COMPUTER RELATED CRIMES:

A COMPARATIVE ANALYSIS OF TANZANIAN AND SOUTH AFRICAN FRAMEWORKS

LINCOLN BENN ZOMBA

ZMBLIN001

Post Graduate Diploma in Law specialising in Information Communication Technology (ICT) Law

Faculty of Law, University of Cape Town

Supervisor: Associate Professor Caroline Ncube

A dissertation to the Faculty of Law, University of Cape Town, in partial fulfilment of the requirements for the Post-Graduate Diploma in Laws in approved courses and a minor dissertation. The other part of the requirement of this degree was the completion of a programme of courses.

Cape Town, February 2014

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and to pretend that it is one's own.

2. I have used the Harvard convention for citation and referencing. Each significant contribution to and quotation in this essay from the work or works of other people has been acknowledged through citation and reference.

3. This essay is my own work.

4. I have not allowed and will not allow anyone to copy my work with the intention of passing it off as his or her own work.

5. I have done the word processing and formatting of this assignment myself. I understand that the correct formatting is part of the mark for this assignment and that it is therefore wrong for another person to do it for me.

Lincoln Benn Zomba 17th February 2014

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

Signature

ACKNOWLEDGEMENTS

I thank God the Almighty for the guidance, strength, courage and hope he gave me throughout my studies.

Associate Professor C. Ncube, I thank you for your time, patience and encouragement. You introduced me to the most fascinating area of law when I needed it above all, and I thank you for calling to express disappointment when you come across something wrong while going through my treatise. Most of all, thank you for believing in me. It has been great honour and privilege to have been your student.

I wish to express my sincere gratitude to Dr Edward Gamaya Hoseah, Director General, the Prevention and Combating of Corruption Bureau and the Government of the United Republic of Tanzania for sponsoring my studies.

My sincere thanks to my colleague and friend Petro Ernest Pesha for his encouragement, support and critical review of this work. The assistance of my fellow students Ephraim Musiba and Elias Francis Mkata must also be recognised.

I wish to thank James McFarlane for professionally copy-editing and proofreading the text to ensure the correct use of language and sound presentation.

Lastly, I would like to thank my wife, Anna Grace, my sons Francis and Brian and my daughter Lulu for their tolerance and understanding when I had to leave them to pursue my studies. Without their support and understanding I would not be where I am today. I am proud of you.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 Background to the problem

> 'Unknown to most of us, we are living inside and alongside a revolution of stupendous power and energy. It is not a communist, socialist, capitalist or even a religious revolution. It is the ICT revolution, the revolution of information communication technologies that is changing the nature and patterns of our social, commercial and political interactions. Like most revolutions, its true scope cannot yet be grasped nor can all the issues it raises be clearly understood even by those at its cutting edges….'[1]

The Internet and other new technologies play an important role in today's global information society, are now essential in every sector of human life and can be used for the preparation and commission of serious and transnational crimes.

The information superhighway has made a virtually borderless world possible. One can have access to information while located anywhere in the world, within seconds and at the click of a mouse. Computer and information technology are used in business, industry, medicine, science, engineering, education, and government, to name but a few fields.[2]

Despite the fact that the terms 'computer crime' or 'cybercrime' have entered into common usage globally there is no international consensus as to what precisely is meant by the terms.[3] Casey distinguishes between cybercrime and computer crime. He defines cybercrime as 'any crime that involves computers and networks, including crimes that do not rely heavily on computers' and computer crimes as 'a special type of cybercrime that are limited and defined in laws such as the US Computer Fraud and Abuse Act and in the UK Computer Abuse Act'.[4] Watney contends that the term 'cybercrime' is preferred to the use of the term 'computer crime'

---

[1] Law Reform Commission of Tanzania 'Report of the comprehensive review of the civil justice system in Tanzania' presented to the Minister for Justice and Constitutional Affairs May 2013 at 71–72, accessed on 17 June 2013.

[2] Sandra Mariana Maat Cyber crime: a comparative law analysis (LLM thesis, University of South Africa, 2004).

[3] Gordon, S & Ford, R (2006). 'On the definition and classification of cyber crime' *Journal in Computer Virology*, at 13.

[4] Collier, D (2004), Chapter 13: 'Criminal law and the Internet' in Buys and Cronje, (Eds), *Cyber law @ SA II: the law of the internet in South Africa*, 2ed at 320.

and agrees with Maat that criminal behaviour is no longer directed only at computers, but involves computer systems, information networks, the Internet and cyberspace.[5]

Computer crime has also been defined as follows:

> …' the use of a computer as a tool in perpetration of a crime, as well as situations in which there has been unauthorised access to the victim's computer or data. Computer crime also extends to physical attacks on the computer and / or related equipment as well as illegal use of credit cards and violations of automated teller machines, including electronic fund transfer thefts and the counterfeit of hardware and software.'[6]

According to Van der Merwe, computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and/or the object of an offence and represents the basis for the suspicion that an offence has been committed.[7] Maat further defines cybercrime or information technology crime as follows: 'Cybercrime encompasses all illegal activities where the computer, computer system, information network or data is target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computers, computer systems, information networks or data.'[8]

It is my view that the above definition has merit because it encompasses all of those illegal activities that are committed by or with the aid of computers or information technology, or where computers are target of the criminal activity.

On the basis of the above, it can be argued that cybercrime has many different facets and occurs in a wide variety of scenarios and environments. Thus current definitions of cybercrime differ depending on the perception of both 'observer/protector' and victim, and are partly a function of the geographic evolution of computer-related crime.[9] On the other hand, in this mini-dissertation I intend to use the term cybercrime in its broad sense, but distinguishing between criminal activity involving stand-alone systems and criminal activity involving the Internet, where necessary.

The history of computer crime dates back to the 1960s, when the first articles dealing with computer manipulation, computer sabotage, illegal use of computer systems and computer

---

[5] Watney, M (2005) 'Regulation of Internet Pornography in South Africa'. Available at http://www.isrcl.org/Papers/2005/Watney.pdf, accessed on 27 July 2013.
[6] Credo, P & Michels, J (1985) *Computer crime in South Africa*.
[7] Dana van der Merwe *Computers and the law* (2000) 188.
[8] Maat op cit note 2.
[9] Gordon & Ford op cit note *3*.

espionage were published. In the 1980s and 1990s computer crime was no longer limited to economic crime, but included attacks against a diverse range of interests, such as privacy infringements, as well as the use of computers and communication systems in organised crime.[10] The advent of the internet has brought substantial change: at phenomenological level the dissemination of illegal contents (intellectual property infringements, child pornography, incitement to racism and xenophobia), 'illegal access to computer systems, system and data interference, illegal interception of non-public transmissions of computer data, new communication tools' also useful for the preparation of serious crimes such as terrorism.[11] The world-wide proliferation of information and communication technologies (ICT) has facilitated the commission and preparation of these types of criminal activities, which pose threats not only to the confidentiality, integrity or availability of computer systems and data to the security of critical infrastructures but also to the intellectual property rights, property and public confidence.[12]

Tanzania's legal system has been governed by the common-law system since its introduction by the Tanganyika Order in Council of 1920. The system is, however, customised with some exceptions and modifications to suit the local circumstances. This system traces its historical background mostly from the British administration during the colonial period. As it was a British protectorate, the law of Tanzania (then Tanganyika) was imported via India by the British administration, where it had been long established.[13] As such, the Tanzanian Penal Code[14] has continued in force since its enactment in 1930 and later adopted in the then Tanganyika on 28 September 1945. The founders of our legal principles could hardly have imagined the way the world has evolved and the revolutionary and continuous emergence of new technology. Legal concepts that were developed many centuries ago are struggling to cope with the advances in technology.

---

[10] Manacorda, S (2012) Cyber-criminality: finding a balance between freedom and security. *International Scientific and Professional Advisory Council*. Available at http://www.academia.edu/2313913/Cybercriminality_Finding_A_Balance_Between_Freedom_And_Security, accessed on 30 June 2013.
[11] Ibid.
[12] Maat op cit note 7.
[13] Available at *http://www.cyber.law.harvad.edu*, accessed on 27 April 2013.
[14] Cap 16 [RE 2002].

This research has established that Tanzania's criminal justice system has been using common-law crimes to fill the gap in investigation and prosecution of computer-related crimes. However, the extension of the scope of application of certain existing common-law and statutory crimes does not provide sufficiently for the criminalisation of conduct that is unique to the Internet. Moreover, it can lead to the breach of the principle *nullum crimen sine lege*, which provides that no action shall be punishable as a crime unless it constitutes an offence in terms of existing laws.[15] In terms of the Constitution of the United Republic of Tanzania,[16] every accused person has the right to a fair trial, which includes the right 'not to be convicted for an act or omission that was not an offence under national or international law at the time it was committed or omitted'.

Although various efforts have been made – and some are still ongoing – Tanzania still lacks comprehensive cyber-law for the specific purpose of regulating the ICT environment. The reform of Tanzania's criminal justice system, particularly the issue of computer-related crimes, has not attracted the attention of the policy makers and other stakeholders in the same way as happened in other areas of law.

1.2 Statement of the problem

Like many other countries, Tanzania has embraced ICT as a key enabler for social and economic development in the country. Currently, ICT has become pervasive in all areas of daily activities in Tanzania.[17] The ever-increasing role of ICT in day-to-day life has attracted the Tanzanian banking industry to embark on the use of digital banking channels, such as the Internet, cellphones, and automated teller machines (ATMs). These channels reduce operational costs and enable customers to conduct banking transactions conveniently. According to Bank of Tanzania (BOT) statistics,[18] the number of banks and financial institutions in the country has increased to 51. Similarly, available data shows that about 15 per cent of Tanzanians have access

[15] The principle of legality. See Snyman *Criminal law* (2002) 39 et seq.
[16] See art 13(6) (c) of The United Republic of Tanzania Constitution, 1977 as amended.
[17] Cyber Security in Tanzania: Report From the Cyber-Security Mini-Conference, Centre for ICT Research and Innovations, Institute of Finance Management, Dar es Salaam, 2012. Available at http://www.academia.edu/1925835/Cyber_Security_in_Tanzania, accessed on 21 April 2013.

[18] Tanzania Mainland's 50 Years of Independence: a review of the role and functions of the Bank of Tanzania (1961–2011) June 2011. Available at http://www.bot-tz.org/Adverts/PressRelease/2011-Nov-04-PressRelease.pdf, accessed on 7 September 2013.

to various financial services in the country.[19] However, the development of the ICT industry discussed above has not yet been accompanied by a parallel development in legal and regulatory reforms.

Recently social media have been used to communicate hate speech and pornography, to bully others and to spread derogatory statements dealing with religion, race, ethnicity and sexual orientation. In response, the Tanzanian Police Force uses its established Cybercrime Unit[20] in the directorate of criminal investigation in an effort to curb such activities. Mr Suleiman Kova, Dar es Salaam Special Zone Police Commander, revealed this on 9 May 2013 when he said: 'The ICT department will be dealing with people using social networks, including Jamii Forums, Facebook, Twitter, YouTube and many others to spread hate speech among religions. It will also deal with disgusting text messages.'[21]

On 8 May, 2013, Parliament urged the government to review laws in order to come up with legislation that will outlaw hate speech. The proposal was presented by Zitto Kabwe (MP for Kigoma North-Chadema), who wanted the government to take serious measures against people instigating hatred and breaching the peace.[22]

Furthermore, there have been some cases of unauthorised online posting of personal information and the online interception and subsequent disclosure of government secret information as well as the posting of false accusations against government operations and leadership. Recently the government had to issue a directive following the revelation of some private communication details, which were published by a section of the media contrary to the Electronic and Postal Communications Act No 3 of 2010 (EPOCA) and the Tanzania Communications (Consumer Protection) Regulations of 2005.[23] The majority of victims of the abovementioned cybercrimes are young females within Tanzanian higher learning institutions and celebrities, usually as a result of a broken offline/online relationship with their boyfriends. As there is no specific law to address the abovementioned crimes, a number of these cases are

---

[19] Ibid.
[20] Established in 2006.
[21] Elisha Magolanga and Henry Mwangonde 'Police to use ICT in curbing cybercrime', The Citizen 10 May 2013. Available at www.thecitizen.co.tz/News/Police+to+use+ICT+in.../-/index.html, accessed on *12 May 2013.*
[22] Parliament of Tanzania, Hansard 8 May 2013 at 40–41.
[23] *Ministry of Information, Culture and Sports, Tanzania Information Services,* 'Government orders probe on phone bugging claims'. Available at www.tanzania.go.tz/press_releasef.html, accessed on 17 April 2013.

either not reported to police stations or are reported and dealt with under the existing provisions of the Tanzanian Penal Code, which are ineffective and do not cover the said cybercrimes. These crimes are increasingly occurring in cyberspace while their impact on internet users, children and internet development is profound.

My experience and practice in the area of investigation of corruption cases, financial crimes and prosecution of high-profile corruption cases has shown that the absence of comprehensive legislation that specifically addresses cybercrimes in Tanzania, lack of guidelines and instructions pertaining to cybercrime investigation priorities, challenges, and inappropriate search and seizure procedures make it difficult for law enforcement officers and prosecutors to investigate and prosecute cybercrime successfully. It has also been observed that law-enforcement officers, public prosecutors, magistrates and information technology (IT) professionals lack the necessary legal tools as well as awareness of cybercrimes.

Police statistics show that more than 500 Tanzanians have been apprehended by the Cyber-crime Unit between 2011 and 2012 and, in the past few years, more than 1.3bn/- have been stolen across the country through cyber-fraud.[24] The Central Bank reported recently that to contain the situation, a joint taskforce had been formed to study the problem. The taskforce comprised experts from the BOT, Tanzania Bankers Association (TBA), Tanzania Communications Regulatory Authority (TCRA), the Financial Intelligence Unit and Cybercrime Unit in the office of the director of Criminal Investigation. It is expected that the taskforce's recommendations will serve as a solution to the problem of cybercrime in order to protect customers from commercial fraud.[25]

On the other hand, the provisions of s 3(1) of the Penal Code have been applied by the courts to punish persons for common-law crimes and the modifications to the common-law system have been made to suit the local circumstances. Moreover, in the absence of specific provisions of law relating to ICT, the courts in Tanzania have in certain instances addressed ICT challenges by interpreting the traditional rules broadly in such a manner as to accommodate the new

[24] Tanzania Police Force: Cybercrime unit statistics June 2012.
[25] 'Cybercrimes pick up as more financial institutions come in', Tanzania Daily News Online Edition 16 April 2013. Available at http://www.dailynews.co.tz/index.php/biz/16447-cyber-crimes-pick-up-as-more-financial-institutions-come-in accessed on *29 May 2013.*

technologies. For instance, in 2000 the High Court in the case of *Trust Bank Tanzania Ltd*[26] had to extend the definition in the paper-based statute to cover printed electronic records. In that case, judge Nsekela (as he then was) adopted the views of the English judge in *Barker v Wilson*[27] and extended the definition of bank records to include the computer printouts.

Moreover, judge Nsekela noted that 'the law must keep abreast of technological changes as they affect the way of doing business'. In another case, that of *Lazarus Mirisho Mafie v Odilio Gasper Kilenga*,[28] the High Court highlighted the lacunae in the law with regard to admissibility of electronic evidence. The court laid down criteria to be met in such scenarios that rendered the e-mails containing defamatory statements inadmissible as evidence. From the above cases, an argument can be made that the rules of admissibility under the Tanzania Evidence Act, 1967[29] (the TEA) which are mostly a codification of common-law principles, are not flexible enough to allow the admissibility of electronic evidence.

As a step towards cyber-legislation, Tanzania has made significant progress in the preparation and drafting of a computer crime and cybercrime bill, though contrary to some of the media reports, the draft bills completed while this work was still in progress, has yet to be approved by the Cabinet and submitted to Parliament for debate.[30] Some of these include the review of the National ICT policy[31] (NICTP), which was too old-fashioned to address the challenges in the sector,[32] amendment of the Tanzania Evidence Act by the Written Miscellaneous Laws (Miscellaneous Amendments) Act[33] to adjust the Evidence Act to incorporate the electronic revolution and its impact on the laws and prevailing procedures. However, one can argue that the amendment of the law of evidence has not been extensive, based on the fact that it was not accompanied by the amendment of the Criminal Procedure Act, the Penal Code and other legislation relevant to the investigation and prosecution of cybercrimes. The other review was led by the Law Reform Commission of Tanzania, and was carried out to

[26] *Trust Bank Ltd v Le Marsh Enterprises Ltd and Others,* Commercial Case No 4 of 2000, High Court of Tanzania, Commercial Division.
[27] [1980] 2 All ER 80.
[28] *Commercial Case* No 10 of 2008, High Court of Tanzania, Commercial Division.
[29] Cap 6 [RE 2002].
[30] September 2013.
[31] The policy is available at http://www.tanzania.go.tz/pdf/ictpolicy.pdf, accessed on 25 March 2013.
[32] Christopher Majaliwa 'Cyber Crime Targeted in New ICT Policy,' Tanzania Daily News Online Edition, 26 November 2012. Available at http://allafrica.com/stories/201211260091.html, accessed on 24 April 2013.
[33] Act No. 15 of 2007.

review the laws affected by ICT; its recommendations have already submitted to the Minister for Justice and Constitutional Affairs.[34] Furthermore, during the workshops of the Support for Harmonisation of the ICT Policies in Sub-Sahara Africa, (HIPSSA) project in Tanzania[35] a draft Tanzania Computer Crime and Cybercrime Bill was developed and submitted to the government. Moreover, serious consideration should be given to criminalise certain cyber-acts as the growth of ICT in Tanzania has offered criminals unprecedented opportunities to commit traditional crimes via computer systems. Failure to pay proper attention to those areas could result in dismissal of cases for lack of either proper investigation or exclusion of evidence by the court on the ground that the evidence was illegally obtained.[36]

1.2.1 Rationale for comparison between Tanzania and South Africa

The approach taken by jurisdictions to regulate cybercrime, countries can be classified into three categories. The first category does not have any legislation on this issue and still depends on traditional penal laws, such as the Tanzanian criminal justice regulatory frameworks. The second category has regulated cybercrime in legislation that deals with electronic transactions issues, such as the South African Electronic Communications and Transactions Act[37] *ch XIII*, which deals with cybercrimes. The third category has enacted specific cybercrime legislation.

Tanzania has to draw lessons from the wider regional and international efforts that have been in place for a decade. Therefore, in developing an appropriate policy and regulatory framework, has much to learn from South Africa. This is because the two countries face the same challenges in relation to cybercrimes. South Africa has been at the forefront of sub-Saharan countries for taking measures to combat cybercrime. Thus it provides benchmarks for Tanzania where specific legislation on electronic transactions is being spearheaded by the Law Reform Commission of Tanzania (LRCT).[38]

---

[34] Law Reform Commission of Tanzania, op cit note 1.

[35] Workshops held at Dar es Salaam in March and August 2013. The objective of the project is to assist the International Telecommunication Union (ITU) member states in the development of policies and laws in the areas of data protection, cybercrime and electronic transactions or electronic commerce. Tanzania is a member of the ITU.

[36] Section 169(1) of Cap 20 [RE 2002].

[37] Act 25 of 2002.

[38] Law Reform Commission of Tanzania, op cit note 1 at 71–75.

1.2.2 Research questions

This study has the following research questions:

(1) Is the Tanzanian legal and regulatory framework adequate to deal with cybercrime issues?

(2) If not, how and to what extent should the existing legal and regulatory framework be improved?

This dissertation argues that the laws relating to common-law and statutory crimes in Tanzania's criminal justice system have not been applied efficiently to combat cybercrimes. This is because the extension of the scope of the application of existing common-law and statutory crimes does not provide sufficiently for the criminalisation of cybercrimes and the scope of computer systems is beyond the capacity of traditional approaches to criminal investigation.

The answers to these questions will be provided in the following chapters. Furthermore, as it was pointed out earlier, the chapters do not comment on the Cybercrime draft Bill, because it has yet to be officially released by the Ministry for Justice and Constitutional Affairs.[39] I shall begin the next chapter by examining the policy and regulatory framework for combating cybercrimes.

[39] Op cit note 30.

CHAPTER 2
POLICY AND REGULATORY FRAMEWORK FOR COMBATING CYBERCRIME

2.1 The Tanzanian ICT Policy

The Tanzanian Government is developing an appropriate policy and regulatory framework that will accommodate technological changes and customer interests. For instance, in 2001 it appointed the Ministry of Communications and Transport (MoCT) as the national ICT co-ordinator and focal point of all ICT related issues. The main tasks of the MoCT were to formulate and prepare the national ICT policy document that would guide the provision of ICT services in Tanzania. The NICTP [40] was launched in 2003. However, in 2008, upon the establishment of the Ministry of Communication, Science and Technology (MCST) the responsibility for NICTP was transferred from the MoCT to the MCST.

The vision of the Tanzanian Government in regulating ICT is vividly captured in the objectives of the policy which were grouped into nine main areas. These are: strategic ICT leadership, legal and regulatory framework, capacity building, ICT infrastructure, ICT industry, ICT productive sectors, service sectors, universal access, and local content.[41] In relation to the legal and regulatory framework, the NICTP 2003 envisaged the enactment of laws relating to cybercrimes and also the review of existing laws to accommodate the technological changes in ICT. However, as the 2003 NICTP has marked its tenth anniversary, there have been concerted efforts and clear progress in only some of the objectives, namely infrastructure, human capital, and public service. Implementation in the focus areas of strategic leadership, legal and regulatory framework, local content and ICT industry, on the other hand, is lagging behind.

Following the above, it is encouraging to note that the Tanzanian Government has announced that it has undertaken the review of the current ICT policy in order to incorporate other relevant issues, including addressing cybercrime, which is reported to be on the increase. Moreover, there is a strong commitment at the highest political level to fully utilise and develop ICT as an enabler of the information society and for the benefit of Tanzanians. For instance, when addressing a meeting of senior police officials in Dodoma recently, President Jakaya Kikwete

---

[40] The policy is available at http://www.tanzania.go.tz/pdf/ictpolicy.pdf, accessed on 25 March 2013.

[41] Mollel, A et al *Electronic Transactions and Law of Evidence in Tanzania (*2007) 45–46.

directed the police force to introduce ICT into their training programmes so that the officers would be able to use modern technology to combat crime.[42]

2.1.1 The South African ICT policy

South Africa does not have comprehensive policies to address the issue of ICT in depth. Thus, the South African ICT sector is not unique. Regarding the present analysis, particularly for the purpose of drawing comparisons between the Tanzanian and South African ICT policies, it is interesting to note that, owing to the rapid development of technologies and their accompanying regulatory challenges, the South African Government has recently appointed a panel, led by Mr Joe Illjwara, to analyse and outline remedial recommendations for South Africa's current policy and regulatory framework and submit a draft green paper for an integrated National ICT Policy by October 2013. It is also envisaged that the panel will be in a position to table a white paper by March 2014.[43] Moreover, the South African Government has published a proposed ICT policy review framing paper 2013.[44] This proposed paper underpins the development of a new communications sector policy framework based on the South African National Development Plan (NDP),[45] which seeks, among other things, to provide a seamless information structure that will be universally available and accessible at a cost and quality at least equal to South Africa's main peers and competitors. Other measures include the formulation of the National Cyber Security[46] Policy Framework (NCPF) which was developed to ensure a focused and all-embracing safety and security environment, which was approved by Cabinet on 7 March 2012.[47]

2.2 Electronic and Postal Communications Act, 2010

In 2003 the Government of Tanzania established a quasi-governmental body known as the Tanzania Communications Regulatory Authority (TCRA) for regulating the communications and broadcasting sectors. The Authority was established under the Tanzania

---

[42] A speech delivered at the Police Force Senior Officials' General Meeting in Dodoma, 12 February 2013.
[43] *Engineering News*, 'DoC aims to publish ICT policy white paper by March 2014', 11 April 2013. Available at http://www.engineeringnews.co.za, accessed on 26 April 2012.
[44] Department of Communications, Notice 429, published in *Government Gazette* on 24 April 2013.
[45] South African National Planning Commission, 'National Development Plan 2030'. Available at http://www.npconline.co.za, accessed on 10 May 2013.
[46] Available at www.justice.gov.za/m_speeches/2013/20130404-dm-cyberlaw.html, accessed on 15 June 2013.
[47] Op cit note 33.

CommunicationsRegulatory Authority Act,[48] which merged the Tanzania Communications Commission and the Tanzania Broadcasting Commission. The Electronic and Postal Communications Act of 2010[49] was passed by Parliament in January 2010 and came into force on 18 June 2010. The EPOCA operates under the functional arm of the TCRA. It addresses primarily the areas of postal codes, digital broadcasting and central equipment identification register (CEIR), SIM-card registration and the computer emergency response team (CERT) which acts as the primary security service provider for the government and the citizens. At the same time CERT acts as awareness raisers and educators.

In Tanzania up to 17 June 2010 cybercrime had to be dealt with in accordance with the Tanzanian statutory and common law providing for specific crimes. The EPOCA comes closest to this function, as it governs limited aspects of cybercrime, focusing only on unauthorised access or use of a computer system. Section 124(3) of the Act deal with the offence of intention to cause loss or damage to the public or any person or any information stored on computers. The penalty for offences committed under s 124(3) is a fine of not less than 500 000 Tanzanian shillings or to imprisonment for a term not exceeding three months or to both such fine and such imprisonment. It is noteworthy; however, that the law is not exhaustive as it does not capture all aspects of cybercrime. Exceeding authorised access, for example is not criminalised. Moreover, the term *unauthorised access* is not defined anywhere in the Act. Unfortunately there is no case law dealing with the application of the above provision of the law as, in practice, the Penal Code is usually resorted to in order to prosecute computer fraudsters, which will be discussed below. One of the major criticisms of the Act is that it covers issues arising from communications only, while key elements of cybercrimes and the principles of data protection are not adequately addressed. Apart from that, there is a debate among legal academics and lawyers who assert that the Act is too punitive, as it concentrates more on punishing offenders than enhancing development of the communications sector.

[48] Act 12 of 2003.
[49] Act 3 of 2010.

2.2.1 The South African position

The South African criminal justice system used to extend the common and statutory law as widely as possible to cybercrimes. However, due to the technological changes that have taken place in the world, the South African common law has been found lacking in many of the tools necessary for combating cybercrime. It was also evident that the common law provided for traditional crimes that were committed online but did not provide for cybercrime and legislation had to be introduced to criminalise conduct such as spamming, hacking and phishing.[50] It was also observed by the courts that the prevailing common law could not admit into evidence disputed documents containing information that has been processed and generated by a computer.[51]

The South African Government in August 2002 implemented the Electronic Communications and Transactions (ECT) Act, which provided for the facilitation and regulation of electronic communications transactions.[52] Furthermore, the ECT Act contains specific statutory provisions on cybercrime relating to information systems and included unauthorised access to data and interception of or interference with data.[53] Section 86(1) read with the penalty clause in s 89(1) contains an anti-hacking and anti-interception provision that criminalises unauthorised access to a computer or computer system, or the interception of information, whereas s 86(2) read with the penalty clause in s 89(1) prohibits unlawful modification of data. Section 86(3) read with the penalty clause in ss 89(1) and 86(4) and with the penalty provision in s 89(2) contain anti-cracking provisions.[54] E-mail bombing and spamming is an offence under the provision of ss 86(5) and 45, whereas s 87 of the Act criminalises cybercrimes of extortion, fraud and forgery.

At this juncture, for the purposes of drawing comparisons on criminal sanctions between the South African ECT Act and the Tanzanian EPOCA Act, it is interesting to note that in South Africa, Van der Merwe correctly criticised the criminal sanctions of the ECT Act for being too

---

[50] Op cit note 10.

[51] Ibid.

[52] The ECT Act comprises 14 chapters and 95 sections and addresses such issues as online contracts (chapter III), consumer protection (chapter VII), protection of personal information (chapter VIII) and limitation of liability of service providers (chapter XI). It makes specific provision in chapter XIII for the investigation and prosecution of Internet crimes.

[53] Goodburn and Ngoye (2004), Chapter 7: 'Privacy and the Internet' in Buys and Cronje (Eds), *Cyber law @ SA II: the law of the internet in South Africa*, 2ed at 185.

[54] Watney, M (2012), Chapter 15: 'Cyber-crime and the investigation of cyber-crime' in Papadopoulos and Snail (Eds), *Cyber law @ SA III: The law of the Internet in South Africa*, 343–344.

lenient to offenders,[55] which appears also to be the case with Tanzania's EPOCA Act.[56] However, in the Electronic Communications and Transactions (ECT) Amendments Bill, 2012,[57] maximum penalties of from 12 months' to ten years' imprisonment, or fines of up to R10 million for contraventions of s 86(1) to 86(3) are being proposed.

Furthermore, it is important to note that the ECT Act has been in place for a decade, whereas the world has experienced significant increases in hacking, security breaches, data mining for financial purposes, misuse of personal information, cyber-security threats and cybercrime. In response to those challenges the South African government, through its Communications department, has introduced proposed amendments in the ECT Amendments Bill. The Bill seeks to amend the ECT Act to bring it into line with the international community with regard to communications. The Bill also seeks to align the ECT Act with current trends in legislation, such as the Consumer Protection Act[58] and the Protection of Personal Information Act.[59] The ECT Act has facilitated the investigation and prosecution of cybercrime and the admission of electronic evidence. For instance, on December 2009 a senior First National Bank (FNB) employee, one Morwesi Theledi, was arrested by the South African Police Services (SAPS) on allegations that she stole her colleague's PIN and passwords and gained access to Amalgamated Beverage Industries' (ABI's) bank account and made away with R27.3 million. The SAPS used the provisions of the ECT Act to investigate the suspect.[60] The ECT Act, in terms of the provisions of s 15, provides for the admissibility and evidential weight of a data message as electronic evidence. For instance, in *S v Motata*,[61] the accused was charged with, *inter alia*, driving a motor vehicle while under the influence of alcohol. After the accused allegedly crashed into the boundary wall of a residential property that belonged to the complainant, the complainant in the matter made certain audio recordings on his mobile phone and took some photos on the scene of the accident with a digital camera. The audio recordings were later transferred from the mobile

[55] The penalty provisions of the ECT Act –, maximum periods of imprisonment of one year for most of the crimes prohibited by s 86 of the Act – seems woefully inadequate when compared with those of similar Acts, such as the RIC Act. See Van der Merwe D (2008) *et al* 76–78.
[56] For instance, the penalty for the offence of unauthorised access to or use of a computer system under s 124(3) would attract a fine of not less than 500 000 Tanzanian shillings or imprisonment for a term not exceeding three months or to both such fine and such imprisonment.
[57] Department of Communications, Notice 35821 published in *Government Gazette* of 26 October 2012.
[58] Act 68 of 2008.
[59] Act 4 of 2013.
[60] Section 86 (1).
[61] Unreported case no. 63/968/07, Johannesburg district court at 622.

phone and stored on the complainant`s laptop. At the trial the court found that the audio recordings were documentary evidence and ruled them to be admissible.

However, in the subsequent application for review by the applicant, the High Court of South Africa stated that a video film, like a tape recording, 'is real evidence, as distinct from documentary evidence, and provided it is relevant, it may be produced as admissible evidence, subject to any dispute that may arise either as to its authenticity or the interpretation thereof '.[62]

In another remarkable case, concerning a South African music celebrity, one Molemo 'Jub Jub' Maarohanye and his co-accused Themba Tshabalala, the magistrate sitting at Protea magistrate's court[63] accepted electronic evidence in the form of cellphone video footage showing the accused persons drag-racing, during which one of their Mini Coopers ploughed into a group of schoolchildren on Mdlalose Drive, in Protea North on 8 March 2010. The duo were found guilty on 16 October 2012 on charges of murder and attempted murder and driving under the influence of drugs and alcohol and each sentenced to 20 years' imprisonment.[64]

[62] *Motata v Nair NO* 2009 (2) SA 575 (T) para 21.
[63] My efforts to procure a registration number of the case from Protea magistrate's court proved futile.
[64] Available at *http://www.news24.com/Tags*, accessed on 15 June 2013.

CHAPTER 3
SPECIFIC CYBERCRIME INCIDENTS IN BOTH TANZANIA AND SOUTH AFRICA

3.1 Electronic banking theft

The term digital banking refers to the use by customers of the Internet, cellphones and ATMs as banking delivery channels. Online banking refers specifically to the use of the Internet for banking transactions, while cellphone banking is defined as the employment of mobile phone devices to conduct one's banking business.[65]

Although digital banking in Tanzania is still in its infancy, it has been noted that with the ongoing migration from traditional banking to digital banking in the past decade and the adoption of digital banking services by the banks and mobile phone companies has made the banking industry grow tremendously. Almost all leading commercial banks in the country now have digital banking services. Furthermore, a number of banks have adopted the use of automated teller machines (ATMs) for providing banking services other than traditional banking service delivery. In early 2012 it was estimated that about 1000 ATMs had been installed with approximately 2 million ATM cards in circulation. This has led to a new crimes include skimming, SIM (Subscriber Identity Module) card swapping, phishing and 'spoofing', ATM bombings and SMS (Short Message Service) interception. Recently, there have been reports that ATM theft has hit several banks in Dar es Salaam, Mwanza, Mbeya, and Arusha.[66] Between December 2012 and March 2013 a number of customers of different financial institutions have complained of having their accounts tampered with at ATMs.

The Tanzanian Police have managed to apprehend some of the perpetrators of these crimes. For instance, at midnight on 10 February 2013 police in Mwanza city arrested Salim Nassoro, Maniki Kimani and Leonard Masunga in connection with the theft of 500 million Tanzanian shillings from various banks using fake ATM cards. According to the statement released by Mwanza police force,[67] the suspects were found with 194 National Microfinance Bank (NMB)

---

[65] Dagada, R (2013) 'Digital banking security, risk and credibility concerns in South Africa' in *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec 2013)* at 148–161.
[66] Jaffar Mjasiri 'Heads roll as ATM theft wave hits local banks,' Tanzania Daily News Online Edition 25 November 2012. Available at www.touch.dailynews.co.tz/.../local-news/11971-heads-roll-as-atm-theft, accessed on 24 April 2013.
[67] Briefing to the press by the Acting Mwanza Regional Police Commander Christopher Fuime, 14 February 2013.

and Diamond Trust Bank ATM cards, 36 Kenya Commercial Bank (KCB) ATM cards and 18 other cards with no logo, and equipment allegedly used to manufacture fake ATM cards. Furthermore, the suspects were found in possession of a camera and three cans of spray paint which they used to black out CCTV cameras to conceal their identity as shown in *Appendix I* to this work.

From the facts of the above case one would have expected the suspects to face cybercrime or computer crime charges. To the contrary, they were arraigned on 20 February 2013 before the Mwanza resident magistrate and charged with the traditional common-law offences of forgery contrary to ss 333, 335(a) and 338 of the Penal Code and stealing contrary to ss 258(1) and 265 of the Code[68] as shown in *Appendix II* to this work. It is my argument that the above case illustrates the inability of the traditional common-law to address cybercrimes such as illegal access to computer system, electronic fraud and so on. Presenting the view of the official opposition in the National Assembly, Mr Joshua Nassari (Member of Parliament for Arumeru East-Chadema), warned against the escalating rate of cybercrime in the country, where thefts of money amounting to 2.2 billion Tanzanian shillings were recently reported to police. Mr Nassari, who is the shadow Minister for Communications, Science and Technology, said cases of theft of 1.3 billion Tanzanian shillings; 8 897 Euros and 551 777 US dollars, which were recently reported to police, represented a huge amount of money for a nation that has a struggling economy, and called for incisive state intervention.[69]

In a move to curb the escalating incidents of theft of cash from ATMs and other related activities, the BoT has teamed up with four other specialised agencies to get to the bottom of cybercrimes whose perpetrators have so far eluded police and financial intelligence. According to the BoT Director for National payment systems, Lucy Kinunda, the high-level task force has drawn expertise from the BoT, the Tanzania Bankers Association (TBA), the Tanzania Communications Regulatory Authority (TCRA), the Financial Intelligence Unit and the Cyber-crime Unit in the office of the Director of Criminal Investigation. Ms Kinunda stated that the major tasks before the team are: to study the escalating incidents of theft of cash from ATMs across the country and recommend measures to curb them.

---

[68] Criminal case no 19 of 2013.
[69] Parliament of Tanzania, Hansard 25 July 2012 at 158–159.

It is expected that the task force recommendations will serve as a blueprint for solving the problem of cybercrime in order to protect customers from commercial fraud.[70] While the researcher acknowledges and welcomes the above projected measures by the Central Bank of Tanzania, he is of the view that there is low awareness and skills among ATM users in Tanzania who provide serious vulnerability threats by ignoring data protection and compromising access credentials. In one incident in Mbozi-Mbeya, a number of teachers surrendered their ATM cards and PIN numbers to their debt collector so that it could be easier for him to recover his money after their salaries were credited to their accounts.[71]

3.2 Child pornography

The World Health Organisation defines child sexual abuse as the involvement of a child in sexual activity that he or she does not fully comprehend and is unable to give informed consent to, or that violates the laws or social taboos of society. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person. This may include but is not limited to the inducement or coercion of a child to engage in any unlawful activity, the exploitive use of a child in prostitution or other unlawful sexual practices, or the exploitive use of children in pornographic performances and materials.[72] Child pornography has received a great deal of attention in recent years from sociologists, criminologists, media and legislatures, as reflected by the enactment of a large number of laws relating to child pornography.[73] Furthermore, it has led to a world-wide discussion on how to regulate the online porn industry.

For instance, the recent decision by the ICASA to grant TopTV three pornography channels on its pay-TV platform has drawn a vast reaction from the public, to the extent that social media

---

[70] 'Cyber-crimes pick up as more financial institutions come in', Tanzania Daily News Online Edition 16 April 2013. Available at *www.dailynews.co.tz ›* Local News, accessed on 29 May 2013.
[71] Ludovick Kazoka 'Teachers main victims of ATM scam – police', Tanzania Daily News Online Edition 17 February 2013. Available at *www.dailynews.co.tz ›* Local News, accessed on 27 March 2013.
[72] 'Ministry of Women and Child Development, Government of India (2007) 'A study on child abuse: India 2007'. Available at http://wcd.nic.in/childabuse.pdf, accessed on 22 June 2013.
[73] Maghaireh, AMS, Jordanian cyber-crime investigations: a comparative analysis of search for and seizure of digital evidence, Doctor of Philosophy thesis, Faculty of Law, University of Wollongong, 2009. Available at http://ro.uow.edu.au/theses/3402, accessed on 16 March 2013.

such as Twitter and Facebook were flooded with quips and comments on the topic.[74] Of particular interest in this reaction was the tension between the constitutional right to freedom of expression; the 'rights' of viewers to receive pornography on television; and the paramount constitutional right of children to be protected from harm.

3.2.1 Child Pornography in Tanzania

Generally, pornography is illegal in Tanzania. However, with greater access to technology and increasing Internet usage, Tanzania's anti-pornography laws are becoming more difficult to enforce. The distribution of pornographic materials over websites has increased and the impact of this activity is severe, especially on children and young persons. In 1998, the Tanzanian Penal Code was amended by the Sexual Offences Special Provisions Act of 1998 (SOSPA)[75] to add provisions relating to sexual and other offenses to further safeguard the personal integrity, dignity, liberty and security of men, women and children. In determining whether pornography involves minors, one has to determine the age at which a person can consent to sexual activity. Due to differences in culture and social values, it appears that there is no definitive parameter of what constitutes the age of consent for sexual activity. For instance, in Tanzania, a person under the age of eighteen years is considered to be a minor, as determined by s 138B of the Penal Code. Of relevance to the present analysis is the fact that the age of consent for sexual activity is eighteen years, according to s 130 of the Penal Code; however, the age of consent for sexual activity in terms of s 13 of the Law of Marriage Act,[76] is 15 years. Consequently, the amended Penal Code provision provides for legal protection to all children under the age of 18 years against child pornography and other objectionable content. However, the use of the Internet for crimes against children is not specifically mentioned in SOSPA, save under s 138B – Sexual exploitation of children. However, it is important to note that the provisions of s 118 of the EPOCA,[77] recognises the need to protect children from undesirable online content by its prohibition on the transmission and distribution of obscene materials via any network facilities, network services or content services. A person found guilty of the sexual exploitation of children

---

[74] Bonnie Tubbs 'TopTV porn gets SA hot and bothered', available at http://www.itweb.co.za/index.php?option=com_content&view=article&id=63585, accessed on 25 April 2013.
[75] Sexual Offences Special Provisions Act 4 of 1998.
[76] [CAP 29 RE 2002].
[77] Act 3 of 2010.

under the SOSPA is liable upon conviction to a term of imprisonment not less than five years and not exceeding twenty years, whereas the penalty for offences committed under the above section of EPOCA shall, on conviction, be a fine not less than 5 million Tanzanian shillings or imprisonment for not less than twelve months or both.

From the sections of the law discussed it can be argued that those who commit the abovementioned offences could be charged under the provisions of s 138B(C) of the SOSPA when read together with the provisions of s 118(a) of the EPOCA on the basis that the website or the Internet is used to create and/or distribute the objectionable materials and that act is regarded as online distribution of obscene materials. Against this background, there is a need for an amendment to the SOSPA given the wider audience and considering the greater effect that the Internet has on a child. Recently, in Tanzania, there has been a public outcry that pornography is increasingly being embraced by children as a favourite source of entertainment due to easy access to pornographic materials through publications, videos, and Internet sites.

A prominent psychologist in Tanzania, Dr Andrew Mchomvu, remarked: 'This phenomenon has exposed children to practices like child-to-child sex and sodomy which were not there before. Incidents of sodomy and rape are now common in families and schools due to the floodgate of porno in our communities.'[78] On his part, Professor John Nkoma, the Director General of TCRA stated that his agency was mandated to license Internet service providers; it did not have control over the content. 'We act as a road that allows cars to pass on but we do not have the power to choose what kind of a car should pass on it.' According to Professor Nkoma, circulation of pornographic materials was a part of cybercrime which has become a major global challenge in telecommunication industry.[79]

3.2.2 Child pornography in South Africa

In South Africa, the rights of the children under the age of 18 years against any form of abuse, maltreatment, neglect or degradation are protected under the South African Constitution.[80] Since

[78] Bernard James 'Concern over increased access of pornographic materials to children in Tanzania,' *The Citizen* Sunday dated 27 May 2012. Available at www. consolationafrica.wordpress.com/.../concern-over-increased-access-to-po, accessed on 26 March 2013.
[79] Ibid.
[80] Section 28 of the Constitution of South Africa, 1996.

the advent of Internet services in South Africa, legislation pertaining to child pornography[81] has been amended from time to time to keep abreast of the technological changes and to close the gaps and loopholes that were caused by the development of the new technology.[82] Owing to the nature of the Internet, children could be exposed, intentionally or unintentionally, to sexually explicit content, including child sex abuse images, which may have negative psychological or behavioral effects on them. Unintentional exposure may occur by accident or inadvertence in the form of pop-ups or misleading domain names, during otherwise innocuous activities.[83]

The Internet has explicitly been included in the definition of publications and all forms of child pornography on the Internet will constitute criminal offences.

The Film and Publications Act covers various provisions that govern the distribution, exhibition and publication of pornography. Of relevance to the present analysis is the fact that the Act treats all forms of pornography on the Internet as publications, with the exception of a pornographic video clip, which could rather be treated as a film, because the images can be seen as a moving picture.[84] In South Africa, the legal age of consent is 16 years. In terms of s 27(1) and s 28 of the Act, any person who creates, produces, imports or is in possession of a publication or film which contains a visual presentation of child pornography, shall be guilty of an offence. Furthermore, under the provisions of s 27A of the Act,[85] Internet service providers are obliged to register with the Films and Publications Board and take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography. A person who fails to comply with the provisions of s 27(4) of the Act[86] is guilty of an offence.

3.3 Cyber-stalking

Cyber-stalking is a new form of computer-related crime occurring in Tanzania. Cyber-stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing

---

[81] Films and Publications Act 65 of 1996.
[82] Section 1*(b)* of the Films and Publications Amendment Act 34 of 1999.
[83] Mathew, LA (2009) 'Online child safety from sexual abuse in India', (1) *Journal of Information, Law & Technology (JILT)*, Available at http://go.warwick.ac.uk/jilt/2009_1/mathew, accessed on 10 April 2013.
[84] Nel, S (2004), Chapter 8: 'Freedom of expression and the Internet' in Buys and Cronje, (Eds), *Cyber law @ SA II: the law of the internet in South Africa*, 2ed at 217.
[85] Watney op cit note 49.
[86] Ibid.

websites and email.[87] Although there is no universally accepted definition of cyber-stalking, the term has been defined as the use of electronic means of communication, including pagers, cellphones, emails and the Internet, to bully, threaten, harass and intimidate a victim. It has also been defined as nothing less than emotional terrorism.[88]

However, it is important to note that the law is not exhaustive, as it fails to provide adequate protection against the abovementioned incidents of cybercrime. It was recently revealed by Dr Zaipuna Yonah, the Director of Information and Communications Technology (ICT) at the Ministry of Communications, Science and Technology, that cybercrime is a critical challenge in Tanzania and the government is taking measures to protect its people from it. He also stated that 'there are so many crimes being reported, but we do not have a strong cyber-crime law to help the victims get legal redress'.[89]

3.4 Hate speech on the Internet in Tanzania

The term 'hate speech' generally refers to epithets or disparaging and abusive words and phrases directed at individuals or groups who represent a specific race, religion, ethnic background, gender or sexual preference.[90] The internet has provided an international stage where hate groups can utter their ideas online before a potentially huge Internet audience, but where they can nevertheless remain anonymous.

The Constitution of the United Republic of Tanzania under art 18(1) stipulates that 'subject to the laws of the land, every person is entitled to freedom of opinion and expression; that is to say, the right to freely hold and express opinions and seek, receive, and impart information and ideas through any media and regardless of frontiers…'.

Although art 18(1) of the 1977 Constitution protects the right to freedom of expression the provisions of s 31(1)*(d)*(e) and 32(1)*(b)*(c) of the Newspapers Act 1976 clearly indicates that the protection would not be afforded to those who have an intention of raising discontent or disaffection among the inhabitants of the United Republic, or who promote feelings of ill-will

---

[87] Jaishankar, K and Uma Sankary, V 'Cyber-stalking: a global menace in the information super highway'. Available at www.erces.com/journal/articles/archives/volume2/vo3/vo2.htm, accessed on 9 May 2013.
[88] Laughren, J 'Cyber-stalking: awareness and education'. Available at http://www.acs.ucalgary.ca/-dabrent/380/webproj/jessica.html, accessed on 1 March 2013.
[89] Ministry of Communications, Science and Technology press release, 25 April 2013.
[90] Buys and Cronje op cit note 84 at 222.

and hostility between different categories of the population of the United Republic of Tanzania that would result in an incitement to cause harm. Note that the provisions of s 31 of the Act articulate that the offence is committed where there is an *intention* on the part of an offender.

For instance, during the 2010 General Elections in Tanzania a hate-message was circulated using the platforms of mobile operators including Vodacom, Airtel, Tigo, Zantel, TTCL and Sasatel to mobile subscribers through telephone numbers +3588976578 and +3588108226. The message was in Kiswahili, but in summary it stated: 'Beware of Dr Willbroad Slaa, the Presidential contestant on CHADEMA ticket in the 31 October 2010 elections as he is all out to cause chaos and bloodshed in the country.' The message very soon gained prominence in the traditional media such as newspapers, radio and television and spread all over the country like a bush fire.

A joint investigation by police force and other state organs established that a local IT specialist dispatched this message using the Finnish country code and telephone numbers. Furthermore, it was revealed that the culprit was operating from the fifth floor of Barclays House in Dar es Salaam. In another recent incident in May 2013, the Dar es Salaam Regional Commissioner, Mr Meck Sadiki, announced the decision of the government to ban all religious hate speech, stating that the prohibition extended to mosques and churches using loudspeakers to spread hate speech. The decision, announced during a meeting of clerics organised by the government as a way to resolve religious tensions, also applied to people who sell cassettes or other recordings containing hate speech.

According to Nel, this is an area where there is a definite tension between freedom of expression and speech that not only insults but also incites and threatens. Various countries have recognised the need to combat hate speech.[91] Tanzania is no exception. There is a need for the government to regulate such behaviour as hate speech circulated via ICT media in Tanzania, that could cause unrest in the country.

[91] Buys & Cronje op cit note 90 at 223.

3.4.1 Hate speech on the Internet in South Africa

Like that of Tanzania, South Africa's Constitution does not extend its protection of freedom of expression to advocacy of hatred that is based on race, ethnicity, gender or religion which constitutes incitement to cause harm.[92]

In terms of s 10 of the Promotion of Equality and Prevention of Unfair Discrimination Act and the Films and Publications Act the distribution of hate speech is a criminal offence. However, the criminal sanctions of the said provisions of law do not extend to *bona fide* scientific, documentary, dramatic, artistic, literary and religious works or to publications that amount to a *bona fide* discussion, argument or opinion on any matter pertaining to religion, belief or conscience. According to the Films and Publications Act, the criminal liability of the Internet service providers (ISPs) for distributing hate speech is based on their knowledge of the nature of the content.[93] From the above the South African approach provides a model for Tanzanian lawmakers to adopt and follow.

[92] Section 16 (1)(2) of the 1996 Constitution.
[93] Buys & Cronje op cit note 91 at 225.

CHAPTER 4

CYBERCRIME INVESTIGATION

The investigation, prosecution and suppression of crime for the protection of the citizen and the maintenance of peace and public order is an important goal of all organised societies. The famous adage says that crime does not pay, and it is generally accepted that once a crime has been committed it should be investigated; the perpetrator should stand trial and on conviction be punished for his unlawful conduct.[94] The term 'investigation' denotes a methodical process of gathering facts and evidence in order to reconstruct an incident objectively and accurately so as to form the basis upon which the evidence of an act or omission can be evaluated.[95]

In an effort to curb cybercrime, the then police service in 2006 established the Cybercrime Unit, a team of police investigators who specialise in cybercrime investigation, including

tracing of 'on-line' suspects;
tracing and location of Internet-based messages and information;
forensic search and seizure of memory-resident data and computer-related information;
forensic analysis of seized material; and
Internet and networked-based surveillance.

The unit operates under the Directorate of Criminal Investigation. The statistics from the Cybercrime Unit indicate that the country is becoming prone to cybercrime as shown in the appended police statistics.

According to annexures 1 and 2 of the statistics, the following generalisations in respect cybercrimes in Tanzania may be drawn:

1. The adoption and use of ICT, particularly mobile and internet technologies in daily activities during the preceding years, has provided new opportunities for cybercrime and hence, escalated incidences of cybercrime.
2. There has been a tremendous rise in the incidence of cybercrime in large cities such as Dar es Salaam, Mwanza, Arusha, Dodoma and Mbeya compared to other regions, mainly

---

[94] *United States of America v Controni* (1989) 48 CCC (3d) 193 at 215.
[95] Hoseah, EG (1999) in *PCB Manual* 1998/99, Prevention of Corruption Bureau, at 85.

because the growing use of Internet facilities and mobile phone services have provided new opportunities for cybercrime.

3. Border entry regions such as Dar es Salaam, Mwanza, Arusha, Kilimanjaro, Tanga, Mbeya and Kagera have recorded a tremendous rise in cybercrime incidents compared to other regions, owing to the fact that there is an expansion of trade along the border regions which goes in tandem with growing use of electronic commercial transactions, thus opening new opportunities for cybercrime.

4.1 Cybercrime investigation challenges

4.1.1 Search and seizure

The purpose of the power to seize articles is to allow law-enforcement officials to obtain evidence to help them investigate and prosecute criminal offences. However, it is imperative to note that the above provisions of the law are in essence aimed at facilitating the process of investigation and collection of tangible evidence of the commission of offences.

In the cyber-world, when the data is contraband evidence, or instrumentalities of crime, the subject of the search will be intangible items, such as data, images, files and so on. Investigators enter a real home or other building, search and seize data or they seize hardware, such as hard disks, and then make a mirror copy.[96] The investigator acquires evidence by entering digital commands through a keyboard, or using forensic tools to retrieve the requested evidence and sends it to an output device, such as a monitor or printer to display the evidence. [97] Forensic experts, scholars, and investigators have addressed the issue of whether computer searches should be conducted on-site or off-site.[98] From a technical point of view, they argue that digital evidence recovery and analysis processes may impose technical and logistical restrictions on the officers executing the search and make an on-site search impossible or impracticable. Hence, the majority of forensic experts and DOJ guidelines recommend that computer searches and acquisition of data must be performed off-site. They argue that the conditions in the laboratory,

[96] Kerr, S O, 'Search and seizure in digital world' (2005) 119 *Harvard Law Review* 538–540.
[97] Ibid.
[98] Ibid.

such as temperature, time flexibility, expert support and other technical issues, such as overcoming password-protected systems are better controlled in the laboratory than in the search location.[99]

On the other hand, Brenner argues that cyber-searches should not be conducted off-site. From a practical point of view, she explains that computer searches using automated search techniques such as a key-word search will take less time and effort to perform on digital containers compared with hard-copy file searches.[100] Such seizures can have immediate and catastrophic effects on computer users who have no connection to the conduct being investigated. Offices cease to function; businesses can no longer operate or service customers; bulletin boards and other forums are shut down.

For their part, the law enforcement agencies explain the above practice by referring to problems inherent in searching not only computers but any other storage system. The searching officers cannot know precisely which part of the system contains the data they seek. This view is shared by Smith, a renowned cybercrime scholar, who argues that a major problem lies in the seizure of digital evidence from hard drives on networked computers in which both relevant and irrelevant materials (as well as legally privileged material) that are contained together. He further contends that in such situations, the practical problem arises when one has to determine which material is relevant to the charges in question. Hence, it creates problems with invalidity of the whole search and seizure procedure. In the American case of *US v Carey*,[101] while conducting an authorised search of the defendant's computer for evidence of drug-related crimes, an agent discovered a file containing child pornography. A subsequent search for more evidence of child pornography exceeded the scope of the warrant and was an unconstitutional 'general search'. Neither the defendant's consent to a search of his apartment nor the 'plain view' doctrine justified the agent's warrantless search for evidence of a non-drug-related crime. But in another case, *US v Caron,*[102] A computer repairman inadvertently found between five and seven images of child pornography while repairing the defendant's computer. An agent asked the repairman to open one such file prior to obtaining a search warrant. The fourth Amendment was not violated

[99] Alaeldin Maghaireh, op cit at 64.
[100] Brenner, S, Frederiksen, B 'Computer searches and seizures: some unsolved issues', (2001/2002) *Michigan Telecommunication and Technology Law Review* 59.
[101] 172 F3d 1268 (10th Cir 1999).
[102] 2004 WL 438685 (D Me 9 March 2004).

because the agent did not exceed the scope of the repairman's 'private search'. It is practically impossible to examine 80 GB of data held on a hard drive in order to determine what is relevant.

Other problems relate to disabling networks when seizing data, especially for large public or private sector organisations that have 24-hour access to networks, and offenders who refuse to provide the decryption key or password. Moreover, with the right sort of elegant technology, computer data in the storage device or media can be erased, replaced with other data, hidden, encrypted, modified, misnamed, misrepresented, or otherwise made unusable at push of a button. It is therefore advisable that a search be done with immediate effect to prevent the destruction of evidence and to preserve the integrity of data.

Furthermore, according to the above view, prudence suggests that the computer search will be futile unless the entire system is seized and removed, so that the contents can be examined at leisure. For instance, on 18 July 2008 four Tanzanian Police Force detectives searched the offices of the *MwanaHalisi* newspaper in Kinondoni, Dar es Salaam, and took away a computer containing editorial inputs which was being used by the paper's managing editor, one Saed Kubenea. It was later revealed to journalists by the Director of Criminal investigations, Robert Manumba, that Kubenea was suspected of colluding with an employee of NBC bank, Peter Msaki, to reveal confidential information regarding the bank's customers.[103] It is worth noting that Silverglate and Viles[104] rightly argued that to seize an entire system for the sake of a couple of documents contained therein is inefficient, overly intrusive and potentially disastrous for the owner of the system. They suggest that a better course would be to have agents sophisticated in the use of computer equipment search the system on-site, and to copy onto a disk the documents which motivated the application for a warrant in the first place.

[103] Media Watch, July 2008 'Activists up in arms as police swoop on newspaper '. Available at mct.or.tz/PDFFILES (Accessed 20 June 2013).
[104] Silverglate, AH & Viles, CT 1991.' Constitutional, legal and ethical considerations for dealing with electronic files in the age of cyberspace', paper presented at the 1991 Federal Enforcement Conference, Georgetown University Law Center, Washington DC May 16–17.

4.1.2 Search and seizure in South Africa

In South Africa a police officer may search on authority of a search warrant. A police officer may also search (without a warrant) any person, container or premises for the purposes of seizing an article referred to in s 20, if the person or occupier consents to the search.[105] Moreover, a police officer, in terms of s 22(b) of the Criminal Procedure Act, may search a person, container or premises for an article referred to in s 20, if he believes on reasonable grounds that a search warrant will be issued to him if he applied for one and that the delay in obtaining the warrant would defeat the object of the search. The context in which the word 'premises' is used implies physical structures or items. However, for the purposes of drawing comparisons with Tanzania in respect of a search of the premises, the lack of recognition of intangible data as an object of search and seizure is problematic. By contrast, in South Africa the ECT Act has taken the concepts *premises* and *articles* to include information systems and data messages. Moreover, the ECT Act, under the provisions of s 82(3), incorporates the relevant clauses of the Criminal Procedure Act by reference, with the provision for necessary changes to keep the two Acts compatible. The two Acts are therefore designed to be used in conjunction with one another.[106] Furthermore, in terms of s 82(1) of the Act, unlike in Tanzania, the law has created 'cyber-inspectors' who, with the authority of a warrant, may search any premises or information systems if there is reasonable cause to believe that the articles/documents/records have a bearing on an investigation. However, it has been argued that the regulation of cyber-inspectors in practice does not work as well as expected and that very few of them have been appointed since the inception on the Act. Further criticism, according to Collier, is to the effect that their appointments to assist the police, who are actually the persons that should investigate cybercrime, is an unwarranted extension of the powers of the Department of Communications.[107]

---

[105] Section 21 of Act 51 of 1977.
[106] Van der Merwe, DP (2008), 'Criminal law' in Dana van der Merwe *et al Information and communications technology law* 82–83.
[107] Buys & Cronje op cit note 4 at 335–336.

4.3 Regional initiatives to combat cybercrime in Africa

The creation of an enabling legal and regulatory environment was identified as a critical factor for the effective implementation of e-Government and e-Commerce strategies at national and regional levels. Against this background, strong back-up support is needed in terms of legislation related to data security, network security, cybercrime, information systems and electronic transactions.[108]

On the other hand, in the quest to understand in depth the policy and regulatory frameworks, it is important to revisit various regional initiatives that have been taken by the African continent to combat cybercrime.

In September 2012 a draft convention on cybercrime was approved by the Fourth African Union Conference of Ministers Responsible for ICT. The objectives of the draft convention are to harmonise legislation relating to e-transactions development, personal data protection, cyber-security promotion and the fight against cybercrime. It is envisaged that the convention will be in force by 2014. Furthermore, it may be observed that the AU Commission is working in collaboration with regional economic communities for harmonisation of legislation for the Eastern, Southern and North African Unions.

For its part, the Southern African Development Community (SADC) and ITU in 2012 ran a regional initiative aimed at harmonising the legal frameworks for southern Africa, in particular those relating to electronic transactions, protection of personal data and cybercrime. It is important at this juncture to note that in 2013 the SADC finally managed to adopt its Model Law on Computer Crime and Cyber-crime.[109] This model law establishes the basic principle of non-discrimination between media, or media neutrality. Key provisions of the model are drafted to establish equivalence between paper documents and electronic messages. It also includes consideration of e-transactions, e-signatures and data protection and privacy.[110]

---

[108]United Nations Conference on Trade and Development (UNCTAD), 2012, Harmonizing cyber laws and regulations: the experience of the East African Community. Available at *unctad.org/en/PublicationsLibrary/dtlstict2012d4*, accessed on 17 June 2013.

[109] International Telecommunication Union (ITU), 2013 'Computer crime and cyber-crime:' South African Development Community (SADC) Model Law. Available at *http://www.itu.int/en/ITU-D/Cybersecurity*, accessed on 17 June 2013.

[110] Ibid.

In the East African Community Development strategy for 2006–2010, cyber-laws and e-justice were identified as key cross-cutting issues that need to be in place for successful implementation of e-government applications and the development of e-commerce in the region. Against this background, the United Nations Conference on Trade and Development (UNCTAD) and the East African Community (EAC) task force on cyber-laws have been working together to formulate legal frameworks for e-commerce. In 2009 the EAC became the first region in Africa to adopt a modern and effective regional harmonised framework for cyber-laws.[111]

Another remarkable initiative is that of the Economic Community of West African States (ECOWAS), which in April 2012 passed a resolution to establish a convention on cybercrime for the Region. A three-day regional workshop organised by the Economic and Financial Commission (EFCC) of Nigeria, and the Australian Federal Police (AFP) deliberated on the need for practical co-operation among West African countries in terms of policing and intelligence-gathering on cybercrime-related issues and other organised crimes. The conference also called upon on law-enforcement agencies in the region to come together and devise policies for tackling the issue of cybercrime.[112]

4.4 Conclusion and recommendations

4.4.1 Recommendations

This work has been an enquiry into the efficiency of the Tanzanian legal and regulatory framework to combat cybercrimes. Its central proposition has been that the current legal and regulatory framework within which ICT operates does not sufficiently provide for the criminalisation of cybercrimes in Tanzania because they were developed in a physical world with much focus on tangible objects. In chapter two, the work has analysed the current NICTP development and its implementation. Several weaknesses were identified, including legal framework limitations. In order to correct the situation, the policy review process undertaken by the government has to consider changes in technology, new national and regional developments

[111]United Nations Conference on Trade and Development (UNCTAD), 2012 op cit note 108.
[112]Nigerian Tribune: 'ECOWAS and the Need for a Convention on Cyber-crime', 18 June 2012. Available at *tribune.com.ng/...42673,* accessed on 16 June 2013.

and recognise the evolving of new acts and policies. A good policy with its implementation strategies and institutional framework has the potential for making ICT an effective tool in achieving countries development goals. For an effective policy review process it is recommended that:

(a) The review of the NICTP should involve stakeholders emphasizing a multi-stakeholder participatory approach involving key ministries.

(b) The development of a Policy vision and mission statement to address universal access and infrastructural developments and sharing with key role players.

(c) The policy has to appreciate such other laws and regulations, such as those governing cyber-usage, e-transactions, confidentiality and privacy.

In chapter three, different types of cybercrime incidents in Tanzania were examined and compared with incidents in South Africa. It was observed that new types of crime have surfaced and existing crimes are now perpetrated through means of sophisticated technology. It was also observed that the existing laws and procedures are generally insufficient to criminalise all forms of cybercrimes and the lack of recognition of intangible data as an object under the criminal law and procedure is a problematic issue. Brenner rightly suggests that countries should evaluate their procedural law governing collection and analysis of evidence to include intangible evidence derived from cybercrimes as opposed to traditional crimes which generate tangible evidence.[113] It is apparent, as in many countries, that intervention by the legislator in Tanzania is necessary to address cybercrimes and related procedural and evidentiary matters. Maghaireh rightly suggested that the legislators[114] enact cyber legislation defining the following actions as crimes:

- accessing the whole or any part of a computer system without authorisation by infringing security measures;
- damaging, deleting or altering computer data without authorisation;

[113] Brenner, SW (2001), 'Cybercrime investigation and prosecution: the role of penal and procedural law' 8 *Murdoch University Electronic Journal* 2. Available at <http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82_text.html, accessed on 3 September 2013.

[114] Alaeldin Maghaireh, op cit at 99.

- seriously hindering without authorisation the functioning of a computer system by inputting, transmitting, damaging, deleting, altering, or suppressing computer data;
- inputting, altering, or suppressing computer data;
- inputting, altering and deleting data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic;
- offering or making available child pornography through a computer system; distributing or transmitting child pornography through a computer system; producing child pornography for a purpose of distribution through a computer system; and
- transmitting any communication containing a threat to injure or harass people.

Promulgating a law to criminalise certain acts is only part of the solution; the other part is creating legal awareness of ICT on the part of the lawyers, magistrates, judges and law-enforcers. Furthermore, the need to educate the public cannot be overemphasised. More efforts must be made by the LRCT to educate the citizens on the dangers of cybercrimes. For instance, as observed earlier, citizens should be educated on the safekeeping and secrecy of passwords for the sake of securing their data.

Chapter four has shown that the Tanzanian Criminal Procedure Act allows law enforcement officers to seize visible and tangible objects and specifies that the subject of the search warrant is either a physical place or an individual. It is suggested that the CPA should be amended to explicitly permit the search and seizure of intangible materials. This can be done by amendment of s 39 of the CPA by expanding the meaning of things connected to search to include the word ‘data’.

4.4.2 Closing comments

In a jurisdiction such as Tanzania, where most statutes have not been brought in line with current trends in cybercrime, it is apparent that intervention by Parliament is necessary. The author recommends the urgent enactment of Tanzanian domestic legislation on electronic transactions that would incorporate provisions necessary for combating cybercrime and eliminate the currently legal barriers. The author also hopes that this mini-dissertation will shed light on the ongoing efforts by the Tanzanian government to enact a comprehensive cybercrime law and enhance cybercrime investigation and electronic evidence. Also the author believes that the research will pave the way for more research in the area of cybercrime in Tanzania.

APPENDIX I

Figure 1: Manufactured fake ATM cards that were found in the possession of the suspects. According to the statement released by Mwanza police force,[115] the suspects were found with 194 National Microfinance Bank (NMB) and Diamond Trust Bank ATM cards, 36 Kenya Commercial Bank (KCB) ATM cards and another 18 cards with no logo.

Source: Mwanza Region Police Force press release.

[115] Briefing to the press by the Acting Mwanza Regional Police Commander Christopher Fuime, dated 14 February 2013.

Figure 2: Equipment allegedly used by the suspects to manufacture fake ATM cards. They were also found in possession of a camera as well as three cans of spray paint which they used to 'blind' the banks' CCTV cameras in order to conceal their identity.

Source: Mwanza Region Police Force press release.

APPENDIX II

The suspects were arraigned on 20 February 2013 before the Mwanza Resident Magistrate's court and charged with traditional common law offences of forgery contrary to ss 333, 335 (a) and 338 of the Penal Code and stealing contrary to ss 258 (1) and 265 of the Penal Code, as shown in the attached charge sheet from Mwanza Resident Magistrate's court in Tanzania.

IN THE RESIDENT MAGISTRATE'S COURT OF MWANZA

AT MWANZA

CRIMINAL CASE NO 19 OF 2013

REPUBLIC

VERSUS

1. MANIKI S/O KIMANI @ KIM

2. SALIM S/O NASSORO @ MWENKELLEY

3. LEONARD S/O MASUNGA

4. AYOUB S/O JACKSON @ JOSEPH

CHARGE

1ST COUNT

STATEMENT OF OFFENCE

FORGERY; Contrary to Sections **333, 335(a)** and **338** of the Penal Code, {Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** on divers dates between **August, 2012** and **09th February, 2013** within City and Region of Mwanza, jointly and together, with intent to defraud the National Microfinance Bank Limited (NMB), forged 95 Automatic Teller

Machine (ATM) Cards all bearing number **0225152975** purporting to be of one **MOLLEL, L. P.** a holder of Bank Account Number **2258103695** maintained by the **National Microfinance Bank Limited.**

2ND COUNT

STATEMENT OF OFFENCE

FORGERY; Contrary to Sections **333, 335(a)** and **338** of the Penal Code, {Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** on divers dates between **August, 2012** and **09th February, 2013** within City and Region of Mwanza, jointly and together, with intent to defraud the National Microfinance Bank Limited (NMB), forged 99 Automatic Teller Machine (ATM) Cards all bearing number **0506056317** purporting to be of one **MUNUO, Z. E.** a holder of Bank Account Number **5068000322** maintained by the National Microfinance Bank Limited.

3RDCOUNT

STATEMENT OF OFFENCE

STEALING: Contrary to Sections **258(1)** and **265** of the Penal Code, [Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** on divers dates between **August, 2012** and **09th February, 2013** within City and Region of Mwanza, jointly and together, stole money the sum of Tanzanian Shillings **Seventy one million one hundred eighty nine thousand and five hundred only (TShs. 71,189,500/=),** the property of the National Microfinance Bank Limited.

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** between **27th January and 5th February, 2013** within the City Region of Mwanza, jointly and together, stole money the sum of Tanzanian Shillings **Two million and Six hundred thousand only (TShs. 2,600,000/=)**, from Account No. **31101611026** of **MITINJE NANGALE KITENGE,** the property of the National Microfinance Bank Limited.

21ST COUNT

STATEMENT OF OFFENCE

STEALING: Contrary to Sections **258(1)** and **265** of the Penal Code, [Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** between **31st August,** and **5th September, 2012** within the City and Region of Mwanza, jointly and together, stole money the sum of Tanzanian Shillings **Four million eleven thousand eight hundred and ninety only (TShs. 4,011,890/=),** from Account No. **61901609060** of **DAMSON ELIAS MKUMBO,** the property of the National Microfinance Bank Limited.

22ND COUNT

STATEMENT OF OFFENCE

STEALING: Contrary to Sections **258(1)** and **265** of the Penal Code, [Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** between **30th January** and **2nd February, 2013** within the City and Region of Mwanza, jointly and together, stole money the sum of Tanzanian Shillings Three million seven hundred thousand only **(TShs. 3,700,000/=)**, from Account No. **31102503105** of **CONFIRMATA GABRIEL MAPUNDA**, the property of the National Microfinance Bank Limited.

23RD COUNT

STATEMENT OF OFFENCE

STEALING: Contrary to Sections **258(1)** and **265** of the Penal Code, [Cap. 16 R. E. 2002].

PARTICULARS OF OFFENCE

MANIKI S/O KIMANI @ KIM, SALIM S/O NASSORO @ MWENKELLEY, LEONARD S/O MASUNGA and **AYOUB S/O JACKSON @ JOSEPH,** between 21st December, 2012 and 08th January, 2013 within the City and Region of Mwanza, jointly and together, stole money the sum of Tanzanian Shillings **Four million and four hundred thousand only (TShs. 4,400,000/=)**, from Account No. **31102500134** of **METHUSELA ENOKA**, the property of the National Microfinance Bank Limited.

DATED at **MWANZA** this 20th day of February 2013

Marungu P.J.

STATE ATTORNEY

BIBLIOGRAPHY

Books and reports

Buys, Reinhardt (ed) *Cyber law @ SA II: the law of the internet in South Africa* 2ed (2004) Van Schaik, Pretoria .

Credo, Paul W & Michels, Jean-Pier *Computer crime in South Africa* 2 ed (1985) Aiken & Carter, South Africa.

Cyber Security in Tanzania: Report From the Cyber-Security Mini-Conference, Centre for ICT Research and Innovations, Institute of Finance Management, Dar es Salaam (2012).

Dagada, R (2013) 'Digital banking security, risk and credibility concerns in South Africa' in *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic*.

Law Reform Commission of Tanzania 'Report of the comprehensive review of the civil justice system in Tanzania' presented to the Minister for Justice and Constitutional Affairs May 2013.

Manacorda, S *Cyber-criminality: finding a balance between freedom and security* (2012) International Scientific and Professional Advisory Council

Ministry of Women and Child Development, Government of India 'A study on child abuse: India 2007' (2007).

Snyman, CR *Criminal law* 4 ed (2002).

Sylvia, Papadopoulos & Snail, Sizwe (eds), *Cyber law @ SA III: the law of the Internet in South Africa* 3ed (2012) Van Schaik, Pretoria.

Tanzania Mainland's 50 Years of Independence: a review of the role and functions of the Bank of Tanzania, 1961–2011 (June 2011).

United Nations Conference on Trade and Development (UNCTAD) *Harmonizing cyber laws and regulations: the experience of the East African Community* (2012)

Van der Merwe DP *Computers and the Law* 2 ed (2000) Juta, Kenwyn.

Van der Merwe D (ed) *Information and communication technology law* (2008) Lexis Nexis, Cape Town.

Journal Articles

Brenner, S, Frederiksen, B 'Computer searches and seizures: some unsolved issues' (2001/2002) *Michigan Telecommunication and Technology Law Review*.

Gordon, S & Ford, R. 'On the definition and classification of cyber crime' (2006) *Journal in Computer Virology*.

Mathew, LA 'Online child safety from sexual abuse in India' (2009) 1 *Journal of Information, Law & Technology*.

South African cases

S v Motata (Unreported case no. 63/968/07, Johannesburg district court.

Motata v Nair NO 2009 (2) SA 575 (T).

Tanzanian Legislation

Communications (Consumer Protection) Regulations of 2005.
Electronic and Postal Communications Act 3 of 2010.
Law of Marriage Act Cap. 29[RE 2002].
Sexual Offences Special Provisions Act 4 of 1998.
Tanzanian Penal Code Cap 16 [RE 2002].
United Republic of Tanzania Constitution, 1977 as amended.

South African Legislation

Republic of South Africa Constitution of 1996.
Criminal Procedure Act 51 of 1977.
Electronic Communications and Transactions Act 25 of 2002.
Films and Publications Act 65 of 1996.
Protection of Personal Information Act 4 of 2013.

South African Bills

Electronic Communications and Transactions (ECT) Amendments Bill, 2012