ICRD

International Multidisciplinary Research Journal - ISSN 2424-7073
Legal Studies – (2019): Pages 33-38
©ICRD Publication

Towards a Framework for Analysing Impediments to Cyberlaw Compliance in Africa

Michael Kyobe
University of Cape Town, Cape Town, South Africa

Abstract

The rise in the level of electronic abuse has led to the establishment of regulatory measures by governments. However, regulation of cyberspace has presented several challenges for IT users and legislators. Cyberlaw reforms are complicated and lengthy, Users of IT face abuse and often responses to cyber-law violations are fragmented and unsatisfactory. In addition, there have been very few studies investigating what motivates compliance with cyberlaws across Africa. Existing research consists of articles and anecdotes and the regulatory compliance theory is under-developed. Consequently, little guidance is available on how to measure and ensure compliance with cyberlaws. This paper examines the factors influencing cyber-law compliance in Africa. The author discusses various theoretical works that explain non-compliance. A framework for analysing factors contributing to non-compliances developed. This framework is then used to identify impediments to cyberlaw compliance in selected African countries.

Keywords: Cyberlaw, Compliance, Impediments, Africa.

Introduction

The developments in the use of information technology in Africa have contributed to the escalation of cybercrime and non-compliance with cyber laws (Mwaita and Owor,2013).There have been very few studies investigating these challenges and their causes across Africa (Oluwo,2009).Consequently, the determinants and consequences of non-compliance are not widely known and little guidance is available on how compliance with cyberlaws may be achieved in Africa. The present study examines cybercrime legislation and compliance issues in Africa with a view to identify the influencing factors which might also serve to measure compliance with cyberlaws. The researcher decided to focus on countries with high and low levels of cybercrime and also at different stages in their cyberlaw reforms. These are South Africa, Kenya, Uganda, Rwanda and Nigeria. Nigeria and South Africa are among the top countries in Sub-Sahara Africa with high cybercrime rates (Oluwu, 2009). South Africa has more established cyber laws than other countries. Kenya and Uganda have recently developed their cyber laws but are increasingly threatened by cybercrime due to high mobile technology usage, high transactions rates and poor security awareness (ITU, 2014).Rwanda on the other hand is in early developmental stages (Mwaita and Owor, 2013).Google scholar and various online databases were used to identify papers on cyberlaw in Africa and the theoretical works on regulatory compliance. In the following sections, this paper presents national efforts toward cyberlaw reforms in the selected countries. The concept of regulatory compliance is then introduced and the theoretical works explaining why entities fail to comply are discussed. A framework for identifying influencers of regulatory compliance is developed and used to examine the factors contributing to non-compliance with cyber-laws in the selected African countries.

Literature Review

Cyberlaw reforms in selected African countries: South Africa has a number of laws regulating cybercrime. Prior to the enactment of the Electronic Communications and Transactions - ECT Act (2002) in South Africa, common law regulated crimes of defamation, indecency (online child pornography), crimen injuria (cyber-smearing) and cyber fraud (Madziwa and Sizwe,2015).However, the applicability of the common law to certain crimes e.g. crimes of assault, theft and extortion was found to be limiting by courts and prosecutors. In 2002, the ECT Act was enacted. The problems relating to cybercrime are addressed in Chapter XIII of the ECT Act, 2002. According to Michalson and Hughes (2005), this chapter introduces statutory criminal offenses relating to unauthorized access to data, interception of data, interference with data, and computer related extortions, fraud and forgery. The ECT Act does not exclude the application of other statutory or common law. Other legislations include the Regulation on Interception of communication related information Act 70, 2002, which regulates the interception of any communication in the course of its currency or transmission. The Financial Intelligence Centre Act (FICA) which provides that an accountable entity, may not conclude a business transaction with a client without having complied with certain information gathering and reporting duties. The Protection of Personal Information (POPI) Act is the first all-encompassing law that addresses information privacy and data protection in South Africa (POPI, 2013). Other countries in Africa have also developed cyberlaws similar to those of South Africa. Presently, Kenya has a cyberlaw framework articulated under the Kenya Information and Communication Act (KICA) – 2009 and the Kenya Communications (Electronic Transactions) Regulations passed in 2010(UNCTAD,2012).Cybercrime legislation in Uganda is mandated through the Electronic Transactions Act 2010;the Electronic Signatures Act 2010; and the Computer Misuse Act 2010 (UNCTAD,2012). Rwanda is in early stages of cyberlaw development. Specific legislation on cybercrime has been enacted through the law on Electronic Message, Signature and Transaction; and the draft ICT bill(ITU, 2014).In Nigeria, cybercrime is regulated through the Money laundering (prohibition) Act 2011; Advance Free Fraud & other related Offences Act 2006; Evidence Act 2001 and the Cybercrime Bill 2013(ITU,2014).

Compliance with Cyberlaws

While governments acknowledge the importance of cyberlaw reforms, adopting existing laws and compliance with them continue to be a major challenge for Africa (Quarshie, 2014; Olowu, 2009). Compliance is a state in which someone or an entity (e.g. an organisation or a nation) is in accordance with established guidelines, specifications, or legislation. Theories about compliance provide accounts of why institutions and individuals comply with or do not comply with laws and according to Grossman et al (2005), rationalist and normative models have been widely used to explain compliance.

Rationalist Theories: The rationalist model of domestic compliance posits that regulated individuals act rationally to maximize their economic self-interest (Jenny, Fuentes & Mosler, 2006). It assumes that an individual weighs the perceived probability of being detected and the severity of the expected sanctions (Jenny, Fuentes & Mosler, 2006). Rationalist argue that by increasing surveillance and sanctioning severity, compliance behaviour can be enforced. However, this model has several limitations. For instance, it does not consider social action based on values, beliefs or emotions. The assumption that self-interested actors calculate the costs and benefits of alternatives does not consider peoples' inabilities to calculate probabilities of compound and conditional events. In addition, reported failures by law enforcement agencies indicate the difficulties in enforcing deterrence (Olowu, 2009; Omeje and Githigaro, 2010).

Normative theories: The assumption that people obey the law because it is in their interest to do so fails to account for factors such as social influence, moral values and perceived legitimacy of the regulations (Tyler,1990; Grossman et al., 2005). The normative perspective on compliance held by the sociology literature is that laws that are developed and implemented fairly should be followed and that individuals and firms will comply if they believe the rules are legitimate and fairly applied. Similar views have been expressed in the public choice literature and psychological theories (Tyler, 1990).

Psychological and Sociological Theories: Psychological and sociological theories of rule compliance integrate individual and social factors (Jenny, Fuentes & Mosler, 2006). Individuals would comply because of a moral obligation to do the right thing. Social norms may exert pressure on an individual to comply in order to avoid being sanctioned by others. The perception of the legitimacy of rules is another factor influencing compliance. Rules that are compatible with local conditions, adequate and not interfering strongly with livelihood strategies are likely to be obeyed (Jenny, Fuentes & Mosler, 2006).Social learning theories emphasise the importance of learning through symbolic interaction with others (Jenny, Fuentes & Mosler, 2006).It is claimed that non-offenders learn the values and norms that conform to convention, whereas offenders learn what is contrary to convention. Research in psychology and sociology therefore recognises the importance of cognitive and social learning processes, individual capabilities, group influence, cooperation, increased awareness and ability to address environmental influences, (Jenny, Fuentes & Mosler, 2006). Researchers maintain that non-compliance will occur mainly in situations where the regulated entity lacks capacity and commitment.

Biological and Biosocial Theories: Biological and biosocial theories argue that humans inherit a set of biological and genetically determined attributes that differentiate them across a continuum, whereby some will have greater propensity to break the law than others in certain conditions. Biosocial theories suggest that there is something inherently defective in the individual who fail to comply or who commit crimes. Researchers have established that the traits of conscientiousness and agreeableness may be strongly linked with an individual's intention to comply with cybersecurity policies (Major et al., 2006).

Research in the business and strategic management fields also shows that structural and organizational components of the firm influence compliance behavior (Malloy, 2003). Large firms have many characteristics that encourage compliance e.g. size, resources, skills, public image, while small sized firms are constrained by poor allocation of resources and limited capital to invest in appropriate technology. Organizations are also realizing the importance of enforcing compliance through good practices, e.g. by using professional and international standards such as ISO 27000 and BS7799-1, SOX and others.

Towards a Framework for Examining Compliance with Cyber-laws in Africa

The literature suggests that compliance with legislation is influenced by various factors. For instance, economic, psychological, sociological, professional, technological factors and biological factors, to mention but a few. There is however lack of consensus on whether these factors or motivations operate exclusively or in combination. Nielsen and Parker (2012) argue that lumping social and economic motivations does not adequately recognise the distinctive power of the individual motivations. They maintain that understanding these distinctive powers is crucial to determining the appropriate regulatory policy. They state that "any theory for explaining regulatory compliance behavior – and especially for suggesting policy responses to non-compliance – should be able to distinguish between situations where an individual or firm is intrinsically and individually motivated to voluntary comply and situations where some sort of social pressure (whether from an official regulator or third parties) is necessary to motivate compliance". While Nielsen and Parker's (2012) argument is valid, motivations are however complex and often do not operate exclusively, e.g. self-interest, duty, fear and trust may combine to influence response to regulation (Etienne, 2010). Etienne argues that if considered individually, one may overlook or fail to account for this complexity. How then does one capture the distinctive powers of the individual motivations without overlooking the complexities of compliance behaviours? In the present study, the researcher proposes a framework (see Figure 1 below), that blends various cyberlaw compliance influences. It recognises the significance of the individual motivating factors but also acknowledges the potential interaction between them, represented here by the circle. The combined effect of these factors (or prioritised factors) then determines compliance with cyberlaws.

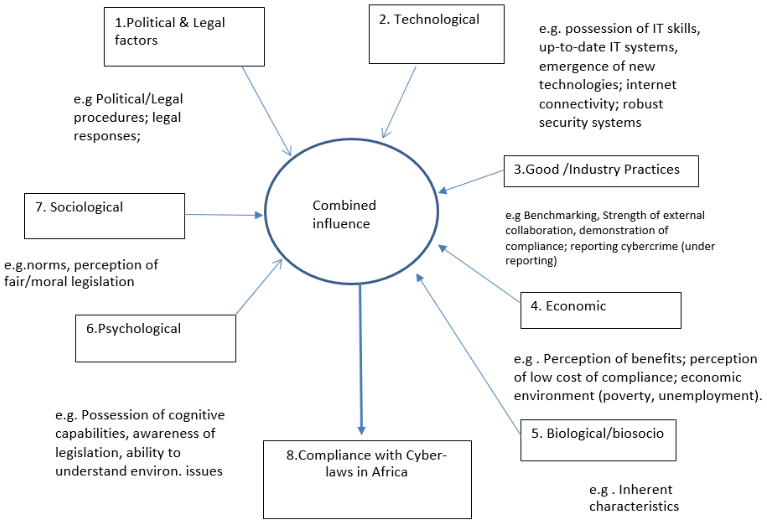
1.Political & Legal factors
2. Technological
e.g. possession of IT skills, up-to-date IT systems, emergence of new technologies; internet connectivity; robust security systems
e.g Political/Legal procedures; legal responses;
3.Good /Industry Practices
Combined influence
7. Sociological
e.g Benchmarking, Strength of external collaboration, demonstration of compliance; reporting cybercrime (under reporting)
e.g.norms, perception of fair/moral legislation
4. Economic
6.Psychological
e.g . Perception of benefits; perception of low cost of compliance; economic environment (poverty, unemployment).
e.g. Possession of cognitive capabilities, awareness of legislation, ability to understand environ. issues
5. Biological/biosocio
8.Compliance with Cyber-laws in Africa
e.g . Inherent characteristics

Figure 1: Factors influencing compliance with cyber-laws in Africa

Analysis of Compliance Issues in Africa Using the Proposed Framework

The researcher will now use the above framework to examine the factors influencing compliance with cyberlaws and the interactions between them in the selected African countries.

1. *Political and Legal factors*: Political and legal factors (at national or international) level may influence law reforms in a country or region resulting in compliance or non-compliance with the laws. Several political and legal challenges East African countries have experienced in their cyberlaw reforms have been reported. These include difficulties in drafting the reforms, unwillingness of political leaders to drive the process, commitment of limited resources to these projects, business attitudes and practices (Mwaita and Owor, 2013; UNCTAD, 2012; East African Internet Governance Forum, 2011). In Uganda, the bureaucratic set up has made cyber law reforms lengthy while in Kenya, delays in combating cybercrime were attributed to the failure to develop an all-inclusive legislation which is also compatible with international standards (Omeje and Githigaro, 2012; EA Internet governance forum, 2011). Cassim (2010) identified ambiguities and inconsistencies in South African cyberlaws. For instance, he reports that while section 15 of the ECT Act facilitates the admission of information in electronic format, the criminal sanctions in the Act are inadequate. He observed that such limitations have led the courts and prosecutors to adopt a cautious approach towards cybercrime cases. Snail (2008) asserts that section 90 of the ECT Act presents many jurisdictional challenges pertaining to cybercrime. In Rwanda, the lack of expertise in cyber-law threatens the reforms (EA Internet governance forum,2011). In Nigeria, the absence of a legal and regulatory framework that clearly recognises the pervasiveness of cybercrime and one that prescribes strong penalties escalates cybercrime (Maitanmi et al., 2013).
2. *Technological*: The developments in technology in many African countries have led to higher risk, rampant corruption and escalation of cybercrime (UNCTAD,2012; Olowu, 2009; Maitanmi et al., 2013). Kshetri (2010) argues that most ICT products targeted for developing countries are low-cost versions. These lack advanced security features and are vulnerable to cyber violations. Cyber vulnerability in Nigeria has been attributed to weak technical and business practices, use of outdated anti-virus software and unsecured networks (Maitanmi et al., 2013).Rwanda also identified lack of technical expertise to handle cyber and legal related aspects of law reforms (EA Internet governance forum,2011; Mwaita and Owor, 2013).Lack of Internet connections especially in the rural areas of Africa and clear ICT policies impact on IT education and risk awareness which subsequently affect compliance with cyberlaws (Grobler and van Vuuren, 2010).
3. *Good practices*: Compliance can be achieved through good practices, standardisation, benchmarking and other quality assurance processes. The current lack of standardized procedures in Africa have influenced the effectiveness of cybercrime investigation techniques and court decisions (Grobler and van Vuuren, 2010; Olowu, 2009). Reports suggest that many countries in Africa have not ensured good IT management practices. The cyber wellness reports (ITU, 2014) indicate that the countries examined in this study do not have officially recognized benchmarking mechanisms to measure cybersecurity development and the effectiveness of cyberlaw reforms. They also do not have officially recognized national or sector-specific research and development (R&D) programs for cybersecurity (ITU,2014).
4. *Economic*: Guerra (2009) argues that crime can be extremely profitable, has low overhead and a little risk of being prosecuted. He shows how the global recession has affected security through job loss resulting in disgruntled workers, the rise in available computer talent with no jobs, increase in demand for counterfeit products and the diminishing ability to prosecute. Youth involvement in cybercrime in Nigeria has been attributed to urbanization, the high unemployment rate, harsh economic conditions, greed, and the uncontrollable desire for massive wealth (Olayemi, 2014). In East Africa, similar factors accounting for insecurity and subsequent non-compliance with the laws have been identified. These include unemployment among the youth, poverty, police collusion with criminals, drugs and peer influence, corruption and the collapse of the family institution (Omeje and Githiagaro,2012:5).
5. *Biological factors*: Aransiola and Asindemade (2011) studied young cybercrime perpetrators in Nigeria. They found that they make use of voodoo, i.e., traditional supernatural power to commit crime. In another study involving 199 males and 198 females in Nigeria, Ojedokun and Idemudia (2013) observed that emotional intelligence moderated the relationship between cyberbullying and personality

factors like psychoticism, extroversion and neuroticism. Olapegba and Idemudia (2012) also found that while dispositional factors such as openness to experience, agreeableness, and conscientiousness did not independently predict smuggling behaviour in Nigeria, extraversion and neuroticism did so.

6. *Psychological and (7) sociological factors*: Researchers have also found that users, law enforcement agents and policy makers in many African countries still lack legal expertise, awareness of the adverse impact of cybercrime and measures to prevent it(EA Internet governance forum,2011; UNCTAD,2012).While online gambling is permitted in Kenya, it is perceived to be immoral in Nigeria and South Africa, although South Africa appears to be moving towards legalising it. Pornography is immoral in Uganda and has been prohibited by the Anti-Pornography Act of 2014. The National Media Monitoring Committee has called on the Communications Commission of Kenya (CCK) to regulate pornography(Mbote,2013).Lack of trust in e-commerce and in the law enforcement agents are major issues in most of the countries studied and this contributes to non-compliance (Omeje and Githigaro, 2012;African Minds for the African Police Oversight Forum, 2008). In Uganda, the police was ranked the highest corrupt public service provider, while in Nigeria the police has been accused of corruption and brutality, arbitrary arrest and detention and impunity (African Minds for the African Police Oversight Forum, 2008).In Kenya, there is a lack of confidence in the ability of law enforcement agencies to handle cybercrime incidents (Omeje and Githigaro, 2012).

Conclusion

This study confirms that African countries are still struggling to ensure compliance with cyberlaws. Major challenges are experienced at the developmental and implementation stages of cyberlaw reforms. In most countries there are concerns relating to ambiguity in the laws, lack of commitment by legislators and lack of awareness of law and severity of cybercrime. The study highlights the importance of cyberlaw harmonisation and the need to consider biological influences which are often ignored in compliance models. This study contributes to the development of the under-developed regulatory compliance theory (Etienne,2010). The proposed compliance framework can be used to understand the effects of the major factors influencing compliance and the complexities in their interactions. It also provides a basis to measure cyberlaw compliance. Since combination of multiple motives (or selected motives) are perceived to explain compliance behaviour more effectively, future studies can adopt a configurational approach to measure this combined effect. Used with cluster analysis, combinations of factors or motivations that influence compliance the most can be determined.

References

African Minds for the African Police Oversight Forum (2008). An audit of Police oversight in Africa, http://www.apcof.org/files/apcof_police_oversight_web.pdf

Aransiola JO, Asindemade SO. Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. Cyberpsychology, Behavior, and Social Networking;14: 759-763. 2011.

Cassim F. Addressing the Challenges posed by Cybercrime: a South African Perspective. Journal of International Commercial Law and Technology; 5:118-123. 2010.

East African Internet Governance Forum (2011). Harmonization of Internet Policies in the Region of East Africa http://www.intgovforum.org/cms/2011/NationalregionalIGFreports/EASTAFRICAIGFreport.pdf.

Etienne J. The impact of regulatory policy on individual behaviour: A goal framing theory approach. Discussion Paper No. 59. Centre for Analysis of risk and regulation;http://eprints.lse.ac.uk/36541/1/Disspaper59.pdf. 2010

Grobler M, van Vuuren JJ. Broadband broadens scope for cyber crime in Africa. Information Security for South Africa (ISSA); Johannesburg, 2-4 August, 2010.

Grossman D, Zaelke D. An introduction to theories of why states and firms do (and do not) comply with law; INECE Conference Proceedings. INECE. www.inece.org/conference/7/vol1/index.html. 2005.

Guerra P. How economics and information security affects cybercrime and what this means in the context of a global recession. http://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-SLIDES.pdf. 2009.

International Telecommunications Union (ITU). http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles. 2014

Jenny A, Fuentes H F, Mosler H. Psychological Factors Determining Individual Compliance with Rules for Common Pool Resource Management: The Case of a Cuban Community Sharing. Hum Ecol; DOI 10.1007/s10745-006-9053-X, http://www-siam.emp-eaw.ch/pdfs/30.pdf. 2006

Kshetri N. Diffusion and Effects of Cybercrime in Developing Economies Third World Qrt, 31;1057 – 1079. 2010.

Madziwa S, Sizwe S. Cyber Crime In South Africa.http://www.hg.org/article.asp?id=5351. 2015.

Maitanmi O, Ogunlere S, Ayinde S, Adekunle Y. Cyber Crimes and Cyber Laws in Nigeria, The International Journal Of Engineering And Science (IJES); 2: 19-25. 2013.

Major DA, Turner JE, Fletcher TD. Linking proactive personality and the Big Five to motivation to learn and development activity. Journal of Applied Psychology; 91:927-935. 2006.

Malloy TF. Compliance and the firm. Temple Law Review; 76: 451-457. 2003.

Mbote K. Kenya urged to act on internet pornography, considers total ban http://www.humanipo.com/news/6392/kenya-urged-to-act-on-internet-pornography-considers-total-ban/. 2013.

Michalson L, Hughes,B. Guide to the ECT Act.http://www.michalsons.co.za/guide-to-the-ect-act/81. 2005.

Mwaita P, Owor M. Workshop Report on effective cycbercrime legislation in E. Africa, Dar es salaam Tanzania, 22-24 August, 2013.

Nielsen V, Parker C. Mixed Motives: Economic, social and normative motivations in business compliance. Law and Policy; 34:428-462. 2012.

Ojedokun O, Idemudia ES. The Moderating Role of Emotional Intelligence between PEN

Olapegba PO, Idemudia ES. Dispositional and Contextual Factors Predicting Smuggling Behaviour among Smugglers in Border Areas in Nigeria, Psychology; 3: 59-64. 2012.

Olayedemi O. A socio-technological analysis of cybercrime and cybersecurity in Nigeria. International Journal of Sociology andAnthropology, 6(3): 116-125. 2014.

Olowu D.Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case foran Inclusionary Framework for Africa. Journal of Information, Law & Technology;1: 1-18. 2009.

Omeje K, Githigaro M. The Challenges of State Policing in Kenya, Peace and Conflict Review; 7:1.2012

Personality Factorsand Cyberbullying in a Student Population, Life Science Journal;10:1924-1930..2013

POPI Act. Protection of Personal Information Act. Department of Justice.http://www.justice.gov.za/legislation/acts/2013-004.pdf. 2013.

Quarshie HO. Using ICT to Fight Crime - A Case of Africa,Journal of Emerging Trends in Computing and Information Sciences; 5: 1 January. 2014

TylerTR. Why people obey the Law. New Haven: Yale University Press, 1990.

UNCTAD. HARMONIZING CYBERLAWS AND REGULATIONS: The Experience of the East African Community. http://unctad.org/en/publicationslibrary/dtlstict2012d4_en.pdf. 2012.