Mtafiti Mwafrika

(African Researcher)

The Case for an African Solution to Cybercrime

A Critical Assessment of the African Union Convention on Security in Cyberspace and Personal Data Protection

Rene Nkongho Eno-Akpa

Center for African Studies
School of Postgraduate Studies and Research
Uganda Martyrs University

Monograph Series
Number 31, 2016

Mtafiti Mwafrika (African Researcher) is a peer-reviewed monograph series of the Center for African Studies (CAS) at Uganda Martyrs University. The series is intended to offer a platform where those interested in African issues can express and exchange their ideas, and contribute towards a better knowledge and understanding of the African reality. The opinions expressed in the series are not necessarily those of CAS. Contributions to the series can be sent to the Editor and those deemed to be appropriate will be published in subsequent issues.

Address questions and comments to:

The Editor
Mtafiti Mwafrika
Center for African Studies
School of Postgraduate Studies and Research: +256-382-410611
E-mail: cas@umu.ac.ug

This issue was edited by Jimmy Spire Ssentongo, PhD. It was reviewed by Joseph Kikonyogo (PhD) and Edward Kafeero (PhD).

Published by the Center for African Studies (CAS)

ISSN 1607-0011

The cover image is from
https://www.newshosting.com/blog/internet-security-defending-your-data-from-cybercrime/

Printed at Marianum Press Limited, P.O. Box 11, KISUBI

About the Author

Rene Nkongho Eno-Akpa is a Winner of the 2012 Open Society Foundation Award for the MA (Public Policy Fellowship) at Central European University and he is specialised in International Public Policy. He also holds an MA in International Relations and Diplomatic Studies of Makerere University, Kampala Uganda. Prior to joining Uganda Martyrs University in 2014 as a Research Fellow in Governance and Development, Rene was the 2013 International Google Policy Research Fellow at the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University Law School, Kenya. During his policy research fellowship at CIPIT, Rene served as the Lead Researcher with a CIPIT outreach project, *Mobilising for Digital Freedom through the AU Convention on Cybersecurity: The voice of private stakeholder actors.* Rene has taught *Internet Law and Governance* and presented at several academic forums.

Table of Contents

List of Abbreviations

ABBREVIATION	MEANING
AUCSCPDP	Africa, the African Union Convention on Security in Cyberspace and Personal Data Protection
ACHPR	African Commission on Human and Peoples' Rights
AU	African Union
CERTs	Computer Emergency Response Teams
CoECC	Council of Europe Convention on Cybercrime
CoE	Council of Europe
COMESA	Common Market for Eastern and Southern Africa
CSIRTs	Computer Security Incidence Response Teams
DAUCCSC	Draft of African Union Convention on the Confidence and Security in Cyberspace
ECOWAS	Economic Community of West African States
EU	European Union
ICT	Information and Communications Technology

ICB4PAC	Capacity Building and ICT Policy Legislative Frameworks Support for Pacific Island Countries
ITU	International Telecommunications Union
MLAT	Mutual Legal Assistance Treaties
OECD	Organization for Economic Co-operation and Development
RAT	Routine Activity Theory
SLT	Social Learning Theory
STT	Space Transition Theory
UNHRC	United Nations Human Rights Committee
UNODC	United Nations Office of Drug and Crime

The Case for an African Solution to Cybercrime: A Critical Assessment of the African Union Convention on Security in Cyberspace and Personal Data Protection

Abstract

Currently, Africa hosts 4 of 10 countries with the highest cybercrime levels in the world. To augment the inadequacy of municipal cyber legislations in Africa, the 'African Union Convention on Security in Cyberspace and Personal Data Protection' (AUCSCPDP) was signed in July 27, 2014 in Malabo, Equatorial Guinea. Basing on documentary reviews, surveillance of media coverage and observations on cybersecurity initiatives across the globe, this critical assessment concludes that the AUCSCPDP is the most comprehensive continent-wide cybersecurity convention. Unlike the Council of Europe Convention on Cybercrime (CoECC, 2001), benchmarked herein, the AUCSCPDP attunes to Africa's context, prohibiting identity flexibility and associative anonymity in ecommerce; outlawing spam; addressing the use of encryption in cybercrime; prohibiting key forms of online discrimination, which all currently constitute Africa's biggest vulnerability in cyber space.

The AUCSCPDP provision for independent expert vulnerability testing of Internet service introduces an essential process through which Africa's ICT development will proactively incorporate online security measures. However, the provisions permitting non-consensual interference with private, personal and sensitive data, the interference with online traffic or content data, and the issuance of search and seizure warrants permit inappropriate and broad ongoing investigation mandates to judges will inadvertently undermine values that the AUCSCPDP is seeking to protect such as rights to privacy and freedom of expression. The provisions covering aggravation and corporate liability are crafted, albeit inadvertently, in ways that will impose unjustified legal burdens on individuals and corporations. By not providing for a model cyber law, by precluding provisions on jurisdiction and avoiding a continent-wide Computer Emergency Response Team, the feasibility of AUCSCPDP will prove difficult to harmonise municipal cyber laws and will hinder international cybercrime cooperation within Africa. This critical assessment

ends by providing options that could fine tune the AUCSCPDP to accomplish the values, objectives and purpose for which it is sought.

Key Words: African Union, Cybersecurity, African Internet Governance, and "Online legislative overkill".

Introduction

Over the past 50 years, the trend towards digitalisation is omnipresent in all modern services, employing the computer and internet connectivity in applications such as e-government, e-commerce, e-learning to avail efficient and effective service delivery and to aid societal development. This trend is especially evident in developing countries of Africa. Of an estimated 2.3 billion internet users globally by 2011, developing nations account for 60% of online users (UNODC, 2013), with users in such areas using high speed 3G+ mobile network services and handheld devices (smart phones, tablet computers) to offer or render public / private information, provide service and initiate actions relating to all aspects of wellbeing.

In the context of user anonymity and automated services online (ITU, 2012), this trend in cyberspace has blurred territorial borders (Rosenzweig, 2012), exposing individuals and societies to acts that violate privacy, fundamental freedoms (e.g., of expression, of access to information), confidentiality, integrity and availability of computer data or systems (Chertoff, 2008; UNODC, 2013; ITU, 2012; Rosenzweig, 2012 & Ilie et. al. 2011). Such acts manifest the threat of cybercrime in this age of information society. While this digitalising trend has had impacts on municipal laws orienting states towards 'resovereingnisation' (Rosenzwig, 2012: 406) through national legislations on cyberspace, the dawning reality that the offender might have acted from country A, used an Internet service in country B, where the victim is based in country C, makes cybercrime a

transnational, multi-stakeholder affair. Regulation via national cybercrime legislation is insufficient – a globally oriented comprehensive national policy or strategy would be a critical component of a continent-wide Internet governance action.

The transnational dimension of cybercrime and the need for a globally harmonised strategy to promote confidence in cyberspace is captured in, for instance, analyses from the Online-Community HackerWatch[1]. HackerWatch reported that in August of 2007, attempts to illegally access computer systems amounted to 250 million incidents worldwide. Analysts generally agree that the lack of harmonised legislation among states is a breeding condition for cybercrime (UNODC, 2013; Ilie et. al. 2011). This lack of harmonious legislative mechanism leads to unprotected or inadequately protected computer systems, the development of software tools that automate transnational cyber attacks and the rise in ownership of anonymous online devices (Rosensweig, 2012) by complex but organised groups of online offenders (ITU, 2012). Such organised online offenders account for illegal accesses or attempts to access computers / computer systems, illegal interference with computer systems, production/storing/disseminating of unlawful online content, and illegal violations of computer data, personal data and sensitive data (UNODC, 2013). It implies that these cybercrimes[2] necessitate both binding[3] and non-binding[4]

[1] HackerWatch offers a unique kind of Internet reconnaissance It collects and analyses users' firewall activity, to identify intrusion attempts, track complex attack patterns, and disclose the sources and targets of Internet threats. See http://www.hackerwatch.org/.

[2] Countries report widespread criminalisation of the 14 cybercrime acts: Illegal access, Illegal interception and illegal interference into computer data, breach of privacy, fraud/ forgery and online identity offences, copyright/ trademark offences, initiating, using or disseminating spam, racism/xenophobic content and child pornographic content online, soliciting or grooming other persons (especially children) into illegal acts and orchestrating or supporting acts of terrorism online (UNODC, 2012).

regional and global strategies to combat their cause and adverse effects. The Information and Communications Capacity Building for Pacific Island Countries (ICB4PAC) Model Policy[5] for Cybercrime reflects the need for a comprehensive, global approach to ensure guaranteed confidence in cyberspace by asserting that;

> Addressing the multi-dimensional challenges of fighting cybercrime requires a comprehensive approach that should include overall policies, legislation, education and awareness raising, capacity building, research as well as technical approaches.

As a rule of thumb, cybersecurity can never be guaranteed solely by introducing national legislation; it must involve various

---

[3] Some Binding instruments include: Council of Europe Convention on Cybercrime (2001) and Additional Protocol on Xenophobia and racism (2003); Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007); EU legislation including on e-Commerce (2000/31/EC), on Combating Fraud and Counterfeiting of Non-Cash Means of Payment (2001/413/JHA), on Personal Data (2002/58/EC as amended), on Attacks against Information Systems (2005/222/JHA and Proposal COM(2010) 517 final), and on Child Pornography (2011/92/EU); Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime (2009) (Draft) African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2013)

[4] Some non-binding instruments include: Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002); International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010); Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011); Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime(2012)

[5] This is the result of the ITU and EU cofounded project in the Pacific Island Countries covering substantive criminal law, procedural law, international cooperation, liability of Internet Service Providers, Electronic Evidence and Crime prevention measures opened for signature in Samoa in August 2011. Available at www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html

strategies in a comprehensive policy (ITU, 2012; Brechbuhl et. al., 2010). This explains the aforementioned quote of the preamble to ICB4PAC Draft Model Policy for Cybercrime. Countries that merely introduce cybercrime legislation without having developed an anti-cybercrime strategy will likely face insurmountable challenges in their pursuit for confidence in cyber space (Brechbuhl et. al., 2010). While more than two-thirds of countries in Europe (mostly, signatories to the Council of Europe Convention on Cybercrime, 2001) report sufficient legislation (substantive and procedural), technical capacity, sufficient organisational structure and various means of international cooperation to deal with cybercrime, the picture is reversed in Africa, the Latin America, Asia and Oceania. In Africa, more than two-thirds of countries view their existing cyber laws and other measures as only partly sufficient, or not sufficient for cybersecurity (UNODC, 2013). This implies that more appropriate legal measures (harmonised across Africa)[6] are essential but must be envisaged and used as a crown on other non-legal continent-wide internet governance measures and structures, which are necessary for halting the growth of cyber crime in Africa.

Cybercrime is growing faster in Africa than any other continent (Yankey, 2013). This is because online participation (in the form of new users and increased usage by existing users) in Africa is increasing faster than in any other continent, presenting new unsuspecting targets for cyber offenses and incorporating new actors of cybercrime. New online participants are, increasingly, using online social networks (such as Mxit developed in South Africa) and e-commerce (such as Mpesa mobile money transfer, which accounts for 70% of financial transactions in Kenya) in

[6] There is need to make sure that such harmonization must be done with appropriate consideration of local context, as various countries have various resources and needs. So the harmonisation does not mean "equal" or "singular" in implementation, even if it might mean this in policy.

the context of insufficient legislation, inadequate technical measures and a lack of training and capacity building to curb ICT abuse by cyber crooks (Yankey, 2013). As a result, the scope of cybercrime in Africa harbours issues such as botnet attacks, phishing, and spam that were not as important when the most widely used and recommended conventions (notably, The Council of Europe Convention, 2001[7]) were passed (ITU, 2012). These reasons help explain why Africa habours four (Nigeria, Cameroon, Ghana and South Africa) of 10 countries with the highest levels of cybercrime in the world (Yankey, 2013).

Against this background, the first African regional forum on cybersecurity held in Yamousoukro (November 2008), charted a way forward including, *inter alia*, an extraordinary conference of African Union Ministers in charge of communication and information technologies (Johannesburg, 2009).[8] The conference resolved that the AU and the UN Economic commission for Africa should develop a legal framework to guide electronic transactions, data protection, and cyber security in Africa. Building on this resolution, an expert group composed by the AU produced an earlier, January 2014 draft *AU Convention on the Confidence and Security in Cyberspace* (DAUCCSC)[9] that was endorsed by the 4th Ministerial Conference of the African Union ministers in charge of communication and information technologies in the Khartoum Declaration of September 2012. In response to protests and online petitions against DAUCCSC from the private sector across Africa, the expert group revised

[7] It is the first international convention on cybercrime whose membership has transcended Europe as a continent. By September, 2013, forty states had ratified it including states out of the Europe such as the USA, Dominican Republic, Australia and Japan. Additionally, eleven states have signed it including Canada and South Africa.

[8] See the Oliver Tambo Declaration, Johannesburg 2009, available at www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf

[9] The earlier draft of the DAUCCSC was produced in January 2013 and it is available on the website www.AU.int

the DAUCCSC, coming up with the *African Union Convention on Security in Cyberspace and Personal Data Protection (AUCSCPDP)* in May 14, 2014[10]. The AUCSCPDP was adopted in Addis Ababa in May 15, 2014 by ministers of justice of all AU member countries and was signed on July 27, 2014, in Malabo at the 23rd Ordinary Session AU summit by the Heads of States of AU member countries. In a bid to critically assess the AUCSCPDP, this paper uses documentary reviews, surveillance of media coverage, and observations on global cyber security to address the following seemingly inescapable questions:

1. What values does the AUCSCPDP seek to secure in this age of the information society? Do these resonate with actual cyber threats and manifestations of cybercrime in Africa?

2. To what extent is the AUCSCPDP apt with regard to the substantive and procedural legal provisions against cybercrime in this age of an information society?

3. How feasible is the AUCSCPDP in the current African context with regard to international co-operation measures, technical measures (e.g. Computer Emergency Response Teams [CERTs]), Human Capacity building (e.g. of prosecutors) and multi-stakeholder cooperation devoted to cybersecurity?

Part One of this paper explores the technical and socioeconomic causes underpinning cyber offences and the observations on, or manifestations of, cybercrime in Africa. Such context will be the basis to examine whether the values, which the AUCSCPDP highlights, are under threat from manifestations of cybercrime in Africa.

[10] The AUCSCPDP is accessible on https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf

The values which undergird the AUCSCPDP include the following: security of digital property and cultural heritage of individuals, organizations and nations; the survival and sovereignty of states; authentic online content; individual rights and freedoms in cyberspace and a controllable multidisciplinary cyber security strategy.[11]

Part One concludes by articulating the degree to which the AUCSCPDP resonates with the Global Cyber Security Agenda.

Part Two of this review assesses the strengths and limitations of the substantive and procedural provisions of the AUCSCPDP on cybersecurity, by bench-marking the CoECC, which is widely used and highly recommended for developing countries by international organisations of global supranational nature such as the International Telecommunications Union (ITU) and the United Nations Office for Drug and Crime (UNODC).

Finally, in **Part Three** we explore the feasibility of the AUCSCPDP in Africa's context with regard to international co-operation measures, technical measures (e.g. CERTs), human capacity building (e.g. of prosecutors), and multi-stakeholder cooperation devoted to cybersecurity.

[11] For more about the values for which the AUCSCPDP was sought, read the preamble of the AUCSCPDP, the *Oliver Tambo (*Johannesberg) *Declaration* adopted in a conference by African Ministers in charge of Information and Communication Technologies in 2009; the Addis Ababa *Declaration on Information and Communication Technologies in Africa: Challenges and Prospects for Development*, which was adopted the Assemble of heads of State and Governments in 2010; the *Abidjan Declaration* (February, 2012) and the *Addis Ababa Declaration on the Harmonisation of cyber legislation in Africa* of June, 2012.

PART ONE

The Evolution and Scope of Cybercrime in Africa: A Theoretical and Conceptual Basis

From the 1960s, cybercrime has evolved from offences against the confidentiality, integrity and availability of computer data and systems through computer-related offences and content-related offences to, more recently, copyright related offences (ITU, 2012). Technical, social and economic factors determine the evolution and spread of cybercrime, informing the substantial and procedural scope, as well as other strategic or policy orientations that any cybercrime legislation should contain.

Technical developments such as the replacement of vacuum-tube-based computer systems with transistor-based computer systems in the 1960s led to increased use of computers and the first cybercrime offences - that being unlawful access to computer databases and intrusions on privacy (ITU, 2012). In the 1970s, the use of computer systems and computerised data increased, as did further illegal interference with computer systems and illegal manipulation of electronic data (ITU, 2012). By the 1980s, increases in the production and usage of computer devices and computer systems led to an increase in software privacy and patent-related crimes. Subsequently, greater interconnection of computer systems (networks) occasioned the introduction of computer viruses through automated malicious software (ITU, 2012). By the 1990s, the introduction of the World Wide Web and growing Internet usage caused certain content (especially child pornography) to transcend national boundaries, becoming available to users in countries where it is criminalised. In the first decade of the 21st century, the nature of cybercrime evolved again to include the use of encryption to hide online identity and to hide crimes related to illegal content.

Additionally, the increase in complex online programming ("cloud computing,[12]") and automated software attacks led to new crimes such as hacktivism, data espionage, "phishing,[13]" spamming,[14] Denial of Service (DoS) attacks, violations of copyright, and "botnet attacks,[15]" all of which combine to make cybercrime investigations particularly complex (ITU, 2012).

On the one hand, knowing these technical developments is crucial for legislation relating to criminalising access, interference and manipulation relating to computer data and computer systems. Such knowledge feeds the need for up-to-date technologies and cyber forensic tools in the procedural provisions of national or international legislations on cybercrime. These technical developments also explain the estimate that 80% of cybercrime originate from organised activity that is established around malware creation and botnet management. With botnet management, personal and financial data that is available online are harvested for abuse or to be sold out to other online criminals in a social network (UNDOC, 2013). On the other hand, the advancement and technical developments have themselves led to social network services

[12] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[13] These are acts that are carried out online to persuade a potential victim to disclose personal or secret information.

[14]Bulk sending of unsolicited e-mails. The OECD (2005) reported that developing countries suffer more from the impact of spam (constituting between 85 to 90% of email is spam because spam filtering technologies are inadequate, the bandwidth and Internet access are scarcer and more expensive than in developed countries.

[15] A group of unprotected computers into which automated software are remotely installed making possible for these unprotected computers to be remotely controlled to get personal details related to identity or financial details, such as bank accounts in order to commit forgery and fraud.

online that constitute and support some social causes of cybercrime.

From a social perspective, Kigerl (2012) proposes the **Routine Activity Theory (RAT)** to explain the cause and spread of cybercrime. He explains cybercrime as the convergence of three major factors. The first factor is the existence of a motivated offender. The second factor is the spotting of a suitable target victim prone to phishing or fraud, which victim may include persons in online services such as banking, shopping, file sharing (drop box), as well as in social networks (Facebook, Twitter). The last factor Kigerl (2012) proposes as precipitating cybercrime is the absence of a capable guardian, for example, the absence of anti-virus programs on computers and/or the absence of deterrent penal measures. The RAT is important in that it helps us to understand that the cause and spread of cybercrime is complex and multifaceted. That is to say, even if legislation were in place, RAT highlights the need for technical measures (CERTs, CSIRTs) to serve as one capable guard. It underscores the need for education and training of potential victims on the use of online resources. RAT also implies that a broad range of stakeholders, which includes government (to effect legislation), academia (to educate and train human resources and build capacity for investigations/prosecution of cybercrime), internet service providers (such as Google, Facebook), and business corporations (e.g. banks), need to co-operate or network in order to implement an effective and holistic strategy to promote confidence in cyber space. The idea of multi-stakeholder networking is deemed crucial for cyber security policy (Brechbuhl et. al., 2010). What the RAT fails to explain is the underlying motivation of the offender and the experience of cybercrime as transnational and global phenomena.

Jaishankar (2011) is relevant in explaining technical factors that influence individual motivation to cybercrime in his **Space**

Transition Theory (STT). Reasserting that the lack of deterrence factors (particularly, legislation and penalties) underpin the motivation into cybercrime, he also points to the idea that current Internet services guarantee identity flexibility and dissociative anonymity online, and thereby motivate the criminal state of mind that actualizes cybercrime. Therefore, Jaishankar (2011) is relevant in providing the basis on which some conventions of cybercrime, including the AUCSCPDP, curtail online anonymity with regard to e-commerce (See, e.g., Art 2 to Art 4 of the AUCSCPDP). Also, the STT explains why personal data may occasionally be retrieved, processed, and stored without consent. For example, basing on informed advice from a national protection authority, personal data can be processed by public institutions, a private law cooperate body operating a public service, or a local community for online acts that affect public interest and state security (Art 10(5), AUCSCPDP). This theory ignores that, in this age of an information-based society, online anonymity is critically necessary for unhindered supply, access and flow of information on sensitive socio-political issues (ITU, 2012; Chertoff, 2008). Building on SST to provide a solution for cybercrime, the need for harsh penalties for cybercrime can be easily justified but the second solution of limiting online anonymity as a measure to curb cybercrime is increasingly contentious. Indeed, in an information society, the second STT solution to cybercrime results in national legislations or international conventions that risk violating the basic rights of privacy and/or freedom of expression.

Similarly, some social motivation behind the spread of cybercrime that is relevant to Africa has been put forward by Skinner and Fream (1997) in their **Social Learning Theory (SLT)**. The SLT postulates that cyber criminal behaviour is learned through a process of interaction, usually in primary groups. The social motivation behind the behaviour is given peer approval and reinforced by the unlikelihood of being

caught by authorities. This theory takes up the economic explanation in that, when Internet scamming brings enormous financial gains to one youth amidst his/her unemployed or underemployed friends, online connectivity inducement and peer-learning will propel peers with reduced self-control to model their lives after such cyber criminals (UNODC, 2011). Of over 60 per cent of all Internet users in developing countries, 45% of the users are below the age of 25, exhibiting a subculture of young unemployed men who take pride in getting rich through computer-related financial fraud (UNODC, 2013). These aforementioned technical, social and economic factors account for Africa's cybercrime experiences.

Current Cybercrime Experience in Africa: Exploring the Scope, Measuring the intensity

An essential and common justification of national and regional strategies and legislation to guarantee confidence in cyberspace rests on the fact that national and regional contexts determine the scope and intensity of cybercrime. Such determination influences the national and regional strategies that may be deemed as appropriate to counter cybercrime. It is on this basis that Jane Duncan (2013) asserts that, generally, cyber terrorism and cyber warfare do not constitute Africa's vulnerability in cyberspace. Similarly, Contador and Pierluigi (2012) assert that hacktivism (hacking aimed at promoting a particular political ideology) and cyber espionage are rare on the African continent. Bearing in mind that different cybercrime incidents across the African continent depend on the specificity of the country's infrastructure, the uptake of technology (Contador and Pierluigi, 2012), and a country's legislation (ITU, 2012), it is possible to determine the range of common cybercrimes but it is generally hard to measure the intensity/impact of cybercrime on the continent as a whole.

With regard to the scope of cybercrime, uniformity in cybercrime has been noted to include, but is not limited to, the following: massive theft of images /identities and spam that cut across all African regions; bank accounts disruptions, and pornography distribution common in East African region; defamation, website defacement, fraud, and illegal online gambling that are common in the Southern African region; money laundering and advanced fee fraud common in West Africa; terrorist financing common in North and East African regions; and malware design production and usage common in Northern Africa – especially Egypt (Contador and Pierluigi, 2013; UNODC, 2013).

When discussing such trends, it should be noted that the ITU (2012) provides some key reasons why cybercrime has proven hard to completely track and record at all levels. First, it is because variations in legislation as well as tracking practices of various countries lead to incomplete records on cybercrime. Second, available statistics only show crimes that are detected and recorded, leaving out much on the African continent owing to lack of technical capacity (e.g., cyber forensics) and human capacity needed by African governments to track cyber crime. With particular reference to the magnitude of online financial scams, fraud, or money laundering that constitute a common online offence in Africa, businesses such as banks fear the negative publicity that would damage trust in their e-commerce and, most often, they choose to cover up cybercrime. Lastly, the fact that cyber attacks are now largely automated means that investigations are necessarily complex and resource intensive. Failure to devote the necessary resources means that such investigations are ultimately unsuccessful. Accordingly, many attempts to measure cybercrime are elusive and unreliable at the national, regional, and global levels.

Nevertheless, to understand the extent of cybercrime in Africa, determine guidelines for regional or national penal provisions to

guarantee confidence in cyberspace, and critique the AUCSCPDP *vis a vis* the values it seeks to uphold in this age of an information society, it is helpful to highlight some statistics relating to cybercrime.

Statistics show that access to Internet, portable online devices, social media utilisation and cybercrime is growing faster on the African Content than any other in the world (Contador & Pierluigi, 2012). With an average Internet penetration rate of 70% into countries representing major regions of the African continent such as Nigeria, Kenya and South Africa, the number of Internet users in Africa is estimated to reach 500 million by the end of 2013 (Contador & Pierluigi, 2013). Correspondingly, at the turn of the millennium, 564 cyber security incidents were reported across Africa but in 2011, such incidents had reached a record high of 18,607. By the first quarter of the year 2012, 8,903 cyber security incidents had already been reported constituting mostly financial fraud, phishing, spam, data breaches targeting mostly African banks, introduction of malware, and Denial of Service (DoS) attacks causing loss of data (Contador & Pieruigi, 2012). A brief survey of how cyber crime manifests in some countries across Africa is instructive to set the basis for analysing coverage of substantive crime in the AUCSCPDP.

Nigeria was reported by 2008 to have made the most money via Internet financial scamming (usually called "419" in Nigeria or advance fee fraud, and primarily targeting the USA) recording an income of 183 Million USD in 2008 (Gunness et. al., 2008). Usually, the victim of a financial scam receives an unsolicited fax, email or online message concerning proposals relating to dubious money laundering or false advertisement of a nonexistent product or service. From Ghana, the *Sakawa* group in Nima is known for selling stolen credit card numbers to USA or Europe as well as ordering goods from the USA or Europe with the said stolen account numbers (Gunness et. al., 2008). In

2013, Zambian local media reported that Zambian Police uncovered a scheme in which foreign criminals recruited and trained Zambians to effect the stealing of 4 Million USD from Automated Teller Machines (ATM) of commercial banks across the country (Chawe, 2013). These are crimes relating to data breaches in e-commerce but other forms of data breaching relating to business secrets and copyright are common in Africa.

In African organisations, other criminal incidents involving breaches of data security target copyrights and trade secrets. An estimated 24% of total global Internet traffic is estimated to infringe copyright, with downloads of shared peer-to-peer material particularly high in countries in Africa, South America, and Western and South Asia (UNODC, 2013). To boost competiveness of indigenous industries, cases of theft of industrial secrets have been reported in Zambia, Uganda, Tanzania, South Africa, Kenya and Namibia (Contador & Pieruigi, 2012). In view of measures needed by Africa to increase confidence in cyber space, it is important to note that criminals in Africa are exploiting the availability of online download tools and techniques of hacking, remote access regimes, and cyber espionage malware - especially primarily designed and used by Egypt (Contado & Pieruigi, 2012).

Furthermore, African Governments surveyed indicated that Internet content also represented a significant cybercrime concern. Some online material targeted for removal by governments include child pornography and hate speech, but also includes content related to defamation and government criticism (UNODC, 2013). Several cases[16] relating to online

[16] Media Workers Association of SA obo Mvemve v Kathorus Community Radio (2010) 31 ILJ 2217 (CCMA); Smith v Partners in Sexual Health (non-profit) (2011) 32 ILJ 1470 (CCMA) cited On 4 and 5 April the Lex Informatica 2013: Cyber Law, ICT Law and Information Ethics Conference that was held in Pretoria.

social media misconduct such as online defamation, for example, have been prosecuted in South African courts in which the applicant sought an interdict to restrain the respondent from posting certain information on social media websites and to remove postings that had already been made (O'Reilly, 2013).

This review on cybercrime manifestation in Africa shows that the values sought after by the AUCSCPDP resonate with the African experience of cybercrime. It is evident that financial fraud, copyright violations and trade secret violations in Africa pose an online threat to property and cultural heritage of individuals, organisations and nations. It is evident that the value of having authentic online content may have been compromised by defamation in social media, hacking & defacement of government websites, the creation & online dissemination of child pornography and hate speech. It is evident that hacking offenses of private or sensitive online data have led to violations of basic rights such as privacy. All these have created the need for multidisciplinary oversight on computers, computer systems, mobile networks, and the Internet. However, the value of preserving the survival and sovereignty of African states, which is highlighted in the DAUCCSC (the earlier draft) and enforced in problematic provisions that violate the rights to privacy and free speech in the AUCSCPDP is largely unfounded. This is because as we have assessed, the manifesting trend of cyber threats and crimes do not in fact, warrant urgent measures that must violate for example, the right to privacy in a bid to guarantee state security. Despite some hacking attempts into government data bases or use of the Internet for terrorism, crimes and threats covering data espionage relating to national security, attacks on critical information infrastructure relating to territorial integrity or cyber warfare are yet to emerge in African countries.

This implies that the AU approach to guarantee cybersecurity should not evoke concepts like state security and national

sovereignty as the basis for undermining human security or basic freedoms like the right to privacy and freedom of expression. To build confidence in cyber space, AU action must address various areas ranging from prevention and detection of cyber threats to the prosecution of cybercriminals, while simultaneously accounting for localized variations in available skills, common cyber threats, and societal demands. Such an approach best fits with the Global Cyber Security Agenda of the forum on World Summit on Information Society.[17]

The Global Cyber Security Agenda

As early as mid 1960s, the creation of a central database authority for government services is recounted especially in the USA (ITU, 2012), giving rise to cybercrime incidents in different countries. Cybercrime by then involved the sabotage of computer data, notably, the 1969 Canadian student protest against a racist professor that led to the burning of a university computer data facility – i.e., Hall Building (Kabay & Whyne, 2009). Also, cybercrime then related frequently to breaching of private or confidential data.[18]

[17] The International Telecommunications Union (ITU) signed a memorandum of understanding with UNODC relating to capacity building and technical assistance to avert cybercrime especially in developing countries (ITU, 2012). On this basis, the ITU has organized the World Summit on the Information Society (WSIS) in two phases that led firstly, to the *Geneva Action Plan (2003)* highlighting measures to build confidence and security in the use of ICTs in the information society and secondly, *to the Tunis Agenda for the Information Society (2005)*, which highlights international cooperation within the framework of UN-GAR and the Council of Europe Convention on cybercrime (ITU, 2012).

[18] In 1970, teenager Jerry Neal Schneider used Dumpster diving to retrieved discarded printouts from the Pacific Telephone and Telegraph (PT&T) company in Los Angeles, used the computarised data to have $30,000 worth of equipment sent to a normal PT&T dropoff point, and collected the property which he promptly stole and sold for personal gain (Kabay & Whyne, 2009).

However, the earliest regional agenda of cyber security is traceable to 1976, when the Council of Europe held a conference dealing with aspects of economic crime and later setting up a committee of experts (1985) to discuss legal measures to combat cybercrime, producing the *Expert Report on Computer Related Crime* whose recommendation (to improve international legal co-operation to combat electronic fraud and forgery) the EU Committee of Ministers adopted in 1989 (ITU, 2012). Furthermore, the earliest global agenda related to cybercrime is traceable to the UN Congress on the Prevention of Crime and Treatment of Offenders, the umbrella under which falls UN General Assembly Resolutions[19] (UN-GAR) 45/121 (1990); UN-GAR 55/63 (2000); UN-GAR 56/121 (2002); UN-GAR 60/127 (2005); and UN-GAR 64/211 (2010) respectively provided for the following:

- preventing and controlling of computer crime through criminal and penal measures by states with especially with regard to the productivity, distribution, dissemination, exporting, importing offering, selling or possession of child pornography;
- establishing procedural instruments of transnational cybercrime investigation (state co-operation with public and private partnerships;
- eliminating safe havens for computer crime by improving public awareness and law enforcement capacity in transnational investigations and prosecutions relating to abuse of information technology, security of computer data and systems;
- harmonising municipal legislations criminalising cyber offense with reference to existing regional conventions such as the Council of Europe Convention on Cybercrime and finding the possibility of negotiating an

[19] Analyses on these resolutions are found in UNODC, (2011); ITU (2012) and UNODC (2013).

international convention under the auspices of the United Nations Office on Drug and Crime (UNODC);

- using UNODC's global network of regional offices to specifically help countries review and update legislation relating to and legal authorities dealing with privacy rights in cyber space, data protection, commercial law, digital signatures and encryption as well as calling for states to use regional conventions for such specifics.

As a specialized agency within the UN dealing with standardisation and development of telecommunications, as well as cyber security issues, the International Telecommunications Union (ITU), through the World Summit on Information Society (WSIS) has come up with five work areas to combat cybercrime and guarantee confidence in cyberspace. These include: 1) Legislative measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation. Legislative measures would deter criminal actions over ICT networks as per the local context of threats with international standards. Technical measures would improve cyber security and procedural measures would facilitate cyber risk management through accreditation schemes, protocols and standards. Prevention of cyber offences, detection of, response to, and crises management of such offences necessitate organizational structures. The protection of critical information infrastructure, expansion of strategies for raising awareness on cybercrime, and the transfer of know-how to aid national policy agenda on cyber security necessitates capacity building. Owing to the transnational nature of cybercrime that usually, implicate a diverse range of stake holders, international cooperation would aid transnational dialogue and coordination in dealing with cyber offenses.

The global cyber security agenda is justified on the fact that countries that chose to solely legislate and criminalise cyber offences face severe difficulties in implementing laws (ITU,

2012; UNODC, 2013). With reference to cyber insecurity in South Africa, Professor Duncan (2013) - Highway Africa Chair of Media and Information Society at Rhodes University - strongly asserts the need to prioritise technical and social solutions. Brechbuhl et. al., (2010) emphasise that cybersecurity is a shared responsibility among all users and providers of ICT networks and infrastructure. It is on this basis that Ilie et. al., (2011) call for collaborative intra-national and transnational activities among public and private sector stakeholders to avert cyber offences and prevent cybercrime.

The AUCSCPDP in the Global Cyber Security Agenda: Steps in the Right Direction?

The Global Cyber Security Agenda of the World Summit on Information Society (WSIS) suggests that the fight against cybercrime can never be limited to legislation. There is broad consensus that the harmonisation of legislation across regions on the globe is an *essential* step amongst other aforementioned measures to halt cybercriminals (ITU, 2012; UNODC, 2013). The implication is that cyber security should be pursued as a policy – comprehensive strategy that identifies different instruments, and co-ordinates stakeholders upon a cost benefit analysis to avert cybercrime. It is on this basis that in Johannesburg (2009), the AU Ministers in charge of Communication and Information Technologies (CIT) discussed vulnerabilities of increasing use of ICT in Africa, calling for a partnership with the UN Economic Commission for Africa to develop a legal framework to aid African countries in addressing electronic transactions, cyber security and data protection (in the *Oliver Tambo Declaration, 2009*).

The 2009 Declaration was endorsed as a resolution of the 14th AU Summit of the Head of States and Government on *Information and Communications Technologies in Africa: Challenges and Prospects for Development* in February, 2010. To move the African cyber security Agenda forward, the AU ministers in charge of

ICT (in their August, *2010 Abuja Declaration*), requested the AU commission to "jointly finalise with the UN Economic Commission for Africa… the Draft Convention on cyber legislation and support its implementation in member states by 2012" (Yankey, 2013, p. 10) within the framework of the African Information Society Initiative (AISI). From this perspective a cyber security convention for Africa would have the objective of harmonising legislation related to e-transaction development, protection of personal data, cyber security promotion, and the fight against cybercrime with the ultimate goal of protecting institutions, persons and states against growing cyberspace offences in Africa.

Finally, the AUCSCPDP is divided into three major chapters. Chapter One covers: regulations of electronic commerce (Art 2-3); publicity by electronic means (Art 4); and electronic contracts and transactions (Art 5-7). Chapter Two covers: a legal framework for personal data protection (Art 8-9); formalities for personal data processing (Art 10); institutional framework for personal data protection (Art 11.); functions of National Protection Authorities (Art 12); consent and legitimacy of personal data processing; principles on objective, relevance and conservation of processed personal data; provisions on accuracy, confidentiality and security of personal data; processing of sensitive data; right to information, to opposition, to correction, suppression or conservation of data by persons whose data is being processed (Art 13 -23). Chapter Three of the AUCSCPDP (Art 24 -31) is set to promote cyber security and to combat cybercrime. It covers material penal laws and procedures for restoring confidence in cyberspace. This Chapter includes provisions for: national policies and strategies (Art 24); organizational structures such as National Regulations Authorities (Art 25(2); protection of critical information infrastructure (Art 25(4); the role of government (Art 26(2); public-private partnerships (Art 26(3) & Art 27(b)(iii) on cyber security issues; awareness raising and capacity building (Art

26(4); international co-operation (Art 28(2),(3),(4); harmonisation of cybercrime legislation (Art 28(1) and national Computer Emergencies Response Teams (CERTs) & Computer Security Incidence Response Teams (CSIRTs).

The material penal measures cover attacks on computer systems (Art 29 (1) and attacks on computerised data (Art 29 (2). Also, penal measures cover content related crimes such as the following: child pornography; xenophobia; discrimination based on race, color, religion, national or ethnic origin and genocide & crimes against humanity (Art 29(3)(1). The penal measures outlaw organized cybercrime groups and provides that devices used for cybercrime be confiscated (Art 29(3)(2)&(3). Also, Chapter Three of the AUCSCPDP addresses online violations against property (Art 30(1); defines criminal liability for corporate persons (Art 30(2); enacts penal sanctions (Art 31(1)&(2) and procedural law (Art 30(3) for crimes specified in the convention. The aforementioned parts of the AUCSCPDP constitute the areas subjected to debates on whether the AUCSCPDP is substantially and procedurally apt, contextually appropriate for the continent and compatible with the global cyber security agenda.

Basing on the provisions of the AUCSCPDP, the nature and prevalence of cybercrime on the continent, and the global cyber security agenda, the AUCSCPDP is judged to be the most comprehensive regional cybercrime convention in terms of the scope of coverage (ITU, 2012, p. 138; UNODC, 2013). The AUCSCPDP spans issues considered critical to make any convention holistic in guaranteeing cyber security. Some issues that are provide in the DAUCCSC but are left out of the celebrated Council of Europe Convention on Cybercrime (CoECC) include, for example, online orchestration of spam, content related to xenophobia, discrimination and genocide, as well as provisions relating to the admissibility of digital evidence or the emerging use of encryption technology. A technical

measure against cybercrime that differentiates the AUCSCPDP from all other regional conventions is the call for member states to adopt rules to compel ICT product Vendors to submit their products for vulnerability tests to independent experts and to provide the public with information related to the vulnerabilities uncovered and the solutions to such vulnerabilities (Art 29(1)(g). Although this idea (based on incorporating security measures into Africa's ICT development) is widely recommended especially, by the International Telecommunications Union (ITU, 2012) and the United Nations Office on Drug and Crime (UNODC, 2013), it has never been tested and the details on how this is to be implemented is not detailed in the AUCSCPDP, raising fears among some ICT stakeholders.

Furthermore, like most other regional or global conventions, the AUCSCPDP provides for organisational structures against cyber crime in AU member governments, in public-private partnerships and in education and capacity building against cybercrime (Art 24; 25& 26). It also provides for international co-operation mostly based on dual criminality, information sharing and harmonization of national laws with regional laws on cybercrime (Art 28) On all these counts, the AUCSCPDP resonates commendably with the global agenda on cyber security. However, a comprehensive evaluation of the AUCSCPDP is incomplete if we do not consider how its actual substantive and procedural provisions resonate with global standards. In Part Two, by benchmarking against the most widely used convention - the CoECC, this critical review examines the impact the AUCSCPDP will have on basic rights (such as the right to privacy, freedom of expression, and access to information) in its attempt at a continent wide internet governance in this age of information society.

PART TWO

Benchmarking the Council of Europe's Convention on Cybercrime (CoECC)

Within the framework of the Council of Europe (CoE), the nature of computer related crimes and its impact on e-commerce were first discussed in a conference in 1976 (ITU, 2012). This was the basis for forming an expert group that explored the possibility of substantive criminal legislation against computer crimes from 1985 to 1989, resulting in an *Expert Report on Computer Related Crimes.* Basing on the recommendations of the report, which provided guidelines for the drafting of an adequate regional legislation to promote harmonization of cybercrime laws in the region and promote international co-operation against cybercrime, the Committee of Ministers and the Committee on Crime Problems of the CoE constituted another Committee of Experts-2 to draft a convention on cybercrime in 1996. From then to 2000, the Committee of Experts held fifteen meetings in open-ended drafting groups and ten plenary sessions, producing a final draft *Convention on Cybercrime* (ITU, 2012). The final draft was adopted by the CoE Assembly in April 2001 and opened for signature in Budapest on November 23, 2001 (ITU, 2012). The CoECC[20] is the first and most widely used international treaty on cyber crime (Ilie et. al. 2013; UNODC, 2013). By September 2013, forty states had ratified the treaty including states out of the Europe such as the USA, Dominican Republic, Australia and

[20] See the treaty document at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Japan[21]. Additionally, eleven states have signed the treaty, including Canada and South Africa[22].

The preamble of the CoECC reveals the aim of the convention – to ensure "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation" (Paragraph 4). To this end, Section one of the CoECC provides measures to be taken at member state level to institute substantive criminal law for offenses that violate the confidentiality, integrity and availability of computer data and systems (such as illegal access, illegal interception, data interference, system interference, misuse of devices); Computer related offences (such as computer related forgery and fraud); and Content related offences (such as child pornography and infringements of copyright). Section two sets standards for its member states procedural provisions for efficient investigations on cybercrime (including procedural safe guards, expedited preservation of stored computer data and partial disclosure of computer data, production order, search and seizure of stored computer data, real time collection of computer data and interception of content data). Section three addresses the issue of jurisdiction and international cooperation relation to cyber crime (including general principles for harmonizing domestic laws of member states, extradition, mutual assistance, spontaneous information to prompt investigation or thwart cyber crime attempts) among member states. The CoECC provides an explicit, prescriptive legal framework for the criminalisation of cybercrime, a key feature that has seen greater harmonisation of national cybercrime laws of state parties to the convention.

---

[21] See the Council of Europe Website at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[22] Actually, Canada, Japan and South Africa did participate in the preparation of the convention.

In contrast, the language of the AUCSCPDP reads many times as broad guidelines to member states for cyber security that may lead to conflict of laws in prosecuting cyber offences across AU member states. This is because, across Africa, different states have diverse legal systems mainly covering common law (in English speaking Africa), civil law (in French speaking Africa), the hybrid system (both inquisitorial and adversarial as in Cameroon), Islamic law, and customary law. As adopted, the AUCSCPDP does not suffice in guaranteeing harmonization of cyber security legislation among the member states (Uchena, 2012). Given the reality that most African states do not have effective cyber laws in place (UNODC, 2013), the AUCSCPDP could do more to harmonise what is likely to eventually emerge in African states as conflict of laws in the area of cyber crime by explicitly establishing a model legal framework for states to adopt and ratify into their municipal laws (Uchena, 2012). To exemplify this process, the Arab League Convention on Combating Information Technology Offences (2010), builds on the Arab League Model Law for E-transactions and E-Commerce (2004) covering e-payments, e-contracts and consumer protection would be a wiser starting position for the expert group that drafted the AUCSCPDP. Without a model law on cybercrime, there is the potency of conflict of laws among municipal legislations of countries in the African Union. By way of comparative analysis of the substantive and procedural provisions of the AUCSCPDP and the CoECC), which is deemed to be practically effective in curbing Europe's cybercrime (Ilie et. al. 2013; UNODC, 2013) this paper illustrates how the AUCSCPDP is practically set to pose violations to fundamental freedoms.

The Violation of the Right to Privacy in the AUCSCPDP

The UN Office of the High Commissioner for Human Rights (UNOHCHR, 2014) reports that mass covert and overt digital surveillance is a dangerous habit that is normalising among national governments. Increasingly, governments threaten to

ban services of telecommunication and wireless equipment companies if they do not provide direct access to communication traffic, tap fibre optic cables for purposes of national security surveillance (UNOHCHR, 2014). Also, Internet related companies are tasked to systematically disclose bulk information on employees or customers (UNOHCHR, 2014) for the sake of national security. Appeals against such intrusions have long been generally squashed by governments who think the notion of 'privacy' defies any categorical description in the realm of national security (Glancy, 1979). However, the Right to Privacy was conceptualised first in 1890 with a definitive content that is enduring.

Glancy (1979) argues that the Right to Privacy is an inevitable development because in historic perspective the notion goes beyond its infusion into legal theory in 1890. Preceding 1890, a wide array of legal concepts and precedents in different aspects of common law (such as property law, protection of trade secrets, family law e.t.c.) all hold the notion of the right to privacy. The jurisprudential conception of the Right to Privacy designates an entitlement guaranteeing the inviolability of an individual's personality (Waren and Brandeis, 1890). It is an individual's entitilement to determine ordinarily, the extent to which one's thoughts, sentiments, or emotions shall be communicated to others or made public (Waren and Bradeis, 1890). In contrast to the notion of privacy in other areas of Common Law, the distinctive category of an individual's Right to Privacy is justified as a fundamental, negative right or entitlement without which very core of an individual's personality would be injured or one's self image affected and distorted (Waren and Bradeis, 1890).

The inalienability of the Right to Privacy has a universal appeal and guarantee. This explains why the International Covenant on Civil and Political Rights provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy,

family, home or correspondence, or to unlawful attacks on his honour and reputation" (Article 17). Against such interference or attacks by governments, the European Union Court of Justice establishes as illegal, the aggregation of private information or "metadata."[23] This is because, in the name of Internet governance for national security, such data may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication and availing such content to various government agency without consent amounts to violations of the right to property. The UNHCHR, 2014 holds that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case" (p.7).

The AUCSCPDP has in particular reference to the African socio-political context, used contested concepts such as *state security* and *public interest* as exceptional circumstances, which state appointed authorities can use to process[24] sensitive data[25] and

[23] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37. See also, Executive Office of the President, "Big Data and Privacy: A Technological Perspective" (available from www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), p. 19.

[24] Automated or unautomated operations and procedures, applicable to data, such as gathering, exploitation, registration, organization, conservation, adaptation, modification, extraction, safeguarding, copying, consultation, utilization, communication through transmission, dissemination or any other form of circulation, exposure or interconnection, as well as the interlocking, ciphering, deletion or destruction (see AUCSCPDP, Art 1)

[25] Sensitive data means all personal data relating to religious, philosophical, political and labor union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions (See AUCSCPDP, Art 1).

personal data,[26] posing a danger to the right to privacy. Even without evidence of cyber warfare on the continent or data espionage offences against critical information infrastructures of AU member countries (Contador & Paganini, 2012), the AUCSCPDP alleges[27] that the potential remote accessibility to computer networked systems poses threats to the *security*, *survival and sovereignty of the states* in Africa, requiring procedures and tools to effectively manage such risks as a *matter of urgency*. To this end, the AUCSCPDP (Art 13(1)(b) 14(2)(f) and 14(2)(i) provide that personal data and sensitive data on computer systems should be processed without consent on behalf of the state on the basis of state security, public security and public interest (10(4)(e) & 10(5)(a). But what is wrong with the use of "Public Interest?"

Basing on the context of the US and the UK, Feintuck (2004) observes that the term 'public interest' is frequently used in legislation and politics without agreement on what it means and what actions in regulation are appropriate to realise "public interest." The meaning of public interest in the US and UK rests on a market-based perspective: welfare or well-being of the general public; commonwealth; and appeal or relevance to the general populace (Feintuck, 2004). As such, the elusiveness in the conception of "public interest" leads regulators into a

[26] Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (see AUCSCPDP, Art 1).

[27] We do not intend to say that online criminality does not and will not pose a threat to African Countries. It is common knowledge that terrorism is and will continue to be a threat to African countries of especially the eastern and northern part of the continent. The use of internet and computer systems to aid or actualize terrorism is sufficiently criminalized in Art 30 of the AUCSCPDP. Cyberwar and data espionage in relation to critical information structure, crimes not yet actualized on the continent have in foresight, been covered in Art 30(1)(b-d) of the AUCSCPDP .

bureaucratic drift (the principal-agent problem in which agencies pursue their own interpretations far removed from expectation of the populace) or a political drift (in which the meaning of public interest becomes susceptible to changes in state governments or strongest political actors that appoint the agencies (Feintuck, 2004). This could explain why the CoECC uses the concept 'Public Interest' only once but specifically narrows it down to the "sound administration of justice." Similarly, the CoECC uses the concepts "sovereignty, security, *ordre public*" only twice (Art 29 & 30), leaving each state party to the CoECC the liberty to deny expedited disclosure of preserved traffic data to another party if such disclosure will impact on the "sovereignty, security, *ordre public"* of the state party hosting the requested data. However, the AUCSCPDP (Art 10(4)(e); 10(5)(a); (13(1)(b); 14(2)(f) and 14(2)(i) employs 'public interest' and 'State Security' with such imprecision that warrants concern when interpreted in the context in which the overall provisions are set.

Colvin and Cooper (2009) hold that the mere existence of such broad legislation with an intrusive nature of investigative power legitimising that a suspect be left unaware that their private information is being collected entails an imminent threat to the violation of the right to privacy. With the AUCSCPDP, data processing on the basis of public interest can mean processing personal or sensitive data for reasons of *security*, *survival and sovereignty of the states,* concepts that have contested meanings in relation to Third World States. The problematic meaning of these concepts in relation to current Third World politics poses the risk of legitimizing the violation of citizen's privacy rights in implementing the AUCSCPDP.

Hardly can African politics in particular, be considered as aligned to 'public interest'. Politics in each African country is characterised by contest to the legitimacy of government power. As the African experience reveals and as analysis on African

politics expounds, within any single African country, there are many nations that are divided along ethnic and religious lines. These many nations contend for different interests, various welfare needs and diverse security needs that cannot be lumped into a unified understanding of 'Public Interest' or 'State Security' (Job, 1992). Most often, these diverse welfare needs or the diverse security interests are in contrast with the welfare needs and security interests of incumbent regimes, which are most often perceived by the populace as exclusively representing other groups (Job, 1992). The fact that governments in almost all African states lack the support of a significant number of other nations within the African state creates a kind of subaltern realism (Ayoob, 1995), which poses an insecurity dilemma (Job, 1992) to the state[28]because it is largely perceived by the average African as patronage institutions to advance regime interest.

This political experience, which is characteristic of the African state clouds the meaning of the concepts "public interest" or "state security" especially in Africa, making the use of such concepts in African legislation equivocal and problematic. In this perspective, state security/interest in African politics may be compatible with regime security/interest but is almost always incompatible with a broad section of national securities/interests, individual security/interest or 'public interest'. As such, exempting the principle of consent with the use of *state security, public security and public interest* in processing personal data or sensitive data in African countries does not translate into processing such data for the wellbeing of the populace or for the commonweal. Against this background, the AUCSCPDP (Art 10(4)(e); 10(5)(a); (13(1)(b); 14(2)(f) and 14(2)(i) will most likely violate the civil liberty to privacy, scare away Internet users, limit access to information, curtail the

[28] These are sets of institutions that constitute the monopoly of force, taking charge to organize and regulate interactions between groups and individuals within that specified territory accorded recognition as an independent and equal party in the community of states.

provision and free flow of socio-political / cultural opinions and information, and ultimately destroy the culture of freedom of expression that is a hallmark of the Internet (Chertoff, 2008).

The Violation of the Freedom of Expression

The increasing use of social media and what is deemed 'unacceptable user-generated Internet content' by many African governments (UNODC, 2013) has met with regulatory provision (Art 31(3)(d) in the AUCSCPDP that will seriously curtail online freedom of expression. In contrast to the AUCSCPDP, the CoECC gives provisions for investigating the use of computer systems for other criminal purposes and for collecting electronic evidence (Art 14ff). Specifically, Art 20 provides for the collection of traffic data in real time. But recognition that the collection of traffic data is, to a significant extent, equivalent to the collection of content data (especially if conducted alongside personal data processing), the authors of the CoECC procedurally limit the power to intercept content data to *a range of serious offences to be determined by domestic law* (Art 21). By implication, this provision (Art 21) enjoins state parties to guarantee the rights to privacy and freedom of expression by specifying, in domestic laws, serious offences that warrant the interception traffic data. Unlike the CoECC, the AUCSCPDP (Art 31(3)(e) reads:

> State Party shall take necessary legislative measures to ensure that, where the imperatives of the information so dictate, the investigating judge can use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system or compel a service supplier to gather and register the data within, the framework of his/her technical capacities, using the existing technical facilities in its territory or that of States parties, or provide support and assistance to the

competent authorities towards the gathering or registration of the said computerised.

Unfortunately, this provision implies that the interception of traffic data and content data will be initiated by investigating judges on a phrase that connotes a condition of no limit, that is, "… where the imperatives of the information so dictate…" Such unfounded basis for curtailing freedom of expression is currently receiving resistance from Internet service providers who are essential in the generation of real time data and content data. For example, the Global Network Initiative has recently filed petitions to 21 countries of North America, South America, Europe and Africa including Ghana, Kenya and Mexico in a bid to save their clients from violations of the right to privacy and freedom of expression (APF, 2013). This initiative of technology giants including Google, Facebook, Yahoo and Microsoft are asking governments to make it legally possible for them to publish requests from governments that data be divulged on broad bases of *national security, law enforcement or electronic communication surveillance* (APF, 2013, NP). The rationale of the initiative is that transparency will tame unnecessary data requests made on such broad bases, and boost the confidence of Internet users with regard to their rights to privacy and freedom of expression (APF, 2013). The AUCSCPDP (Art 31(3)(e) is a dangerously vague condition that will create sufficient conditions for limiting freedom of expression online. But is there any such thing as a limitless freedom of expression in any law?

Like the AUCSCPDP,[29] any legislation aimed at enhancing the right to freedom of expression is crafted with limitations. As

[29] Indeed the AUCSCPDP has limits to freedom of expression by extensively criminalising online content relating to Child Pornography (Art 29(1) (a-e); Racism and Xenophobia online content perpetuating discrimination based on race, color, ancestry, national or ethnic origin or religion or cyber offences against groups based on such characteristics (Art 29(1) (f-g); and Genocide

such, all International human rights instruments require criminalisation of extreme forms of expression. On this basis, the United Nations Special Rapporteur on the promotion and Protection of the Right to Freedom of Opinion and expression identifies four forms of expression that must be outlawed. These include: child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred or incitement to discrimination, hostility or violence; and incitement to terrorism (UNODC, 2013), and these are commendably[30] executed by the AUCSCPDP. Furthermore, municipal legislations generally exercise the leeway of determining limits to freedom of expression based on her legal tradition or socio-political context, an acceptable practice from the perspective of international human rights discourse (UNODC, 2013). That is why some concepts commonly used to limit freedom of expression in various countries include 'national security', 'public safety and prevention of disorder or crime,' 'public order,' 'public health,' and 'public morals' and 'state of emergency' are acceptable.

However, the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the

---

(Art 29(1)(h). These limitations on freedom of expression are in line with international human right laws. Any other provision for limiting freedom of expression needs to be specified.

[30] Some critics in online discourse on the AUCSCPDP disagree that the draft convention has commendably criminalized discrimination. They hold that the draft goes too far in outlawing "discrimination" and that if discrimination is not aimed at inciting or executing violence, merely supporting a discriminating view should not be illegal. As such the critics hold that Art 29(3)(e) of the AUCSCPDP violates freedom of speech, especially if the kinds of data specified- "creating, downloading, disseminating or circulating in whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using a computer system"- are not meant by intent or nature to incite, or perpetuate an attack or hate.

Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR (African Commission on Human and Peoples' Rights) Special Rapporteur on Freedom of Expression (2006) jointly declared that in "many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues (n.p.)." Furthermore, the United Nations Human Rights Committee (2011) has strongly expressed concerns for specific limitations on freedom of expression based on issues such as *disrespect for authority, disrespect for the state, defamation of the head of state, or the protection of the honour of public officials* (p.9). Nowadays, the Internet and social media are commonly used across Africa for political activities and for socio-cultural expression, and research findings show that some content-related online material targeted for removal by mostly Third World governments include, *inter alia*, defamation and criticism against government (UNODC, 2013). Basing on this context, the broad and vague basis (Art 31(3)(e) for the interception of traffic data and content data in the AUCSCPDP is simply and clearly set to curtail freedom of expression within AU member states.

Duncan (2013) holds that by incorrectly situating the processing of personal/sensitive data without consent and the interception of traffic data/content data within the context of an urgent need to secure the state, safeguard 'public interest' and the 'imperative of information,' policy overreactions of the AUCSCPDP (Art 10(4)(e); 10(5)(a); (13(1)(b); 14(2)(f); 14(2)(i) and 31(3)(d) will have dire consequences on citizens of AU member states. In the words of Mark Neoclesus, the "emergency powers" created to violate privacy and curtail freedom of expression "gradually strengthen beyond their original scope, then get justified and legitimized to become everyday rule of law, the emergency becomes permanent and the exemption the rule, the sun then fails to set on the sunset clauses" (cited in Duncan, 2013, n.p.). The violation of citizens' civil liberties within AU member states

could worsen additional AUCSCPDP provisions (Art 29(1)(g); 30(1)(b); 31(2)(a) that directly amount to legislative overkill.

Online Legislative Overkill in the AUCSCPDP: An Additional Burden on the individual

In addition to violation of the rights to privacy and freedom of expression, individual citizens will suffer from disproportionate penalties in relation to cybercrime committed on their identity either knowingly or unknowingly. As the literature review on cybercrime incidents in Africa reveals above, data breaches by organized groups of criminals commonly aimed at stealing and selling personal data (for example bank account numbers and PINs) in cyber space, as well as using stolen personal data to order goods and services online, are more common compared with hacktivism and cyber espionage (Gunness, 2008; Contador & Pieruigi, 2012). Also, it is common knowledge that the cyber user in Africa is, on average, not yet sufficiently educated on cybercrime. As such, the average cyber user in Africa is negligent (e.g. not logging off social network sites) or careless (e.g. owning a private laptop with no installed antivirus software). Consequently, countless private online accounts are frequently hacked and offences (e.g., phishing attempts, scamming and spamming) executed with use of the victim's personal data. Yet when stolen personal data is used for cyber crime, the victim will be liable of an aggravated cybercrime and an additional penalty provided for in Art 30(1)(b) and Art 31(2)(a) of the AUCSCPDP.

The provisions (Art 30(1)(b) and Art 31(2)(a) of the AUCSCPDP qualify all crimes committed with use of ICT as having an aggravated circumstance (Art 30(1)(b) and will permit additional punishment (Art 31(2)(a) for all such crimes. The implication is that the provisions create a sufficient condition for disproportionate punishment over minor offences such as spamming, possession of stolen goods, abuse of trust, extortion

of money, (spurring up this concept of "legislative overkill"). To this end the provision reads:

> State party shall take necessary legislative or regulatory measures to consider as an aggravating circumstance the use of information and telecommunication technologies to commit offenses such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money, terrorism, money laundering, etc. (Art 30(1)(b).

The ITU (2012), having noted that such provisions (Art 30(1)(b) and Art 31(2)(a) are absent from all other regional conventions on cyber security, wonders why the mere fact that an offender who additionally sends an email before committing a traditional offence like breaking into a bank deserves an aggravated sentence. The AUCSCPDP, therefore, fails to capture the essence of 'aggravating circumstance' in the context of cybercrime legislation.

In municipal legislation against cybercrime, aggravating circumstances are commonly used to provide special protection to computer systems and computer data that are critical to the functioning of infrastructure such as *banking, telecommunications, health services, public services or government computers* (UNODC, 2013, p. 85). Aggravating circumstances should also serve to tailor multilateral criminal provisions to local municipal context. For example, Northern and Eastern parts of Africa may, in relation to their context of increasing terrorist threats, create as aggravating circumstance in their municipal laws the use of ICT to aid or commit terrorist acts. In the same vein, western African countries may create in their cybercrime legislation an aggravating circumstance if the financial fraud or advance fee fraud is committed with the use of ICT.

The AUCSCPDP fails to provide such possibility for AU member states to contextualize the provision on aggravating

circumstance (Art 30(1)(b) and Art 31(2)(a) by mandating that all offences aided by or executed with ICT be designated as aggravated crimes that attract additional punishment.

Compared with four other multilateral conventions that create aggravating circumstance in cybercrime legislation, the AUCSCPDP leaves a lot to be desired. First, the League of Arab States Model Law highlights aggravated penalties only for crimes of illegal access to computers/ computer systems '*with intention of nullifying, deleting, destroying, disclosing, damaging, changing or re-disseminating personal data or information*' (Art. 3) or '*in the course of or because of the discharge of his functions or has facilitated commission of the offences by a third party*' (Art. 5). Second, the League of Arab States Convention provides for aggravation if access leads to the '*obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries, or to the acquirement of secret government information*' (Art. 6). Third, the *COMESA Cybersecurity Draft Model Bill* (2011) creates as aggravation, the illegal access to '*government computers*' or '*computer systems used for critical infrastructure operations*' (Art. 19). Fourth, the *EU Directive on Attacks against Information Systems (2013)* creates aggravated penalties for committing cyber crime in a group, with a tool designed to launch cyber attacks that considerably disrupt system services, cause financial loss, cause loss of personal data, conceal the identity of the culprit and/or cause prejudice to the rightful identity owner (Art. 9). Unlike these multilateral instruments, the AUCSCPDP unwisely puts forth a limitless provision for aggravation, creating the circumstance of legislative overkill. There are other provisions of legislative overkill that will affect corporations negatively.

Online Legislative Overkill in the AUCSCPDP: An Additional Burden on Corporations

The AUCSCPDP has imposed an unjustified limitless liability and a limitless penal burden to corperations whose online services are used to commit cybercrimes. To this end, the AUCSCPDP reads:

> State Party shall take necessary legislative measures to ensure that corporate bodies other than the State, local communities and public institutions can be held responsible for the offenses defined in this Convention, committed on their behalf by their organs or representatives. The liability of the said corporate bodies does not exclude that of the physical persons who are the authors or accomplices of the same offenses (Art 30(2).

This provision seems mutually incompatible with Art 29(1)(g),[31] which provides that all Internet service providers in AU member states will operate only after their products and services have been vetted by an independent expert. The vetting of online services provided for in the AUCSCPDP is an important way of ensuring cooperate liability in cyberspace, reflecting an essential aspect of a good cybersecurity legislation (ITU, 2012; UNODC, 2013). The mutual incompatibility between Art 29(1)(g) and Art 30(2) stems from the idea that once an online service is vetted as safe for use, the corporation providing the vetted service should ideally, not be liable for cyber crimes committed with that service. This implies that although Art 29(1)(g) of the

[31] Article 29(1)(g) spells out that "State Parties commit themselves further… (g) to compel ICT product vendors to submit their products for vulnerability and guarantee tests to be conducted by independent experts and researchers and to divulge to the public any form of vulnerability found in the said products and the measures recommended for a solution thereto".

AUCSCPDP needs to be revised to answer questions[32] about its clarity, the idea it already represents- of incorporating a threshold for security features in ICT development and of imposing some corporate liability for cybercrime will amount legislative overkill if the unlimited liability that is further imposed on corporations in Art 30(2) and 31(1)(c)[33] not addressed. The unlimited liability imposed on corporations by the AUCSCPDP is worsened by the absence of any safe harbor provisions to shield Online Service Providers (OSPs) or Internet Service Providers (ISPs) from intermediary liability. These limitless liability and lack of safe harbor provisions[34] to shield

[32] The questions surrounding the purpose of Art 29(1)(g) the AUCSCPDP are the follows: With mutuality between rapid evolution / developments in the ICT sector and rapid increase in cyber crime, should vulnerability tests for a particular product or service be conducted once? If vulnerability tests should be conducted more than once, at what interval must it be conducted? Why should public institutions be exempted from either of criminal, civil or administrative liability if it orchestrated or aided a cybercrime offence as provided for in this convention? In the case of corporations that extensively use online services for delivering their products such as media houses and financial institutions, why should there be a limitless liability (not specified as criminal, civil or administrative)?

[33] The Article reads that "State Parties shall take necessary legislative measures to ensure a corporate body declared liable in terms of this convention is subject to effective, proportional and deterrent sanctions which include penal fines" and this is dangerous if there are no safe harbor provisions in the AUCSCPDP.

[34]Following various international models (e.g., the Digital Millennium Copyright Act in the United States, the Electronic Commerce Directive 2000 in the European Union, etc.), safe harbour provisions for Internet Service Providers and other intermediaries, shielding such entities from liability for the actions of user third parties, should be included in the AUCSCPDP. Although Article 9(2)(b) for safe harbor provision relating to the processing of personal or sensitive data of their clients by ISP or OSPs without the authorization of the Public Protection Authority as required by this convention. However, safe harbour provisions are still needed to shield ISPs and OSPs from intermediary liability with regard to the illegal content and copyright violations brought upon their service platforms.

corporations dealing with internet services will end up imposing an unnecessary burden to important stakeholders to Africa's economic health and to Africa's knowledge economy[35].

In contrast, the CoECC (Art 12) does justice in its provision on corporate liability. First, the CoECC does not discriminate between public and private corporations with regard to the responsible provision or use of online services and products. Second, the CoECC provides that, for corporations to be liable for cybercrime, the offence must have been committed for the corporation's benefit by any natural person, acting either individually or as part of an organ of the corporation [Art 12(1)]. Third, the offence must have resulted from lack of supervision or control by the corporation [Art 12(2)]. Lastly, the CoECC provides that each state party should limit within their domestic laws, corporate liability to criminal, civil or administrative specification [Art 12 (3)]. Therefore, the CoECC aids corporations in contributing to both knowledge economy and improves the Gross Domestic Products (in terms of more ICT products and services) of their state parties. In contrast, the AUCSCPDP limits the knowledge economy by shutting down

[35] Furthermore, such provision on broad co-operate liability will slow down African economies, considering how ICT growth is fueling GDP in South Africa, Kenya, Nigeria and Egypt to mention but a few. For example, as an economic sector in Kenya, growth in ICT outperformed all other sectors of the Kenyan economy over the last decade, growing at an average of about 20 per cent per year. Indeed, in the same period Kenya's economy grew at an average rate of 3.7 percent of GDP The World Bank indicates that without the forward push generated by ICT, growth would have stood at 2.8 per cent-commensurate with population growth-and therefore leading to economic stagnation. For More information, see World Bank Poverty Reduction and Economic Management Unit Africa Region- World Bank, (2010). "Kenya at the Tipping Point? With a Special Focus on the ICT Revolution and Mobile Money," *Kenya Economic Update,* Edition No. 3, Available on: http://siteresources.worldbank.org/KENYAEXTN/Resources/KEU-Dec_2010_with_cover_e-version.pdf, Accessed on: 21/06/2013.

the current growth of ICT products and services on the continent with limitless corporate liability for cyber offences, to be enforced dangerously by judges with overly broad powers.

The Absolute Powers of Judges: a basis for unjust civil liberties' curtailment and for procedural flaws in the AUCSCPDP

The AUCSCPDP provides broad ongoing investigation mandates to judges that amount to violating civil liberties and negatively affect corporations that host traffic and content data. The investigating judge can "where the imperatives of information dictates" (Art 31(3)(e) order the interception of traffic data or content or compel an Internet service provider to gather and register such data. The judge can issue a warrant to anyone for the conservation and the protection of the integrity of data in their possession for as long as two years to aid judicial proceedings (Art 31(3)(d). Where computerised data stored within any facility "is useful for revealing the truth," the investigating judge can "issue a search or seizure warrant, to access or seize a computer system or part of the system or any other computer systems where the said data are accessible from the original system" (Art 31(3)(a). According to the UNODC (2013), two issues are to be considered whenever access to subscriber data, traffic or content data and search or seizure of the same is to be warranted.

First, in international instruments, the limits and safeguards to such investigative powers must be addressed including some procedural requirements such as 'probable cause' or 'reasonable grounds' of suspicion of a serious offence (UNODC, 2013). Second, in municipal law, powers to issue search or seizure warrant by the investigating judge should be addressed, for example, by determining whether it should be based on sworn evidence, report of a cybercrime act or an affidavit from a

prosecutor or police office (ITU, 2012; UNODC, 2013). In utter contrast, the broad mandate for judges to intercept traffic and content data in the AUCSCPDP is a direct violation of the right to privacy and freedom of expression. Similarly, the broad mandate for judges to issue search or seizure warrants over computer data or computer systems will make corporations vulnerable to absolute powers of judges.

With AUCSCPDP provisions (Art 31(3)(a), (d)&(e) crafted in a very broad manner, host institutions to computerised data or computer systems are subjected to the discretion of judges implementing the AUCSCPDP in ways that will be potentially incompatible with the institution's contractual obligation to their clients. For example, research by UNODC (2013) shows that social networks retain registration data for up to 90 days after account deletion and retain transactional data and IP logs for not more than 90 days. Also, messaging service providers keep actual content, links, cookies, location information, log data, widget data for only up to 37 days after account deletion (UNDOC, 2013). Furthermore, communications and information services providers sampled for research do not retain chat room dialogue or instant messenger conversations or member directory logs (UNDOC, 2013). Worse still, Email IP/ connection logs, group IP logs, Internet connection access logs, transactional data and video message content have different retention periods not exceeding 6 months.[36] These data retention periods are clearly compatible with the CoECC [Art 16(2)] that subjects ISP to legal warrants to retain data for periods not exceeding 90 days, renewable by cybercrime

[36]For more information check out http://support.twitter.com/articles/41949-guidelines-forlaw-enforcement#;
http://pages.ebay.com/securitycenter/LawEnforcementCenter.html;
https://www.facebook.com/safety/groups/law/guidelines/; and
http://myspace.desk.com/customer/portal/articles/526170-law-enforcement-support.

investigation authorities. Rather, the AUCSCPDP provision (Art 31(3)(d) requiring ISP or any person to retain data for up to two years would add unnecessary burden on ISPs, forcing them to violate internal regulations that feed into contractual obligations that they should uphold to their clients.

This review has so far critically reviewed both substantive and procedural provisions in the AUCSCPDP. The strengths of the AUCSCPDP lie in the fact that the draft is well attuned to the African context. For example, scamming, advanced fee fraud, Automated Teller Machine hacking pose the greatest threat to e-commerce across Africa, making Art 2 to Art 5 of the AUCSCPDP, which prohibit identity flexibility and associative anonymity in ecommerce well attuned to context. Also, having established that spam poses more negative impacts upon Africa that any other continent (OECD, 2005), the AUCSCPDP (Art 4(3) & 4(6) rightly outlaw indirect, unsolicited and automated mails especially in e-commerce.

Also, Chapter One of the AUCSCPDP addresses new trends in cybercrime that were left unaddressed by the CoECC, specifically regulating the use of encryption to pose cyber offense. Furthermore, the AUCSCPDP (Art 29(3)(1)(f) and (g) addresses in the specific context of Africa, the generation and dissemination of offensive online content aimed at attacking or discriminating against a person on the basis or categories of race, color, ancestry, ethnicity and religion that was originally left out by the CoECC for fear that it may limit freedom of expression. With growing use of social media in African countries, Art 29(3)(1)(f) and (g) are appropriate in the African context where conflicts more often than not, based on or fueled by online contents, which negatively target those aforementioned categories.[37] Unique to the AUCSCPDP, Art 29(1)(g)

[37] However, this strength of the AUCSCPDP (Art 29(3)(1)(f) and (g), which is set to secure online content that guarantee mutual coexistence of peoples, unfortunately left out 'Gender', a category in which online discrimination and

(providing that all online services and products should be vetted by an independent expert body) adds more credit the AUCSCPDP. This will serve to set a threshold for secured internet service provision in Africa, a process in which internet service development and use will forthrightly incorporate security elements as an essential feature.[38] In terms of the essential areas of work on the global cyber security agenda of the WSIS, needed to secure cyber space, the AUCSCPDP stands out as the most comprehensive international instrument.

However, taking into account the current lack of cybercrime legislation in most African countries (UNODC, 2013) and the fact that the AUCSCPDP does not provide a model cybercrime law, the provisions or mere guidelines of the AUCSCPDP will likely lead to possible conflict of laws between different AU member states. Worse still, some AUCSCPDP provisions are crafted in ways that will likely permit the violation of the right to

---

attacks are highly probable in most African countries that are highly partriachal in socio-cultural expressions of life. To fully reflect the objective underpinning the provision, the Article needs to be recrafted to include the 'Gender' category.

Also the strength of Art has been compromised by Art 29(3)(1)(e)of the AUCSCPDP that outlaws even permissible views on religion, racism or xenophobia by providing that "State parties shall take necessary legislative and/or regulatory measures to set up as a penal offense the fact of… creating, downloading, disseminating or circulating in whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using an a computer system.

[38] However, what may be worrying about this provision is that Africa does not seem prepared to implement such a provision. No clue is given in the provision about the composition, nature and roles of the expert body charged with vulnerability testing. Furthermore, given that the constant development of internet service leads to new forms of cybercrime, the provision is not really specific on the intervals at which internet service or products have to be vetted by the expert body as adequate for use. That is the reason why this review appraises the idea underpinning the provision but recommends that it be recrafted to meet its noble objective.

privacy and freedom of expression. Furthermore, this review has this far shown how the AUCSCPDP overly empowers investigating judges to facilitate unjustified imposition of burdens on the individual citizen or corporations and ISPs if the convention is passed in its current form. Notwithstanding the aforementioned concerns on the substantive and procedural provisions of the AUCSCPDP, to guarantee a secure Internet and a healthy online economy in Africa's cyber space, there is need to ask: How feasible is the AUCSCPDP in the current African context with regard to technical measures, organizational structures, Human resources/capacity and multi stakeholder/ international cooperation devoted to cyber security?

PART THREE

The Feasibility of implementing the AUCSCPDP

Absence of adequate technical measures for international co-operation in the AUCSCPDP

Research (ITU, 2012) establishes that legal measures are a crucial aspect of cyber security policy needed to prevent and combat cyber offences as it undergirds what cyber offences are to be criminalised and specifies the scope of procedural powers. Ideally, legal measures further specify Internet service provider responsibility, determine jurisdiction[39] over transnational cyber offences, and specifies the range of available mechanisms for international cooperation over cybercrime prevention, investigation, and prosecution (UNODC, 2013). It is in this vein that the CoE Convention on Cybercrime [Art. 22 (a), (b), (c), (d)] enjoins each state party to specify in their legislation what jurisdiction will apply when a cybercrime is committed *in its territory; or on board a ship flying the flag of the party; or on board an aircraft registered under the laws of that party; or by one of its nationals*, in another state where the offense is punishable. Jurisdiction is a crucial issue especially in this era of cloud computing. *This challenge is becoming increasingly acute as computer services move to geographically distributed servers and data centres, collectively known as cloud computing*[40] (UNDOC, 2013: p.216).

[39] The importance of jurisdiction is expressed by almost all cybercrime conventions having provisions that address the issue of jurisdiction (including the following: The ITU/CARICOM/CTU Model legislative text; the Commonwealth Model Law; the Draft COMESA Cybersecurity Model Law; League of Arab States Convention on Combating Information Technology Offences and the CoECC) except the AUDCCSC.

[40] A technical innovation that centrally, provides Internet services or Internet access to more than one country.

The provision on jurisdiction is important in that it serves to ensure that at no point will cyber crime be unpunished due to its transnational nature. Jurisdictional provisions are, for example, crucial in a scenario where a cyber offence is committed by a national of State A in an aircraft merely registered in state A (that prosecutes on basis of the territoriality principle) in the airspace of state B (that prosecutes on the basis of the nationality principle). Secondly, the jurisdiction provision serves as an additional facilitation mechanism for international co-operation, which ideally should be established in cybercrime conventions beyond traditional mutual assistance. Having set up international cooperation on cyber security within the context of investigations, proceedings or collection of electronic evidence (Art. 23), the CoECC serves as the legal basis for extradition (Art. 24), mutual assistance (Art. 25), and the spontaneous sharing of confidential information (Art. 26), which is necessary for effective cooperation for cybercrime offenses. Unlike the CoECC, the AUCSCPDP specifically leaves out provisions on jurisdiction over cybercrime and falls short of prescriptive, procedural and substantive provisions relating to international cooperation on cybercrime.

The AUCSCPDP rightly situates international cooperation as one strategy for preventing or prosecuting cyber offenses (Art 28) but has no substantive provision addressing issues relating to jurisdiction and extradition over cybercrime. The AUCSCPDP also falls short of prescriptive and procedural provisions dealing with international cooperation over cybercrime as it only provides for mutual legal assistance (Art 28(1), Information sharing through computer Emergency Response Teams and Computer Security Response Teams (Art 28(3) and Public Private Partnerships (Art 28(4) among member states. Commenting on these limited provisions on international cooperation in the AUCSCPDP, the ITU (2012: p. 139) analyse that international cooperation is far from feasible in the AUCSCPDP.

Based on previous research[41] Rosenzweig (2012) concludes that, nowadays, the use of Mutual Legal Assistance Treaties (MLAT- which he described as an outdated 1800 model) has been the greatest setback to international cooperation over cyber offences amongst other provisions for cooperation within the framework of the CoECC, which include addressing issues of jurisdiction, extradition and spontaneous information sharing. MLATs typically necessitate that any country receiving a request on such basis must validate the request *vis-à-vis* their own criminal provisions in a lengthy verification process that, on average, lasts a minimum of three months before investigations or orders for search, seizure or preservation of electronic data of evidence is commenced (UNODC, 2013). The new trend that is being adopted in Europe to replace MLATs is *Mutual Legal Recognition* – MLR (UNODC, 2013).

MLR is based on the principle of mutual trust in criminal justice systems between member countries of the European Union, permitting a simplified and accelerated procedure that has seen the development of a *European Arrest and Evidence Warrant* (UNODC, 2013). The mutual trust in criminal justice systems is facilitated when cybercrime legislation is highly harmonized across countries participating in MLR and such harmonization has fed into proposals for a European Investigation Order that will be enforceable in all countries of the EU (UNDOC, 2013).

This means that the more prescriptive nature of CoECC (compared with the AUCSCPDP), which permits for greater harmonisation of cybercrime legislation among state parties to the CoECC (UNODC, 2013), has its implementation slowed down whenever the MLAT is evoked for cooperation rather than the provisions for jurisdiction issues, extradition and

[41] Two years after the Signing of the CoECC, Amalie M. Weber (2003), assesses the use of Mutual Legal Assistance treaties in her work, "The Council of Europe's Convention on Cybercrime: Discussing the purpose of MLATs", *Berkeley Technology Law Journal.*

spontaneous information requests. This implies that without provisions on jurisdiction concerns, extradition and spontaneous information sharing and jurisdiction in the CoECC, the MLAT would be inadequate for international cooperation over cyber threats among state parties to the CoECC.

Despite the CoECC difficulty in implementing the MLAT compared with other COECC provisions for international cooperation over cybercrime, the AUCSCPDP provides only for MLATs and information sharing, indicating again broadly, that AU member countries should make use of existing international, regional or intergovernmental means (Art 28(4) to foster cooperation over cybercrime in Africa. The difficulty that will result in using the AUCSCPDP for international cooperation is because the convention is set to give AU member states the legal basis to *resovereignise cyberspace*[42] (Rosenzweig, 2012) in ways that will likely lead to lesser harmonisation of municipal cybercrime legislation in African states compared with state parties to the CoECC. Lesser harmonisation due to lack of a continent-wide model law will then render the dominant use of MLATs more difficult in Africa over cybercrime issues. Furthermore, the absence of technical capacity for effective international cooperation, especially such as the absence of Computer Emergency Response Teams (CERTs) or Computer Security Incidence Response Teams (CSIRTs) in Africa, will further complicate the feasibility of the AUCSCPDP.

The Gross Absence of CERTs / CSIRTS in Africa: An obstacle to implementing the AUCSCPDP

CERTs and CSIRTs are indispensable to monitor, detect, analyse, and investigate cyber threats and cyber incidents for the purpose of issuing early warnings, aiding prosecution, and

[42] That is, to assert more independent state control of computer / online data and cyber space within each state territory.

promoting international cooperation on cyber offences (ITU, 2012). In more developed countries in Europe and America the multi-sector nature of cybercrime has caused the development of thriving CERTs and CSIRTs by various stakeholders such as governments, banks, telecom operators and academia (UNODC, 2013; ITU, 2012). This explains why the AUCSCPDP provides for National Regulatory Authorities dealing with forensic investigation, international cooperation, and prosecution of cyber crime, as well as national institutions that conduct surveillance, issue early warnings, and co-operate on cyber threats. **FIRST**, a global organisation of computer security incident response teams from governments, commercial bodies and educational institutions has a register of over 200 members[43], including only 11[44] out of 54 African states that do host CERTS (Wanjiku, 2013). **FIRST** enables a single global contact point for all incident response teams to more effectively foster cooperation and coordination in preventing, stimulating rapid reaction/pro-action, and to promote information sharing amongst its members on cybercrime threats and incidents.

Although national CERTs/CSIRTs are provided for in the AUCSCPDP, Art 28(3), the gross absence of CERTs across the continent does not resonate well with the global agenda on cyber security and creates the context that will obstruct implementation of cyber laws across African countries. The global agenda on cyber security emphasises the use of legislation as the summit of multi-facet strategies that should ideally be sought after education and training, technological developments, and institutional and organizational structures (e.g. CERTS and CSIRTs) is already aimed at reducing cyber threats (Musa, 2011; ITU, 2012). This explains why G8 and EU directives did establish 24/7 contact points for cyber security purposes across

[43] For more information, see FIRST < http://www.first.org/>.

[44] The countries are South Africa, Kenya, Burkina Faso, Tunisia, Morocco, Cameroon, Sudan, Egypt, Ghana, Mauritius and Ivory Coast.

Europe as early as 1999 (ITU, 2012), creating a context that made the legal validation of such contact points in the CoECC (Art 35) appropriate and the implementation of their cybercrime convention feasible. Similarly, in Africa, having set up the CERTs in Ivory Coast in 2010 and then passing laws related to cyber security and data protection in 2012, the national CERT received 1,892 incidence reports and investigated all cases resulting in 71 arrests and 51 convictions for cyber security-related crimes (Musa, 2011; Wanjiku, 2013).

To pass the AUCSCPDP when only 11 of 54 AU members have established CERTs will make the implementation of the convention practically more difficult. To begin, the setting up of a Continental CERT comparable to the European Information Security Agency (ENSIA)[45], which the convention does not do, would have subsequently facilitated the establishment of national CERTs in each AU member state (Uchena, 2012). This absence of a continental CERT[46], which would drive a concerted effort to establish and nourish the national CERTs provided for in the AUCSCPDP, will frustrate implementation efforts. This is aggravated by the reality that most African countries do not have a good record of establishing legal initiatives in reasonable time (Uchena, 2012: p. 128).

[45] This intergovernmental organisation is a model contact centre of excellence for all EU Member States and all European institutions (public and private) dealing with network and information security. It disseminates information, technical advice and standards for good practices on emergency and incidence response on cyber crime and threats in Europe.

[46] Note that the African information security industry initiative - (Africa-CERT) already operates as an international team of trusted African computer incident response teams with a view to achieving cooperation in addressing cyber security issues by enhancing private sector participation in Africa. However, it is doubtful whether coordinating public sector and national efforts and responses to cyber security without a legal status in the DAUCCSC. For more information, see AfricaCERT <http://www.africacert.org/home/about-africacert.html>.

The Inadequacy of prosecutorial / judicial capacity for cyber crime: A pitfall for AUCSCPDP

Legal initiatives aimed at prosecutorial and judicial capacity-building for cybercrime are currently in dire need across Africa and will constitute a pitfall of implementation of the current format of the AUCSCPDP. Art 26(4) provides that each AU member states should conduct educational and training aimed at cyber security. An enforcement of the current AUCSCPDP is only logically and strategically possible if investigators, prosecutors and judges in Africa are educated on key aspects of cybercrime and cyber security (ITU, 2012). Research (UNODC, 2013) indicates that less than 50% of African countries currently have adequate capacity for effective cyber forensics. In contrast, 80% of countries in Europe and Asia have adequate capacity for cyber forensics, a contrasting situation that makes the CoECC more implementable than the AUCSCPDP (UNODC, 2013).

The contrasting situation is further demonstrated in that 80% of prosecutors in developed countries exhibit skills in IT above intermediate level and the prosecutors are able to access and use sophisticated ICT devices needed for effective cybercrime prosecution (UNODC, 2013). In developing countries 60% of prosecutors reported most basic or no ICT skills and of all prosecutors that have specialized skills in cybercrime prosecution, only a quarter had access to sophisticated devices needed for effective work (UNODC, 2013). More effort at organising workshops, short courses and other forms of accredited training, led by governments of AU member states to augment the overall capacity of prosecutorial and judicial staff that will engage with cybercrime, must accompany implementation of the AUCSCPDP.

Public-Private Partnership/ wider stakeholder engagement: A threat to Promulgation of the AUDCCSC

Public-private partnerships and stakeholder engagement are central to cybercrime prevention (ITU, 2012; UNODC, 2013). There is a need for government efforts to involve Internet Service Providers, Website hosting providers, banking, academia, and companies (e.g., telecommunications, computer software, and hardware companies) to guarantee an effective policy strategy and effective promulgation of cybercrime laws within and among countries. Ample stakeholder involvement in cyber security legislation facilitates information sharing, case tracking assistance, electronic evidence collection assistance, and benchmarking of good technical practices aimed at cybercrime prevention and prosecution. More to these, private stakeholders support international cybercrime policies / laws by raising public awareness, which is a crucial element for effective promulgation of municipal and international cybercrime laws. For example, since 2011, Google's *Good to Know* programme (conducted in 40 languages) is an awareness raising campaign that gives tips on online security specifically, on features such as cookies and IP addresses to the public through newspapers, magazines and public transport (UNODC, 2013). Similarly, Disney ran a TV and Website campaign aimed at educating 100 million children and parents on cyber security across countries in Europe, the Middle East and Africa (UNODC, 2013). Notwithstanding the enormous potential for collaborating with private stakeholders to ensure better cyber security in Africa, 60% of African countries reported lack of public-private partnership for cyber security on the continent, a reversed picture for Europe and America (UNODC, 2013).

Although Art 26(3) and Art 28(4) of the AUCSCPDP provides for public private partnerships, the entire process to draft the convention has precluded public private partnership and a wider

stakeholder engagement within Africa. DotConnectAfrica, commenting on the DAUCCSC (the January 2013 draft), holds that;

> interventions that are of a continental or global levels that require signing of such conventions must be properly drafted and understood by all the stakeholders, this includes the governments, businesses, academia and citizens… (2013, NP).

Conclusion and Recommendations

With the use of documentary reviews, surveillance of media coverage, and observations on cyber security across the globe, this critical assessment has examined the aptness of the AUCSCPDP with reference to current the African political, social and economic context. By benchmarking the Council of Europe Convention on Cybercrime (CoECC), the paper assesses the substantive and procedural aptness of the AUCSCPDP in relation to the following objectives: *to protect the rights of persons in data gathering and processing; to create legal and institutional mechanisms for the exercise of Human Rights in cyberspace; and to protect the survival and efficacy of institutions against cyber threats and attacks*. In relation to the African context, this critique assesses the feasibility of the AUCSCPDP with regard to available international co-operation measures, technical measures, prosecutorial capacity and multi-stakeholder cooperation.

The assessment concludes that in terms of the scope of substantive legal provisions, the AUCSCPDP is the most comprehensive continent-wide cybersecurity convention on the globe. Unlike any other cybersecurity convention on the globe the AUCSCPDP is more holistic, with provisions covering: electronic commerce (contractual obligations of electronic providers of goods/ services and vulnerability testing of online services); data protection issues; illegal online content (especially relating to pornography, xenophobia, ethnic or racist based attacks); cybercrime; and other aspects of cybersecurity policy

involving education and international cooperation. The objectives and comprehensive nature of the AUCSCPDP notwithstanding, there is ample room to fine tune the provisions to make it better aligned to the spirit of the convention and to the context of Africa.

However, the AUCSCPDP seems to have been rushed over, resulting in articles crafted in ways that will inadvertently undermine values that the convention sought to protect such as rights relating to privacy and free expression. The use of words with elusive meanings such as 'public interest, state security' in relation to retrieving, processing or storing computer data or criminalising online communication is, within the current African political context, vulnerable to invasion of privacy and to the lack of freedom of expression.

This paper shows that almost all of the values sought after by the AUCSCPDP resonate with the African experience of cybercrime but that the value of preserving the survival and sovereignty of African states highlighted in the DAUCCSC (the January 2013 draft) lacks evidence when assessed with regard to the manifesting trend of cyber threat and crime urgent measures. The emergency powers created by the AUCSCPDP violate privacy and free speech under the guise of addressing exceptional circumstances – i.e., when ICT poses a threat to state survival and 'public interest' in Africa – lacks evidence as reviewed in the current trend of cybercrime across Africa. As an organisation whose membership accommodates diverse forms of governments ranging from democrats to dictators, the urgent call and emergency powers set up to avert such virtual threats in the AUCSCPDP is already an alarm of curtailment in civil liberties within the AU. Policy analysis on this issue (Duncan, 2013) basing on the African context posits that such emergency powers gradually strengthen beyond their original scope, then get justified and legitimised to become everyday rule of law - the

emergency becomes permanent and the exemption the rule, the sun then fails to set on the sunset clauses.

Additionally, provisions related to aggravation and corporate liability are crafted, albeit inadvertently, in ways that will impose unjustified legal burdens on individuals and corporations, thereby extremely depicting 'legislative overkill' that will adversely affect online economy. The procedural provisions relating to interfering with online traffic or content data, issuing search and seizure warrants in a bid to avert cyber threat and offences permit inappropriate and broad ongoing investigation mandates to judges. Also, by not providing a model law on cybercrime, it precludes the strategic rationale of the AUCSCPDP to harmonise national legislations on cybercrime. As such the AUCSCPDP inadvertently creates high probability or grounds for conflicting laws over cybercrime issues among AU member states.

More so, the transnational nature of cybercrime and the lack of provisions relating to jurisdiction and extradition over cybercrime in the AUCSCPDP will make international co-operation unfeasible within Africa. Furthermore, considering that only Mutual Legal Assistance is provided for to aid international co-operation on cybercrime within the AU, that there is a lack of human resources (e.g. trained prosecutors) and of sufficient technical capacity (e.g. cyber forensics), and that there is a limited culture of multi-stakeholder cooperation relating to cyber security, the AUCSCPDP runs the risk of being highly unfeasible for providing confidence in cyberspace.

For a more effective African convention for confidence and security in cyberspace, the draft would benefit from the following recommendations. First, the processing of private and personal data of individuals without consent or the processing of such data by authorisation of the Public Protection Authority, as per the DAUCCSC, may benefit from clarifying or

substituting the concepts 'public interest and state security' in the following ways:

- That the processing of personal data of public interest may be conducted not 'especially for historical, statistical or scientific purpose' as the current draft spells out but may be conducted, *specifically*, *for historical, statistical or scientific purpose*.
- That the processing of personal data on behalf of the state for reasons of 'state security, defense or public security' would not be equivocal if the processing of personal data on behalf of the state is for the reason of *threats to critical information technology infrastructures safeguarding the defense of the state*.
- That the processing of personal data without consent to 'execute a mission of public interest' would be unambiguous if it reads as, *execute a mission aimed at protecting the public from imminent physical, social, cultural or economic harm*.
- That the processing of sensitive data should not be done on grounds to 'execute a mission of public interest' but categorically, to *execute a mission aimed at protecting the public from imminent physical, social, cultural or economic harm.*

These aforementioned suggestions will enhance the individual right to privacy within the AU member states, underscoring the AUCSCPDP rationale for legislating the protection of personal and sensitive data.

Second, the inadvertent violation of freedom of expression, granting the investigating judge power to order the interception of traffic and content data on the basis of 'where the imperatives of information so dictate' could be rephrased to reflect the spirit and objective of the AUCSCPDP of protecting fundamental freedoms online. To suggest, *the investigating judge may intercept traffic or content data in the pursuit of electronic evidence or to facilitate the*

prosecution of a serious crime specified in the municipal cybercrime legislation of AU member states.

Third, the use of aggravation and the imposition of additional punishment for any sort of crime involving the use of ICT in the AUCSCPDP could be maximised if it is allowed to be a way of letting all AU member states to embed the spirit of the convention against cybercrime into each local context. To this end, *each member state* could be allowed *to enact legislative provisions to create as aggravation, crimes specified in their municipal cyber legislation, which are deemed most devastating to local context or local efforts to guarantee cybersecurity.*

Fourth, in line with the AUCSCPDP objective of harnessing e-commerce, the limitless liability put on corporations for cybercrimes committed through their platform needs revision. To this end, the AUCSCPDP may be rephrased to impose liability on *all corporations (both public and private)* for cybercrime committed on their platform *if the crime accrues benefit directly to the corporation or if the crime is a result of negligence or the deliberate omission of cyber security measures by the corporation.* Additionally, the AUCSCPDP could better support corporations in the use of ICT for commerce and development by enjoining *each member state to limit corporate liability in their municipal legislation to criminal, civil or administrative sanctions or measures.*

Fifth, the high probability for the abuse of broad powers for cybercrime investigation and trials by judges in the AUCSCPDP needs to be checked. To meet this need, *the* AUCSCPDP *may permit search and seizure warrants; interception of traffic and content data; or the retrieval or storage order for computer data by an investigating judge for specified purposes*. These purposes could include: (1) *gathering electronic evidence for a cybercrime based on sworn in evidence, an affidavit, or police investigation reports; (2) prosecuting cybercrime, (3) sentencing for cybercrime; (4) request from a state party, exercised in accordance with international co-operation measures of the* AUCSCPDP.

Sixth, there is *need for the* AUCSCPDP *to enjoin member states to enact provisions addressing the issue of jurisdiction over cybercrime*. Such provisions, whether based on the principles of territoriality, active or passive nationality, habitual residence or addressing offences committed on board a ship flying the flag of a member state or an aircraft registered in a member state, will enhance international cooperation over cybercrime. To further enhance international cooperation among the AU member states, *the* AUCSCPDP *should include provisions addressing extradition requests relating to cybercrime and cyber threats* to beef up the current provisions on international cooperation in the convention.

To augment or provide capacity for harmonizing cyber legislation in each AU member state; to aid efforts in the establishment of CERTs for each AU member state; and to coordinate or support public-private partnerships to raise awareness, issue early warnings and develop technology devoted to cybersecurity, there is need for an African convention to provide for a continent-wide institution. If it were modeled after the European Security Information Agency (ENSIA)[47], it will make implementation of the DAUCCSC more effective. While these recommendations do not pretend to perfect the DAUCCSC, they serve as alternatives to support the values and objectives that underpin the convention.

[47] "The agency serves as a centre of excellence for Member States of the European Union and European institutions in network and information security. It renders advice and recommendations on cybersecurity and also disseminates information on standards for good practices. The ENSIA also facilitates contacts between EU Member States, European institutions, and private business and industry actors, and has also been active in promoting cybersecurity in developing countries" (Uchena, 2012, p. 129).

REFERENCES

African Union, 2014. *African Union Convention on Security in Cyberspace and Personal Data Protection.* [Pdf] Addis Ababa: Yedaly Malabo. Available at: <http: //pages.au.int/sites/default/files/en-AU%2520Convention%2520on%2520cybersecurity%2520pers %2520Data%protec%2520AUCyC%2520adopted%2520Malabo .pdf&sa [Accessed 31st August 2016] .

African Union, 2013. *Draft African Union Convention on the Confidence and Security in Cyberspace.* Available at: <http://www.au.int/en/cyberlegislation> [Accessed 7th February 2012]

Agence France-Presse, 2013. *Tech-backed Coalition Makes Transparency Push Global.* Available at: < http://phys.org/news/2013-09-tech-backed-coalition-transparency-global.html> [Accessed 7th July 2013].

Mohammed, A., 1995. *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Boulder: Lynne Rienner.

Brechbul, H., Bruce, R., Dynes, S. and Johnson, M. E., 2010. Protecting Critical Information Infrastructure: Developing Cybersecurity Policy, *Information Technology for Development*, Vol. 16 (1), pp. 83-91.

Brian, L.J., 1992.The Insecurity Dilemma: National, Regime, and State Securities in the Third World. In: L.J. Brian, ed. 1992. *The Insecurity Dilemma: National Security of Third World States*. Boulder: Lynne Rienner, pp.11 – 35.

Chertoff, M., 2008. The Cyber Security Challenge, *Regulation and Governance*, Vol. 2 (4), pp. 480-484.

Chawe, M., 2013. *Cyber crime costs Zambian banks $4m, Africa Review.* Available at: <http://www.africareview.com/News/Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html> [Accessed 22nd June 2013].

Colvin, M., and Cooper, J. eds., 2009. *Human Rights in the Investigation and Prosecution of Crime*. Oxford: Oxford University Press.

Harrison, C. and Paganini, P., 2012. *Joining Hands against Cybercrime in Africa: Security Affairs.* Available at: <http://securityaffairs.co/wordpress/10131> [Accessed 11th July 2013].

Harrison, C. and Paganini, P., 2013. *Africa – Cybercrime has turned the web as a hub of evil: Security Affairs.* Available at: <http://securityaffairs.co/wordpress/17919/cyber-crime/cybercrime-turned-web-hub-evil.html> [Accessed 23rd September 2013].

Council of Europe, 2001. *Convention on cybercrime*. Available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.html> [Accessed 1st May 2013].

Common Market for Eastern and Southern Africa, 2011. *Cybersecurity Draft Model Bill.*

Dot Connect Africa, 2013. *Comments to the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.* Available at: <http://dotafrica.blogspot.com/2013/10/dotconnectafrica-comments-to-draft.html> [Accessed 1st November 2013].

Duncan, J., 2013. *Cybercrime in South Africa: A Crisis, Mail and Guardian.* Available at: <http://mybroadband.co.za/news/security/80589-cybercrime-in-south-africa-a-crisis-expert.html> [Accessed 30th July 2013].

Economic Community of West African States, 2011. *Directive on Fighting Cybercrime.* [Pdf] Abuja: Olugbenga Ashiru. Available at : <http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Cybercrime.pdf> [Accessed 6th June 2013].

European Union, 2013. Directive on Attacks against Information Systems. Available at :< http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2013-321#BKMD-4> [Accessed 8th July 2013].

Feintuck, M., 2004. *The 'Public Interest' in Regulation***.** Oxford: Oxford University Press.

Glancy, J. D. 1979. Invention of the Right to Privacy, *Arizona Law Review*, 21(1), pp. 1-39

Gunness, A., et al, 2008. *Cybercrime and Computer Misuse Cases in Mauritius and the African Region.* Available at: <http://www.slideshare.net/curiousEngine/cybercrime-and-computer-misuse-cases-presentation> [Accessed 1st July 2013].

ICB4PAC, n.d. *Model Policy Guidelines and Legislative Texts on Cybercrime.* [Pdf] Geneva: International Telecommunication Union Available at: <http://www.itu.int/ITUD/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf> [Accessed 1st January 2012]

Ilie, M., Mutulescu, A-S.; Artene, D. A.; Bratu, S.; Făinişi, F., 2011. International Cybersecurity through Cooperation, *Economics, Management & Financial Markets,* Vol. 6 (2), pp.438-450.

International Telecommunications Union, 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Available at: <www.itu.int/ITUD/cyb/cybersecurity/legislation.html> [Accessed 5th July 2013].

Jaishankar, K., 2011. Expanding Cyber Criminology with an Avant-Garde Anthology. In: k., Jaishankar, ed. 2011. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton: FL: CRC Press.

Job, B. L., 1992. The Insecurity Dilemma: National, Regime and State Securities in the Third World. In Job, B. L. ed., *The Insecurity Dilemma: National Security of Third World States*. Boulder, CO: Lynne Rienner, pp.11-35.

Kabay, E. M., Bosworth, S., and E. Whyne. eds., 2009. *Computer Security Handbook,* 5th edn. New York: Wiley.

Kigerl, A. 2011. Routine Activity Theory and the Determinants of High Cybercrime Countries, *Science Computer Review,* Vol. 30 (4), pp. 470-486.

Musa, S. B. M., 2011. *Computer Incident Response Team: Role in combating cybercrime*. [Pdf] Malaysia: Jalan IMPACT. Available at: <http://www.itu.int/ITU-D/asp/CMS/Events/2011/CyberCrime/S6_Mohamad_Sazly_Musa.pdf> [Accessed 8th September 2013].

Organization for Economic Co-operation and Development, 2005. *Task Force on Spam: Spam Issues in Developing Countries*. Paris: Directorate of Science Technology and Industry, Committee on

Consumer Policy and Committee for Information Computer and Communications Policy.

O'Reilly, K., 2013. *South African Law Coming to Grips with Cyber Crime*. Available at: <http://www.saflii.org/za/journals/DEREBUS/2013/75.html > [Accessed 20th June 2013].

Rosenzweig, P., 2012. The International Governance Framework for Cyber Security*, United States Law Journal*, 37(2).

Skinner, W. F., and Fream, A. M., 1997. A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 4(34), pp.495-518.

League of Arab States, 2010. *Arab Convention on Combating Information Technology Offences*. Cairo: The Arab Republic of Egypt.

League of Arab states, 2004. *The Arab Model Law for E-transactions and E-Commerce*. Cairo: The Arab Republic of Egypt.

Uchenna, J. O. 2012. A discourse on the perceived defects of the draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security, *Journal of Computer, Media and Telecommunications Law,* Vol. 17 (4), pp.112-143.

United Nations, 2011. Freedoms of opinion and expression. *International covenant on civil and political rights*. [Pdf] Geneva: Human Rights Committee. Available at: <http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf > [Accessed 11th July 2013].

United Nations Office on Drug and Crime, 2011. *Monitoring the Impact of Economic Crisis on Crime*, Vienna: *Rapid Impact and Vulnerability Assessment Fund*. [Pdf] Vienna: UNODC Statistics

and Surveys section. Available at :< http://www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf> [Accessed 11th July 2013].

United Nations Office of Drug and Crime, 2013. *Comprehensive Study on Cybercrime*. New York: United Nations.

United Nations, 2014. *The Right to Privacy in the Digital Age: Annual Report*. [Pdf] Geneva: Office of the High Comissioner for Human Rights. Available at: < http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> [Accessed 11th January, 2015].

United Nations Special Rapporteur on Freedom of Opinion and Expression, et al., 2006, *International Mechanisms for Promoting Freedom of Expression: Joint Declaration*. Available at: <http://www.osce.org/fom/23489> [Accessed 11th July 2013].

Warren, D., S., and Brandeis, D., L., 1890. The Right to Privacy, *Harvard Law Review* 4(3), pp. 193-220

Wanjiku, R., 2013. *Africa Increases Cybersecurity Efforts*: *IT World.* Available at: <http://www.itworld.com/security/362093/africa-increases-cybersecurity-efforts> [Accessed 1st July 2013].

Yankey, A., 2012. *The AU Draft Convention on Cybersecurity and E-transactions*: *Cooperation against Cybercrime Conference*. [Pdf] Strasbourg: Auguste Yankey. Available at: <http://www.coe.int/t/dghl/cooperation/economilccrime/cybercrime/cy_octopus2012/presentations/Update_AU_convention_CyberSec_Strasbourg_presentation.pdf> [Accessed 6th July 2013]

Yankey, A., 2013. *African Union Perspectives on Cybersecurity and Cybercrime Issues: The AU Draft Convention on Cybersecurity and related Activities*. [Pdf] Yaoundé: *Commonwealth Telecommunication Organization*. Available at: <http://www.cto.int/media/events/pst-ev/2013/Cybersecurity/Auguste%20Yankey.pdf> [Accessed 1st July 2013].

List of Back Issues

Author(s)	Title	Year
Joseph Kisekka	A Return to the Past: Three views of nation building in Uganda	2012
Tabitha Naisiko, Godfrey Netondo, Lucy Maina and Fuchaka Wasswa	Corporate Social Responsibility approaches in enhancing environmental quality and community well-being in Busoga: The case of Kakira Sugar Works Limited.	2012
Maximiano Ngabirano	Typology of victimhood: The concept of justice between the biblical conflict of Cain-Abel and the Great Lakes Conflict of Hutu-Tutsi	2008
Remigius Munyonyo	Village reflections and dialogue on gender and HIV/AIDS using human rights based and visionary approaches to development in a Ugandan context	2007
Stephen Agaba	Participatory justice: An overview of Gacaca Courts in Rwanda	2006
S.M Najjuma and Diana T. Kyarugahe	Studying and parenting: Experiences of student mothers in Ugandan Universities	2006
Jane Osongo	Patriarchy and the subordination of women among the Abasugi of Western Kenya	2005
Peter Kanyandago and Levis Mugumya (eds.)	Celebrating 10 years of academic excellence(Mtafiti Mwafrika Special Edition)	2005
Tabitha Naisiko	Traditional African Religions (TARs): On	2005

	HIV/AIDS, health and morality in Africa.	
Sperenza Namusisi	Interdisciplinarity in Uganda 's education system	2005
Emmanuel Katongole	Where is Idi Amin? On violence, ethics and social memory in Africa.	2004
Remigius Munyonyo	An evaluation of Uganda's plan for Modernization Agriculture(PMA) using the right to adequate food(RAF) and sustainable co-existence(SCE) approaches	2004
Maximiano Ngabirano	Grand narratives of the Great lakes region of Africa and their contribution to current conflicts.	2003
Remigius Munyonyo	Sustainable development in the dock: A need for sustainable co-existence in Africa	2002
Prisca Kobusingye	African dual career couples: Problems and challenges of the modern business environment.	2001
Maurice Mukokoma	The Motivation Dilemma: A case of Uganda	2001
Adela Barungi	The environmental question in Global Economics: The African story	1999
Remigius Munyonyo	Decentralisation in Uganda: Theory and practice	1999
Nduhukire-Owa-Mataze	Africa: a continent existing and entering a century in a sickbay. Part one: Africa's development paralysis	1999

Nduhukire-Owa-Mataze	Africa: a continent existing and entering a century in a sickbay. Part two: Myths and deceptions of African mal-development.	1999
Nduhukire-Owa-Mataze	Africa: a continent existing and entering a century in a sickbay. Part three: Globalization means death, renewed national liberation means survival	1999
Nduhukire-Owa-Mataze	The caging of African women: Towards a radical understanding of women's economic position in African societies today.	1999
Rosemann P.W.	Africa as the other of the West: Problems, challenges and chances	1999