NINE NINE NINE:

e-GOVERNMENT AND THE CAMEROON CYBERSECURITY LEGISLATION 2010: OPPORTUNITIES AND CHALLENGES

Patricia Ngeminang Asongwe
Lecturer, Faculty of Laws and Political Sciences, University of Yaounde II, Cameroon

ABSTRACT: The EGOV.CM programme, led by the National Agency for ICT (ANTIC) aims to promote access to government information and services, provide IT support to the public administration reform programme, promote the objectives of national policies and provide an appropriate legal and regulatory environment. However, government and citizen reliance on ICTs presents a security challenge, given the emergence of cybercrime across the globe. This requires changes to legislation drafted before the electronic age. Outdated laws result in impunity, with the country a safe haven for cybercriminals, while e-government transactions may be unprotected and may therefore be discouraged. Cameroon's e-laws of 2010 (cybersecurity and electronic communications) provide a legal framework for the protection of ICT networks and critical infrastructures, creating an enabling environment for e-government services. These research notes highlight the importance of the e-laws for effective Cameroonian public administration, and discuss the challenges for implementation of e-government.

KEYWORDS:
Cameroon e-laws 2010, e-government in Cameroon, cybersecurity

BACKGROUND TO E-GOVERNMENT IN CAMEROON

The last 13 years have witnessed an era of initiatives to develop and harness the benefits of ICT for the nation's development. Mokube (2010) sketches a brief history of movement towards e-government, noting the following events. The 1998 laws (Telecommunications Law No 98/014 of 13 July 1998 and Telecommunications Law No 98/014 of 14 July 1998) provide the legal backing for ICT evolution in Cameroon. These laws brought an end to monopoly control in the telecommunication sector in Cameroon. They gave birth to telecom liberalisation and privatisation, ushering in new players in telecommunications and encouraging investment in ICT. Further progress in legislation was made in 2001, instituting minimum service standards in the telecommunications sector through a series of decrees laying down the modalities for the operation of telecommunications networks and the provision of telecommunications services (Law No 2001/0130 of 23 July 2001). These developments led to an opening up of citizens' and business demand for ICT availability.

The finalization of the National Programme for Governance and Strategic Management of the State (Cadre National d'Objectifs Strategiques) provided the foundation for e-government strategies. A draft e-government strategy, EGOV.CM was formulated as a collaborative exercise between ANTIC and the United Nations University (UNU) and presented for adoption in 2011.

A range of public institutions provide the foundation for development of ICT in government. The Telecommunications Regulatory Board (TRB) under the auspices of MINPOSTEL, the National Agency for ICT (ANTIC), the computer divisions in government departments and the National Centre for the Development of Computer Services (CENADI) are the relevant organisations and are all available online. Furthermore, major e-government initiatives were taken in relation to the computerisation of records, including state personnel and salaries (SIGIPES), public finances (SIGEFI), customs transactions (SYDONIA), transport titles (driving licence, car ownership) (SYSTAC) and electoral documents (ELECAM). The PRIMO project provides online tender documents (Mokube 2010; Kamga, 2011). Each of these e-administration programmes requires network security and ways of preventing or reducing cybercrime.

Equally important are initiatives in ICT infrastructure development, including establishment of RASCOM, to provide access to satellite resources and investment in access to the SAT3 undersea cable system for access to international bandwidth. There is ongoing deployment of approximately 3 200km of fibre optic cable nationwide, in partnership with Huawei.

The emerging reality is that the country's public administration is in transition to e-processes. If digital government is dawning for Cameroon's population of approximately 18 million people, then online security is important for resilience, continuity, sustainability and further development (Pollifroni, 2006; Asongwe, 2010).

Security is a challenge in all e-government processes. With the growing number of personal data devices and other sophisticated technology, criminals are becoming better able to conceal their actions. Protecting critical network infrastructures requires a comprehensive view of security that combines physical, digital and procedural components. These components provide the level of cybersecurity necessary to guard against the many known and unknown threats in cyberspace. Cameroon's businesses, government administration and society depend to a high degree on the efficiency and security of ICT. Cybercrime can affect service providers, banks, petroleum data insurances, the stock exchange and the communication sector. Compromise on one network can allow an intruder either direct access to a partner's private data or indirect access by allowing a back door into the partner's network. Thus, cybersecurity law covers the ICT sector as a whole, not only the e-government component.

The virtualisation of services creates a number of challenges in respect of security and confidence. Specific threats to cybersecurity include use of unsecured networks; misconfiguration of computer systems; poor user and administrator education; poor software design; network and system design issues; substandard operational procedures and protocols; weak passwords; and lack of awareness or indifference (Schechter, 2004).

HIGHLIGHTS OF CAMEROON'S E-LAWS

The 2010 e-laws regulate activities in Cameroon's cyberspace, dealing with cybersecurity and cybercrime in electronic communication, electronic commerce and electronic government (Republic of Cameroon, 2010a; Republic of Cameroon, 2010b). For development of Cameroon's e-government and information society, the protection of network infrastructure and e-services

is of paramount importance to cybercitizens. In the ongoing debate on cyberlaw, enhanced cybersecurity and governing regulations are not a luxury, but a necessity for Cameroon's e-government applications (Asongwe, 2011). Hence the laws are geared towards enhancing trust and confidence in the use of ICTs, encouraging e-commerce and e-government, and protecting the security of transactions and the privacy of citizens.

The e-laws encompass a variety of legal issues related to use of the communicative, transactional and distributive aspects of network information devices and technologies. The legislation secures commercial activities online, proscribing and spelling out sanctions for unwanted activities in cyberspace. The key themes include the jurisdiction of the legislation and judicial cooperation agreements with foreign countries, security of networks, intellectual property, freedom of expression, e-commerce, business ethics and individual privacy. For the purposes of this discussion, only a few issues relevant to e-government are discussed, noting that e-government is understood to incorporate forms of e-commerce.

1. CYBERSECURITY AUDITS

The cybersecurity law (Law No 2010/012) provides that ICT infrastructure and information systems of operators, access providers and Internet service providers (ISPs) must undergo an obligatory security audit. The scope and conditions for rating cybersecurity, according to a severity scale, are determined by MINPOSTEL. Security audits and severity scale ratings are to be undertaken each year, or more often if necessary, and reports presented to the Minister.

2. BUILDING TRUST AND CONFIDENCE IN THE USE OF ICT

The provision for electronic certificates (for authentication), electronic signatures (for integrity), and public/private keys (for privacy) establishes the legal regime of digital evidence, security, cryptography and electronic certification activities. This has the effect of protecting human rights and privacy and also personal data. This is intended to enhance the use of ICT by citizens[1].

3. APPROPRIATE LAWS FOR A DIGITAL CAMEROON

The electronic communications law (Law No 2010/013) aims principally at harmonising the domestic criminal substantive law elements of offences, with connected provisions in the area of cybercrime, providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as other offences committed by means of a computer system.

4. SUPPORTING A DEMOCRATIC ENVIRONMENT

The law provides for freedom, privacy and protection of human rights, which enhances democracy. Appropriate implementation would enhance an individual's possibilities of communication and interaction, for example where there is participation in public service processes by way of electronic polls, or e-voting [2].

1 See generally Part II of the 2010 security frameworks for cybersecurity and electronic communications, Laws No 2010/012 and 2010/013.

2 Law No 2011/013 of 13 July 2011 relating to voting by Cameroonian citizens

5. PROMOTING EFFECTIVE SERVICE DELIVERY AND ELECTRONIC GOVERNMENT

Together the laws can play a key role in improving service quality, as well as achieving the economic objectives of the country and region by securing information and transaction systems.

Law and regulation provides the basis for educating the public on how cybersecurity can help foster a good environment for a more secure Internet, thus building confidence in using e-government websites and conducting online transactions. The 2010 laws provide a framework for the protection of transactions with respect to various e-government models:

- Government to Business model (G2B): This model concerns the activities carried out by public institutions with external suppliers, for example, e-procurement activities and e-auctions online. In Cameroon, these activities are conducted by institutions like the Department of Public Contracts.

- Government to Citizen model (G2C): This model concerns the activities carried out by public institutions with respect to citizens, for example, utilising institutional web portals to provide online services, such as the presentation of individual tax returns or the application for electronic documents from the Registry Offices. This is also relevant to the provision of e-medicine, e-education and other services to the citizens, where privacy may be infringed. The digital revolution multiplies the individual's possibilities of communication and interaction in an exponential fashion, making it possible to re-launch the classic idea of the individual at the center of the democratic e-society, where privacy and security are protected.

- Business to Government model (B2G): Online activities such as the submission of tax returns online.

- Government to Employees model (G2E): This model concerns the activities carried out by public institutions in relation to employees, for example, providing online services such as e-learning activities and refresher courses for employees through institutions such as the Advanced School of Public Administration.

- Government to Government model (G2G): This model concerns the activities carried out by public institutions with respect to each other, including electronic integration between several departments, or between central and local public institutions, or with other foreign public institutions, for example intelligence activities or international co-operation actions.

The laws aim to build trust in the online relationship between citizens and government, provide a legal framework for a public service that is efficient, a judicial system that is reliable, and an administration that is accountable to the public[3]. There is a predictable legal framework with rules known in advance and therefore protection of the independence of the judiciary. There is available information and transparency that enhances policy analysis, promotes public debate and reduces risks of corruption. Securing cyberspace can assist in achieving public sector reforms or desired transformation, but implementation of these laws has many challenges.

CHALLENGES FOR THE EFFECTIVENESS OF THE E-LAWS

The advantages of the e-laws for e-government are yet to be effectively harnessed, due to the lack of appropriate enforcement. The reasons for weak implementation include:

LACK OF WILLINGNESS TO CHANGE THE STATUS QUO

The reality of stakeholder collaboration and concerted action is not yet achieved as implementation is in the hands of a highly centralised government, which is interested in regulating cybercrime, while the law enforcement cadre is unfamiliar with approaches to cybercrime detection and gathering digital evidence.

LANGUAGE BARRIERS

The bilingual nature of the country (French and English) and multiple local languages based on the more than 250 language groups in Cameroon make the sensitisation and education of the population especially difficult at the local level.

LACK OF ADEQUATE FUNDS

Network connectivity and security requires a significant financial investment.

THE EXISTENCE OF NEIGHBOURING COUNTRIES WITH NO CYBERLAWS

While local limitations of resources and expertise present hurdles to effective law enforcement, one of the transnational challenges of a legal nature that should be considered is that states like Chad, Central African Republic, Nigeria, Equatorial Guinea do not have cyberlaws, making it difficult to sign judicial cooperation agreements. These countries would potentially serve as safe havens for cybercriminals.

THE EVOLVING AND COMPLEX NATURE OF THE PHENOMENON

Computers and the Internet present new ways to engage in old crimes, such as fraud and piracy. It has also become possible for criminals to perpetrate new harmful acts, like Internet scamming, notably high in Cameroon (Akuta, Ong'oa & Jones, 2011). Considerable difficulties also exist with respect to the coercive powers of investigative agencies, especially with respect to encrypted data and investigations in international networks, the range of jurisdiction in criminal matters, and the liability of intermediary service providers on the one hand and content providers on the other. The country is taking measures to combat computer-based crime;

3. See generally Part II of the laws.
4. These are important elements of good governance according to the World Bank.

however, national laws alone are not sufficient to address the global nature of cybercrime because online crimes are inherently international.

LACK OF IMPLEMENTATION OF LOCAL LEGISLATION

Local legislation for the sector is not supported by implementation. For example, the May 2009 law on the identification of mobile telephone subscribers in the country has yet to provide any effective impact on crimes like online harassment, defamation and threats. The reason for this unfortunate situation is that there is no effective control on the sales of SIM-cards and no recognised sales points. Subscribing is therefore clandestine and a fertile for crimes.

RECOMMENDATIONS: GENERAL ACTIONS FOR THE WAY FORWARD

Governments must comply with a combination of legislative guidelines and standards that cover areas relevant to e-government. Bearing in mind that archaic laws, old regulatory regimes and overlapping and conflicting authorities can all greatly complicate or halt the implementation of government projects, the development of a new regulatory framework building on the 2010 e-laws should be seen as a priority. Specifically the following actions are recommended:

COLLABORATION AND CONCERTED ACTION

Telecom stakeholders, including government, citizens, the private sector, civil society, academia, media and international organisations based in Cameroon should collaborate in the search for crime-free cyberspace.

STRUCTURING NATIONAL RESPONSE STRATEGIES

Anti-cybercrime strategies should be introduced, in order to offer advantages of reduced cost and time for development of e-government and e-commerce. While international cooperation is necessary, Cameroon will have to develop its own national cybersecurity strategy, authorities and capabilities, adequate for the needs of governmental entities on the national and sub-national levels, as well as for the needs of the private sector and civil society. Strategy should include establishing reporting mechanisms through setting up an online cybercrime complaint center; enhancing digital forensic technology research; adopting standardised investigation procedures; improving technology support through cooperating with academic and research institutes, information technology enterprises, Internet service providers and other organisations; and training regularly (Asongwe, 2011).

LOCAL EXPERTISE

The optimal solutions that might be adopted depend on the resources and capabilities of the country. Therefore there is the need to produce effective security processes and master the ICT related risks; collaborate with legal, law enforcement and technical professionals; and scan best practices globally to create local processes. In April 2010, the Cameroon government spent XAF174 billion on cybersecurity equipment and expertise obtained from the South Korean government. This is an exorbitant amount given the economic standing of the country, which has a GNP per capita of USD2 300. It is necessary to create local knowledge based on well recognised standards, to answer specific local needs by integrating local cultural values in national standards, which may be derived from international standards.

TRAINING OF LAW ENFORCEMENT OFFICERS

It is further necessary to introduce training initiatives to help combat cybercrime in order to deliver secure and effective e-government processes. Training should be conducted on a regular basis and private-public partnerships in training should form the basis for capacity building. In order to continue the development and delivery of effective cybercrime training to law enforcement officers at a regional level, it is necessary for them to partner with organisations and industry to create a network to take responsibility for the training programmes and offer appropriate academic qualifications. Academic institutions are in a position to use their considerable pool of research and education expertise to support both government and industry in the development of education programmes designed to facilitate the enhancement of skills and qualifications relevant to the area of cybercrime. This will help cut down the cost of implementing security measures.

The e-laws (cybersecurity and cryber crime; electronic commerce) deal with key economic, legal and social issues that will enable Cameroon to take a quantum leap to effectiveness in its public service delivery. The 2010 e-laws, if appropriately implemented, can enhance effectiveness of e-applications. It is possible to conclude that these laws are vital for the enhancement, continuity and sustainability of digital government. Therefore the cybersecurity legal framework must be appropriately enforced for a secure, resilient, sustainable and continuous Cameroon network as critical infrastructures on which e-government processes repose.

REFERENCES

Akuta, E., Ong'oa, I. & Jones, C. (2011). Combating cyber crime in sub-Sahara Africa: A discourse on law, policy and practice. *Journal of Peace, Gender and Development Studies*, 1(4), pp. 129-137, retrieved 12 June 2012 from www.interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al.pdf.

Asongwe, P. (2011). Cameroon's public administration since 1998: Tracking the opportunities and challenges of digital governance. Paper presented at the Fifth eGov Africa Forum, 26-28 April 2011, Yaounde.

Asongwe, P. (2010). A model regulatory and legislative framework for Cameroon. Presentation to the 1st CTO Cybersecurity Conference, 16-18 June 2010, London.

Kamga, A. (2011). e-Government: The way to … Cameroon. Paper presented at the eGov Africa Forum, 26-28 April 2011, Yaounde.

Mokube, P. (2010). State of e-governance in Cameroon. Presentation at Seminar on Electronic Governance Cameroon, July 2010, Yaounde.

Pollifroni, M. (2006). Cyber crimes and egovernment applications: some empirical evidences. eGovernment Workshop '06 (eGOV06), 11 September 2006, Brunel University, West London.

Republic of Cameroon (2010a). Law No 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon, Republic of Cameroon, Yaounde.

Republic of Cameroon (2010b). Law No 2010/013 of 21 December 2010 relating to electronic communications in Cameroon, Republic of Cameroon, Yaounde.

Schechter, S. (2004). Computer security strength and risk: A quantitative approach. PhD thesis, Harvard University.