel Involved in Combating Data Misuse

The existence of data abuse makes it necessary to take control measures. However, the efforts are meted with more challenges than opportunities, some of which lack of a clear legal framework governing personal data protection, thus relying on International guidelines and regulations as well as ICT policies of institutions involved in events of infringements. But once a culprit is taken to court there is also a challenge in the applicability of the law of evidence on online transactions. The

traditional laws governing court proceedings have no creation of online transactions or procedures on prosecuting them.

Training is also a challenge as most law enforcers are not well trained in ICT Law let alone personal data protection thus not skilled to deal with online legal challenges. Tanzania participated in drafting a proposed Bill on cyber security which is said to get stuck within the sector Ministry, which however is not on data protection. This leaves online data subjects unprotected and susceptible to sabotage by cybercriminals in the country.

There is a high relationship between data protection legal regime and the right to privacy which is a fundamental right guaranteed under the Constitution of the United Republic of Tanzania as amended from time to time. It is a risky situation to live in, due to speedy development of information technology worldwide, as Tanzania is not excluded from using online facilities whereby electronic communications are extensively used, in which case sensitive personal data are supplied, processed and stored expansively.

The lacuna may turn the country a safe haven for cyber crimes causing some investors to dodge from trading with Tanzania for fear of occurrences of computer related offences such forgeries, frauds, illegal access or illegal interference to their personal data. The fact that online transactions in the country are widely used, data misuse have become rampant exposing consumers online to the dangers of unauthorized access to their data with no remedy at hand, because there is no legislation to address such issues in the country.

Citizens' privacy rights are also put in jeopardy for lack of clear protection. Some online consumers are not aware of their rights during processing of their sensitive personal data. This has occasioned denial of justice to many consumers caught unaware thus not able to assert their rights by lack of a clear and substantive legal protection known to the citizens.

6.3 Recommendations

According to the research findings there is evidently some technological measures taken to prevent harm occasioned by misuse of data, like encryptions, those measures offer partial solutions to the problem, leaving a gap to be filled by a legal framework. The government should therefore take a drastic step to put in place a suitable legal framework to go in line with ICT growth, to govern its applications and safeguard personal information being processed and stored vastly. The existing framework has proved to be limited in scope and outdated. It is hereby recommended that:

i. Since there is no legislation on data protection in the country, the government should strive to enact one in the likeness of Data Protection Act, 1998 of the United Kingdom whereby the eight basic principles described herein above shall be emulated. Issues of individuals' privacy should be given utmost consideration since privacy rights are constitutional.

ii. The SADC countries Model Law on Data Protection is a good guiding tool at hand as it gives a detailed coverage of all issues pertinent to personal data protection, recognizing sensitive and non sensitive data, rights of data subjects including but not limited to right to rectify, delete or object to processing of

one's data. This being homemade guidelines for regional harmonization of data protection.

iii. The legislation to be enacted should put into consideration encompassing all the six basic tenets as enshrined in the European Union on Data Protection Directive as above discussed in order to ensure that there is data protection in the country so as to encourage e-commerce which is vital in boosting our national economy through foreign trade.

iv. Bodies dealing with regulation of telecommunications and electronic money processing particularly the Bank of Tanzania, TCRA, should also ensure they make principles and guidelines that encompass data protection for ensuring security to users of the services.

v. The anticipated legislation should consider creation of awareness raising programs as part and parcel of the mandate of the legislation and enforcers thereto.

vi. The government also should ensure that cybercrimes are well regulated under Tanzanian legal regime because data protection principles, if breached they lead to cybercrimes. Such issues are cross-cutting.

vii. The anticipated legislation should also consider creation of training programs for the law enforcers to give an effective use of the law upon enactment.

6.4 Conclusion

The aim of data protection is to create a secure environment for online activities. As Tanzania has decided to recognize ICT growth as a vehicle for national development, without ensuring personal data protection to the users who are the

agents of ICT growth, cyber activities will not be secure and national development cannot be achieved. Issues of Data protection are as sensitive as cyber security itself. All stakeholders should therefore come together to install a sound legal framework to enable arriving at an optimum anticipated information security level.

To arrive to this, the government has to put in place a comprehensive legislation guided by the Model Law on Data Protection for SADC countries, and borrow a leaf from the above analyzed eight data protection principles in the Data Protection Act, 1998 of United Kingdom and where necessary the six basic tenets of the European Union Directive on data protection. It is possible to have a suitable data protection legal regime provided the government ensures will power to legislate and govern.

ICT offers great opportunities for economic growth through foreign investments. Concerted efforts need to be employed in unison in line with the borderless nature of electronic communications to overcome challenges of cyber security for personal data protection. The draft Bill lying at the sector Ministry should be reviewed and tabled to the Legislature so that country gets a clear law on data protection.

Mindful of the right to information, the same should not undermine the protection of personal information. Personal data should only be accessed for lawful purpose and all illegal interferences should be meted with deserving punishment. This can only be assured by the presence of governing law.

REFERENCES

Abdallah Ally and Dr. Jabiri Kuwe Bakari, "Legal Challenges Brought by Developments of ICT in Tanzania" 8th December 2010

Abdallah ally, "Legal Challenges Brought by Developments of ICT in Tanzania: An Assessment of the growth of mobile banking services" 11th June 2012

Adam J. Mambi, ICT Law Book: A sourcebook for Information & Communication Technologies and Cyber law, Mkuki na Nyota DSM 2010.

Aparna Viswanathan, CYBER LAW:Indian & International perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes, Butterworths Wadhwa 2012.

Bainbridge, D. "Introduction to Computer Law" 5t Edition , Pearson Education, London, 2004

Bank of Tanzania, "Risk Management for Electronic Banking and Electronic Money Activities" - Consultative document March 1998

Bank of Tanzania, Banking Supervision: Supervisory methodologies, Acts, Regulations and Circulars in Place" last updated on 13th July 2012

Bank of Tanzania: "Electronic Banking Group Initiatives and White papers" October 2000

Bank of Tanzania: "Management and supervision of cross-border electronic banking activities" final document, July 2003

Bank of Tanzania: "Risk Management principles for electronic banking" – final document, July 2003

Bank of Tanzania: Payment System Statistics

Buckland, J. A. "Combating Crime: Prevention, Detection and Investigation" 1st Edition MacGraw – Hill, New York 1992

Chetty, P, 'Presentation on Data Protection Bill'

Cornwall, H. "Data theft, Computer Fraud, Industrial Espionage and Information Crime" Heinemann Educational Books, London, 1987

Electronic Privacy Information centre: "Cybersecurity Privacy Practical Implications

Electronic Privacy Information centre: "EU data Protection Directive"

Electronic Privacy Information centre: "Surfer beware II: Notice is not enough" June 1998

Electronic Privacy Information centre: "Surfer beware III: Privacy Policies without privacy Protection" December 1999

Heathcote, P. M. 'As' Level ICT, Payne – Gallaway Publishers, Ipswich

HIPSSA, Model Law on Data protection, ITU and EU 2012 at page 7

http://anujagarwal.hubpages.com/hub/advantages-and-disadvantage-of -internet-banking. visited on 27/5/2013

http://anujagarwal.hubpages.com/hub/advantages-and-disadvantage-of -internet-banking. visited on 27/5/2013

http://en.wikipedia.org/wiki/Telecommunications_data_retention visited on 27/5/2013

http://epic.org/privacy/cybersecurity/ visited on 25/4/2013

http://epic.org/privacy/intl/eu_data_protection_directive.html visited on 20/4/2013

http://epic.org/privacy/socialnet/ visited on 15/4/2013

http://epic.org/reports/surfer-beware2.html visited on 25/5/2013

http://epic.org/reports/surfer-beware3.html visited on 20/6/2013

http://methodotsolution.com/2010/06/advantage–and–disadvantage-of-online–

banking visited on 25/4/2013.

http://mmublog.org/wp-content/files_mf/wef_mfsd_ report_2011.pdf visited on 25/4/2013

http://techblog.brodies.com/2012/04/03/confused-over-whether-you-are-a-data-controller-or-data-processor-then-read-this/ visited on 16/4/2013

http://www.africanliberty.org/content/tanzania-analogue-digital-new-era-tanzania-broadcasting

http://www.bis.gov.uk/policies/business-sectors/information- visited on 09/5/2013

http://www.bis.org/publ/bcbs35.htm visited on 25/5/2013

http://www.bis.org/publ/bcbs76.htm visited on 13/4/2013

http://www.bis.org/publ/bcbs98.htm visited on 25/3/2013

http://www.bis.org/publ/bcbs99.htm visited on 02/4/2013

http://www.bongoslang.blogspot.com visited on 25/3/2013

http://www.bot-tz.org/BankingSupervision/Registeredbanks.asp visited on 03/4/2013

http://www.bot-tz.org/BankingSupervision/Supervisorymethodologies.asp visited on 25/7/2013

http://www.bot-tz.org/PaymentSystem/statistics.asp visited on 25/8/2013

http://www.deloitte.com/view/en_ZA/za/marketsolutions/popi-act/index.htm#%3EUnderstanding%20the%20lmportance visited on 06/4/2013

http://www.doingbusiness.org/data/exploreEconomies/tanzania/ visited on 25/6/2013

http://www.doingbusiness.org/data/exploreEconomies/tanzania/protecting-investors/ visited on 25/3/2013

http://www.ico.gov.uk/for-organisations/data-protection/the-guide/the-principles,aspx visited on 25/5/2013

http://www.ico.gov.uk/for-organisations/data-protection/the-guide/the-principles,aspx visited on 25/4/2013

ICO, The Guide to Data Protection

International Records Management Trust, FOSTERING TRUST AND TRANSPARENCY IN GOVERNANCE: Investigating and Addressing the Requirements of Building Integrity in Public Sector Information Systems in the ICT Environment, Tanzania Case study, January 2007

Justice Yatindra Singh, CYBER LAWS, 5th Edition, Universal Publishing Co. Ltd, 2012

Kamuzora, F. "E-Commerce Journey of Tanzania SMEs: The case of Tourism Industry" A paper presented at the Tanzania Development Gateway Workshop on 'The use of ICT for SMEs Development: Opportunities and Challenges' Dar Es Salaam April 11, 2005

Kenneth C. Loudon and Jane P. Loudin "Management Information Systems: Managing the digital firm" Pearson Education International, 2006 10th Edition

Lawrence Lessig, "Code and Other Laws of Cyberspace, Basic Books" New York, 1999

Loudon, K.C, 'E-Commerce Business, Technology, Society, '2nd Edition

Mambi, A., 'The Status of Cyber Laws in Tanzania'. A paper presented at Cyber Laws Work Shop for EAC, 24-28 April 2006, Kampala Uganda.

Manolescu, D. "Data Protection as a Fundamental Right" published as part of the Effective Newsletter, Issue No. 5, (2010)

Neil Robinson, Hans graux, Maarten Botterman and Lorenzo Valeri: "Review of EU

data protection Directive:Summary" May 2009

Pria Chetty, (an International Legal Expert on Data Protection) and Baraka Kanyabuhinya, (a National Legal Expert, Data Protection) a Training on DATA PROTECTION LAW, HIPSSA Project, Support for Harmonization of the ICT Policies in Sub-Sahara Africa 07th March 2013

Prof. Kierkegaard, S., Prof. Waters, N., Prof. Greenleaf, G., Assoc. Prof. Bygrave, A. L., Prof. Lloyd, I. and Prof. Saxby, S.; on 30 years

The Charter of Fundamental Rights of the European Union, 7th December 2000, Official Journal

The Universal Communication Service Access Act, 2006, Government of Tanzania

Ulanga, P. (2010) "Cyber Security in Tanzania –Country Report" Accessed at http://www.itu.int/osg/spu/cybersecurity/contributions/Tanzania_Ulanga_paper.pdf

UNCTAD (2012), *"Mobile money for business development in East Africa Community, a comprehensive study of existing platforms and regulations"* Available

World Economic Forum Report (2011) "*The Mobile Financial Services Development report*". Accessed at [http://mmublog.org/wp-content/files_mf/wef_mfsd_ report_2011.pdf

Wounds, J., "A Practical Guide to the Data Protection Act", The Constitutional Unit, 2004

www.gocsi.com

www.ucl.ac.Uk/constitution