International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

The Fight against Cybercrime in Cameroon

Prof. André Boraine[a*], Dr Ngaundje Leno Doris[b]

[a]*Country, University of Pretoria, Pretoria, South Africa*

[b]*Higher Technical Teachers Training College, kumba, P.O.Box 249 Buea Road, Kumba*

[a]*Email: andre.boraine@up.ac,* [b]*Email: dorisleno2008@gmail.com*

Abstract

With the on-going Anglophone crisis in the two English-speaking regions of Cameroon, individuals, businesses and the government are increasingly becoming at risk of being targeted by cyber criminals. Amid this challenge, Cameroon has enacted a law relating to Cyber Security and Cyber Criminality (hereinafter referred to as the Cyber law) and trained personels to fight cybercrime. In spite of these measures, cybercrime is still rampant and the question is why? This contribution therefore examines the measures put in place to combat cybercrime with the aim of showing that the measures are inadequate. Also, the contribution explains why cybercrime is prevalent in Cameroon and concludes with measures to prevent and minimise the impacts of cybercrime (recommendations). This paper aims to raise awareness and improve knowledge of data protection rules, especially among investigating officers, students, specialists and non-specialist legal practitioners who have to deal with data protection issues in their work.

Keywords: Fight; Cybercrime; Data; Protection; Cameroon.

1. Introduction

Technological developments and globalisation have brought considerable advantages to the people of Cameroon and the rest of the world. Technological developments in the form of computers, mobile phones and especially the internet have increased the flow of personal data, and the exchange of personal data between public and private actors, individuals, associations and companies [1]. This exchange of information has made personal information available publicly and globally which has gone a long way to improve on the quality of life, efficiency and productivity. Despite these advantages, technological developments have exposed users to numerous potential risks, such as scamming [2], pharming, skimming, SIM-box fraud, defacement, unauthorised disclosure, identity theft, to name a few [3]. Armed with the above-mentioned challenges, Cameroon has enacted a legal framework relating to Cyber Security and Cyber Criminality (otherwise referred to as Cyber Law) [4] and periodically trained personels to combat cybercrime in the country [5].

---

* Corresponding author.

Against this backdrop, this contribution examines the measures put in place to combat cybercrime with the aim of showing that the measures are inadequate. Also, the paper explains why cybercrime is prevalent in Cameroon and concludes with measures to prevent and minimise the impacts of cybercrime. This paper aims to raise awareness and improve knowledge of data protection rules, especially among investigating officers, students, specialists and non-specialist legal practitioners who have to deal with data protection issues in their work.

2. Cybercrime and its types

The UN General Assembly resolution on cyber security [6] addresses cybercrime as one major challenge. Though it is abstruse to quantify the impact of cybercrime on society, one may say without fear or contradiction that cybercrime has made it difficult for developing countries to promote e-business and participate in online service industries [7]. In this context, it is useful, to define the term cybercrime. Definitions abound for the term. The variety of approaches, demonstrates the fact that there is no single definition for the term. One common definition describes cybercrime "as any activity in which computers or networks is a tool, a target or a place of criminal activity" [8]. Cybercrime may be defined as offences committed through the internet. Going by Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the "Stanford Draft") [9], cybercrime refers to acts in respect to cyber systems. Reference [10] described cyber crime as "a range of offences including traditional computer crimes, as well as network crimes". For Gercke, cybercrime is narrower than computer related crimes because it involves only a computer network while computer-related crime covers even those offences that bear no relation to a network [11]. Gercke's definition is good but like other definitions, it falls short of the fact that it does not sufficiently fetch out the different types of cybercrime or what constitutes acts of cybercrime. Though it is difficult to develop a typology or classification system for cybercrime, one approach can be found in the cyber law which distinguishes between different types of offences, namely, cryptography, unauthorised disclosure of confidential information, invasion of privacy and private indecency (pedophia, child pornography and homosexuality) [12].Cybercrime is rampant in Cameroon. The National Agency for Information and Communication Technologies (ANTIC) reminded that over 90% of software and operating systems used in Cameroon are hacked including email addresses and social media accounts of businesses, individuals and government members resulting to lamentable losses for operators, individuals, businesses and the state [13]. Assongmo reported of the prevalence of telephone calls fraud in Cameroon. In 2015, the mobile phone sector lamented losses of 18 billion FCFA for operators with another 46 billion for the state [14]. In 2014, anti-corruption commission reported that "cyber criminality cost 3.5 billion to Cameroon between November and December 2013" [15]. For Abeng, scammers are still doing a brisk business because there has been more talk than action. He recounted the story of a British national who came to Cameroon to track down scammers who fleeced out millions of pounds, but unfortunately, he was found dead in the capital city of Cameroon, Yaoundé [16]. In response to the different offences committed, the government has put in place measures to combat cybercrime. This includes but not limited to the enactment of the cyber law and training of personnels.

3. Measures to combat cybercrime in Cameroon

3.1. Legal framework on data protection

The cyber law is one of several pieces of legislation introduced to deal with individual rights and information policy. The Penal Code [17], CEMAC/UMAC Regulation [18] and the Decree on the Modalities of the Protection of Consumers of Services of Electronic Communication [19] are other statutes which are closely related. The cyber law is a long piece of legislation with over 97 sections divided into four parts [20]. In essence, cyber law seeks to protect individual's right to privacy and ensuring confidence in the use of electronic and information systems [21].

3.1.1. Protection of the right to privacy

Though not define, a user is an individual or legal person whose information is processed by an operator. Users have many rights that companies must respect such as the right to delete personal data from the internet snappily called the "right to be forgotten, the right to correct inaccuracies in personal data [22], right to notification of personal data breaches to individuals, namely where the breach is likely to negatively affect their personal data or privacy and the right to request for transmission of one's personal data [23]. It is worth mentioning that under cyber law; only the following rights are guaranteed: right to reply, request for correction of their personal data in the case of defamation [24] and right to privacy. The right to privacy is a fundamental and inalienable right enshrined in international instruments such as the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights [25]. This right is available to all humans irrespective of sex, race, religion or colour from birth till death, and cannot be transferred or taken away. The right to privacy otherwise called 'the right to be left alone' concerns situations where the private right or life of an individual, intimate situations and sensitive or confidential information is protected from public scrutiny. This is strengthened by the maxim 'live and lets live' which means allowing other people to make their choices while you are allowed to make your choices or while living our lives we must ensure that it does not negatively affect the lives of others. This right to privacy forms an intrinsic part of the right to respect of private, family life, home and correspondences and Cameroon affirms this right in its national laws but does not recognise data protection as a fundamental right [26]. The respect to private life and right to protection of personal data are closely related but differs. For Advocate General Sharpston [27], they both strive to protect the autonomy of human dignity of individuals by granting to them a personal sphere in which they can freely develop their personality, think and shape their opinion. They differ in their formulation and scope. While the respect to private life consists of a general prohibition or interference subject to some public interest criteria that can be justify in certain cases, the protection of personal data is a modern and active right [28]. The constitution of Cameroon provides to everyone the right to respect for the rights of others, the inviolability of the home or correspondences except in accordance with the law or decision from a judicial power [29]. As per the Constitution, everyone has the right to enjoyment of his home, family, private life without interference from others. Trespass to one's property and interference to one's life in the form of assault or battery is prohibited [30]. The assessment of whether or not there is or has been an interference with private life hinges on the facts of each case. For example, the recording by an employer of information relating to the name and remuneration paid to employees cannot be regarded as an infringement with private life except the employer transferred the employees' information to 3rd parties or the general public. It stands to reason therefore that upon receipt of information, the recipient is expected to keep it secret. The principle of confidentiality is an important principle that applies to all disciplines. It is not just the controllers and operators or providers of communication and

information services that will have to comply with the principle of confidentiality [31]. Lawyers, teachers, counselors, Health care providers, insurers, banks and any other company dealing in sensitive personal data will also be on the hook. This is to ensure that access to personal data is limited solely to authorised persons and '... to prevent unauthorised disclosure of information to non-recipients enabling the reading, listening, intentional or accidental, illegal copying during storage, processing or transfer' [32]. Cyber law recognises the importance of protection of information obtains in strict confidence from users and places on operators a number of obligations, one of which is the duty of confidentiality. According to Lord Golf, 'confidentiality is a duty which arises when information comes to the knowledge of a person (confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential and ... that he should be precluded from disclosing the information to others' [33]. All processing of personal data must be based on lawful grounds. These lawful grounds must be established, for example, by obtaining authorisation and consent of the person concerned. Authorisation is necessary for compliance with a legal obligation to which the controller is subject. Authorisation is required in recording communications and traffic data related thereto in a professional setting with a view to providing digital evidence of an electronic communication [34]. Similarly, ANTIC personnels and experts of corporate bodies in charge of security audits are not to disclose without authorisation confidential information they are privy to on the occasion of a security audit, failing which they shall be punished with imprisonment from three months to three years and a fine of 20,000 to 100,000 CFA francs [35]. In addition, consent must be obtained to process personal data lawfully, but it should be noted that consent is not a cure for activities that would otherwise be considered unlawful. Under the Law, it is unlawful to listen, intercept, store communications, the traffic data related thereto or monitoring without the consent of the users concerned [36] or 'use electronic communication networks and information systems for the purpose of storing information or accessing information stored in the terminal equipment of a natural person or corporate body ... without the prior consent of the person' [37]. In Cameroon today, it is common to find cases of peoples' numbers being transferred to social networks such as facebook, twitters and whatsapp without the person's consent. We equally have cases of heath personnel's who go around collecting people's data in the name of distributing filarial or mosquitoes nets or dose and MTN network calling on customers to update their identification with their national identity card receipts without a consent form for them to sign. These are some of the common infringements of the principle of confidentiality and hence, the right to privacy. Breach of confidentiality leads to unlawful destruction, loss, alteration and unauthorised disclosure of, access to, personal data transmitted, stored or otherwise processed. In the event of personal data breach, the Law gives the person who is victim of defamation the right to reply and may request for correction [38] and the criminal investigation officers with general jurisdiction and authorised officials of ANTIC, the power to carry out investigations [39], in accordance with the provisions of the Criminal Procedure Code [40]. The investigation which entails the collation of evidence, identification of offenders and bringing offenders before the legal department is carried out without notification to the user of the breach [41]. Breach of confidentiality attracts a big penalty. This is aimed at deterring operators from disclosure of information. The Law punishes anyone who uses any device to attach, record or transmits private or confidential electronic data without the consent of the author [42], who uses illegal means to collect the personal data of another in order to invade his or her privacy and undermine his or herself esteem [43] or who uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true [44].

The case of *the People of Cameroon v Ekume Otte Sakwe* [45] is illustrative of this point. *In casu*, Sakwe, a resident in Buea was charged by the judicial police officer for publication of force information about three companies which were Yadikwa Immobilier, Agro Agricultural Cooperative Ltd and Darling Home without being able to attest its veracity thereby committing an offence punishable by section 78 (1) of the Law. After examination by the examining magistrate, Sakwe walked away a free man for want of concrete evidence. Similarly, in *the People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim* [46], the accused were examined by the examining magistrate for publication of false information that they had puppies to sell when in fact did not have. After full hearing and consideration of evidence tendered before the court of First Instance of Buea, the accused were found not guilty on the count of cyber crime (pet scam) and so were consequently acquitted. Also, the Law punishes anyone who for financial gain, uses any means to introduces, alter, erase or delete electronic data such as to cause damage to someone else's property [47]. This was the situation in *The People of Cameroon v Kadji Valery* [48]. In this case, Kadji, a student of the University of Buea, fraudulently acquired a sum of money from a lady in Yaoundé. The matter was reported to ANTIC which investigated into the matter and traced Kadji's account at BICEC Buea which was credited with the sum of 1,090,000 CFA francs. With this, ANTIC held that Kadji could not have had such an amount in his account if not of scamming and so was charged under section 73 (2) of the Law [49]. Unfortunately, the case was discharged for lack of evidence to show that the money in his account was gotten from illegal act. This is one of the complications of proving scamming and other cyber crimes in the country.

3.1.2. Building trust in the electronic system

A number of measures are in place to ensure trust in our electronic system, one of which is the fact that none is allowed to operate an electronic communication or information system in the country without a licence, that is, a certificate, an indication that the sector is highly regulated. Certificates are issued by the ANTIC for the purposes for which they are intended [50]. In fact, ANTIC is liable for prejudices caused to people who rely on certificates they present, particularly if the information on the certificates are inaccurate or incomplete [51]. In respect of security, staff of ANTIC and auditing experts must audit the security systems of providers and certification authorities [52], and the report sent to the Ministry [53]. Though the conditions and terms for the conduct of security audits are not defined in the Law [54] security auditing is done periodically in confidence [55], with the aim of ensuring compliance of the Law. In complying with the Law, businesses are required to enhance existing consent forms and have customers re-sign to comply with the tougher requirements, to provide customers with information about the reasons for collection and processing of their personal data, who will receive such information when transferred and the duration for which such information is retained. This is farfetched for the simple fact that the Ministry has failed to monitor the evolution of issues related to security and certification activities in the country [56]. More so, operators must take administrative and technical measures to guarantee the security of the services they provide in order to forestall personal data from being destroyed, lost or accidentally damaged [57]. The measures are not defined and so it is left for the operators to decide. Operators are also required to ensure the availability of material stored in their systems for 10 years [58] and inform users of the following: of the risks of using their network, risk of security violation and the existence of techniques to ensure the security of their communication [59]. Companies who provide access to information are required to inform users of the dangers associated with the use of unprotected data system, need to install

parental control devices and means to restrict access to certain services such as the use of anti-virus against spywares [60].

3.2. Training and seminars General guidelines for the preparation of your text

The cyber Law is an internal evolution applicable only to companies that are located in Cameroon as well as persons who process the personal data of an individual (data processors and controllers) [61]. Data encompasses a program, facts, information or concepts intended to be processed in any form by terminal equipment [62]. Data may take different forms such as a person's name, email address, IP address held in manual files, computer databases, videos and other automated media about living individuals or corporate body, physical material or copies made in the presence of persons taking part in a search [63], connection data [64], traffic data [65] and data which form part of an accessible record (concerning health, education, housing or social services) and which would not otherwise be covered by the definition. This category is included so as to preserve certain rights of individuals in respect of such data. In Cameroon, data is controlled by ANTIC, an institution created by a presidential decree [66] and placed under the supervision of the Ministry of Post and Telecommunication (the Ministry). It is headed by a director and deputy director in the persons of Dr. Ebot Enaw and Madam Paulette Abenkou E'ba. ANTIC has varied functions ranging from the regulation, control, monitoring of activities related to electronic security [67] detection and provision of information on computer risks and cyber crime activities and carries out criminal investigations in collaboration with the Telecommunications Regulatory Board and judicial police officers [68]. Most importantly, it regulates the internet thus becoming a key agent in the restriction of certain activities carryout on the internet [69]. The director and his team are working timelessly in ensuring that cyber crime is reduced in the country by organising seminars in specific towns such as Buea, Douala and Bertoua to equip law enforcement officers such as the police, gendarmes, magistrates and state counsels with skills needed to identify, locate, track down scammers and create awareness on various preventive measures [70]. In a four days seminar organised in Yaoundé [71], 50 staffs of ANTIC were trained on the following aspects: collection of electronic evidence and its deontology as well as techniques of preparing and drafting legal statements. The training was aimed at imbuing personels with skills to better investigate, detect and prosecute crimes committed with the use of information and communication technologies. 33 out of the 50 staffs were special judicial agents with legal jurisdictions in cybercrime sworn in March 2016 [72]. This of course shows that ANTIC is not sleeping as far as the fight against cyber crime is concerned. In as much as ANTIC is striving so hard to curb cyber crimes in the country, cyber crimes are on the rise. According to Abeng Roland, member of the international criminal bar, Cameroon and American associations, the surge of online criminality is due to the absence of punishment, lavish lifestyles of most scammers and slow response by the government to the problem [73]. Leno on her part attributes this increase to a number of factors: high rate of unemployment in the country, difficulty in the detection and prosecution of culprits, lack of awareness of the cyber law and lack of education of the public on the law and the importance of compliance.

4. Limitations: Reasons for the prevalence of cybercrime

Having examined the Law, it is clear that the government is not behind in the fight against cybercrime. We see

this in the various laws and institutions established to assist criminal investigating officers, that is, the forces of law and order in the fight against cyber crimes. For this, the government should at least be applauded. In spite of the government efforts, cyber crime is prevalent. Leno attributes this to a number of factors: limited knowledge of users, inadequacy of the Law, lack of expertise on the part of investigating officers, lack of evidence, lack of monitoring activities and anonymity of culprits. For Leno, these factors have capaciously contributed to the rise of cyber crimes in the country, and hence, violation of individual rights to privacy.

4.1. Inadequacy of the Law

Cyber law has not adequately deterred scammers from committing crimes because the sanctions are less severe. When we look at the sanctions, we find that the maximum imprisonment term meted out on scammers is ten years making scamming which is a serious offence a misdemeanour rather than a felony [74]. Also, the fine to be paid is greater, but it is an irony because scamming is a lucrative crime wherein scammers make much money, so paying a heavy fine will not have much effect on the culprit. This of course makes them very comfortable in committing further crimes. With this, one can adequately describe the Law as being a window dressing and can be circumvented. Scamming is a worldwide crime which requires international cooperation through ratification of many international instruments dealing with cyber criminality, but shamefully, Cameroon has not ratified many of such instruments [75]. This constitutes a big challenge making it practically difficult to combat cyber crimes in Cameroon and across. In Cameroon today, it is revealed that more than 60% of the population have access to the internet [76], so are aware of the Law and cyber criminality, but still fall victims to scammers (limited knowledge of users). This is because most users of either the telephone or internet are not yet versed with some tactics used by scammers to perpetrate their acts. In a country where the opportunity to educate the entire population on cyber criminality and the tactics used by scammers does not usually present itself, it is easier for many scammers to steal from their victims and even receive money for goods sold without actually receiving the goods as was in the case of *the People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim* [77]. Although we have a good law, the majority of the people are not aware of the existence of the law. Those who know of the law and can access it, especially people of the Anglophone regions do not understand the provisions of the law because of the language and the terms used. The repetition of sections and improper connotations of terms makes it difficult for the people to understand.

4.2. Lack of expertise among investigating officers

The complex nature of cyber crimes requires expert knowledge in the recovery and interpretation of digital evidence, but most investigating officers do not have the skills needed to do so. At present, only very few forensic centres exist and the question is how digital evidence will be presented to enable a conviction? [78] This is why most cases end up at the preliminary stage. If there is any challenge that has made many culprits to walk home free is the problem of evidence. Unlike real crime such as a felony or misdemeanour, it is elusive to obtain evidence of a cyber crime. This difficulty arises from the use of sophisticated programs in their computers and passwords by culprits that only experts can decode. The sophisticated nature of the programs makes it easy for culprits to automatically destroy or delete evidence within a few seconds when assessed by anyone, especially the forces of law and order. Magistrate Eware Ashu affirms the complex nature of cyber

crimes and the difficulty in proving them, but held that "... it should not be an excuse for resorting to illegal short cuts to secure a conviction." [79] For her, the non-observance of certain technicalities imposed by the law for the investigation and prosecution made the accused persons to walk away free. The wide nature of cyber space and discrete nature of cyber crimes make it very difficult to identify or locate a culprit, and thus to obtain evidence. Today, most scammers operate at home with no surveillance camera to detect or locate them. In an interview with a scammer, he had this to say 'i have my private modem and laptop that i use to browse at home. Nowadays, we do not use the cybercafé anymore. Because of the accessibility of internet and the fact that the law enforcement officers are always carry out surveillance in cafes, I prefer to work at home where no one will know my whereabouts or know what activity i am engaging in' [80]. With this, it is glaring that culprits cannot let go of their activities because of the benefits they get from it and the fact that they are not afraid of being arrested or prosecution [81]. When interviewed, a scammer had this to say 'we are not afraid of arrest or prosecution. Rather, what we are afraid is the amount of money we have to pay or we lose when arrested by the police called 'settlement to the police' (bribing their way out of the prosecution)' [82].

4.3. Lack of monitoring activities

As per the Law, the Ministry has a duty to monitor the evolution of issues related to security and certification activities in the country [83], but has failed woefully in the discharge of its duties. No follow-up of the activities of companies to ensure that the law is implemented or comply with, leaving companies at the mercy of their own acts. The lack of monitoring activities or follow-up whose aim is to ensure compliance accounts for the rise of violation of the law, in particular, the rights of individuals. The poor governance system of the country and centralised nature of the ministry are behind the current state of affairs in the country. To maintain public confidence in the Law and hence the protection of individual rights to privacy, it is necessary for the government to do more by implementing the following proposals.

5. Recommendations

In view of the challenges discussed above, the following recommendations or proposals are made. The recommendations set forth below are designed to avert and minimise the impacts of cybercrime on individuals, businesses and organisations. For the benefits of readers and researchers, Leno considers that the Law should provide clear meanings or definitions to key terminologies such as data, cybercrime and avoid repetition of sections and use of terms that are of no use, so as to avoid confusion [84]. The truth is more people are unaware of the existence of the Law. The lack of awareness due to either the language barrier or ANTIC's inability to disseminate the Law has made it difficult for many to understand the law and for Anglophone judges and magistrates to interpret the Law. The Law was translated from French into English [85], but the translated version is inadequate and nebulous. With respect to translation, much needs to be done. Translation should be done by experts or people with skills and knowledge of the law to avoid confusion and duplication of the law) and encourage dissemination of the law. This time, several trainings should be organised by ANTIC in collaboration with scammers and hackers in the different towns and regions of the country on the existence of the Law, the importance of compliance of the rules, the penalties for non-compliance, the rights of users with respect of their personal data and the tactics of scamming. This will help to reduce the rate of violation of the

right to privacy. The trainings of the investigating officers should focus on equipping them with the skills needed to recover and interpret digital evidence. This requires an increase in the forensic centres in the country to help train investigating officers on the presentation of digital evidence and thus the conviction of cyber culprits. In addition, there should be collaboration between the Law enforcement officers and Information Technology professionals so as to reinforce the fight. As for users, their trainings should focus on some of the tactics used by cyber criminals, how to recognise when they are in danger of becoming a victim, what to do when they encounter a cybercriminal. It is evident from the above that the best chance for success in the fight against cybercrime is when we approach it from different angles. The legal process is just one way but the best methods are proactive rather than reactive- that is, it is best to prevent the crime before it happens. Since it is not possible to avert cybercrime, organisations and individuals can take steps in advance to minimise the impacts cybercrime will have on them or their organisations. In so doing, they can use backups of data to restore data, spare servers or use cybercrime insurance to recoup losses against crimes. They may install an AV package to check in-coming and out-going mails. Many of our teenagers today engage into hacking or scamming for a number of reasons: to impress their friends and to make big money. To avoid this, the peers of con-artists may be used to shame rather than admire their peers. This method is effective when it comes to young people [86]. Equally, the names of arrested con-artists should be printed in a newspaper to deter others from committing such crimes. The premise here is that the fear of publicity will likely deter others from engaging in such activities [87].

6. Conclusion

Cameroon has a law for protecting data privacy. This Law subject companies that collect, store and process information of individuals, that is, companies with digital presence in the country. This includes insurers, banks and other companies dealing in sensitive personal data. Despite government's effort in ensuring that individual rights to personal information are protected, violations of this fundamental right keep racing on. The author attributes this to a number of problems such as limited knowledge of users, inadequacy of the Law, lack of expertise on the part of investigating officers, lack of evidence, lack of monitoring activities and anonymity of culprits. These problems have rendered many Cameroonians bankrupt and some homeless as a result of scamming and hacking of accounts. A lot needs to be done to redress these problems and as seen above, a lot of training must be carried out to educate the people and the investigating officers. This will go a long way in informing the people and ensuring compliance of the Law.

References

[1] B. Mbodiam and M. Cisse. "Business in Cameroon" www.businessincameroon.com/pdf/Bc5/pdf, Jun.4, 2019 [Feb. 12, 2018].

[2] K. Ngalla. 2016. "Cameroon's Dilemma in Fighting Cybercrime" African Independent Business Journal. Vol 1, p1. Available: https://antic.cm/index.php/en/component/k2/item/348 [June. 3, 2019].

[3] Ibid.

[4] Law N° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality (hereinafter referred to as Cyber law).

[5] National Agency for Information and Communication Technologies (ANTIC).

[6] UNGA Resolution: Creation of a Global Culture of Cyber Security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[7] M.Gercke. (2012, September 12). Understanding Cybercrime: Phenomena, Challenges and Legal Response. (2nd edition)' [On-line]. Pp4-12). Available: itu.int/ITU-D/cyb/cybersecurity/legislation.htm [date accessed Jun. 4, 2019].

[8] "Carter, Computer Crime Categories: How Techno-Criminals Operate", FBI Law Enforcement Bulletin, 1995, p21. Available: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf, Apri. 25, 1995 [Jun.4, 2019].

[9] The text of the Stanford Draft is published in: The Transnational Dimension of Cyber Crime and Terror, p225, http://media.hoover.org/documents/0817999825_221.pdf, [Jun. 4, 2019].

[10] M.Gercke. (2012, September 12). Understanding Cybercrime: Phenomena, Challenges and Legal Response. (2nd edition)' [On-line]. p12). Available: itu.int/ITU-D/cyb/cybersecurity/legislation.htm [date accessed Jun. 4, 2019].

[11]. Ibid.

[12]. Sections 60 to 85 Cyber law.

[13].N. Assongmo. "Cameroon is a Country vulnerable to cyber-criminality" USENET: https.//www.google.com/amp/s/www.businessincameroon.com/index.php, Sept. 9, 2016 [Mar. 24, 2019].

[14]. Ibid.

[15]. Ibid.

[16]. Voa.com. "Cameroon urged to Act against cybercrime" USENET: https://www.google.com/amp/151740.htm, Feb. 10, 2011 [Feb.10, 2018].

[17] Law No. 2016/007 of 12 July 2016 relating to the Penal Code.

[18] Regulation No. 01/CEMAC/UMAC/CM of 4th April 2003 on the Prevention and Suppression of Money Laundering and Financing Terrorism in Central Africa.

[19] Decree No. 2013/0399PM of 27th February 2013.

[20]. Part one provides content to key terms such as cipher, encryption, and security audit just to name a few. Part two deals with electronic security and cyber security. This part places on the Ministry of Post and Telecommunication the duty to formulate and implement policies relating to electronic communication security. The National Agency for Information and Communication Technologies, hereinafter referred to as the Agency, is responsible for the regulation of electronic security activities in collaboration with the Telecommunications Regulatory Board. Part three identifies crimes that may be committed through the internet and their various penalties and part four relates to international cooperation with other countries.

[21]. Section1, Cyber Law.

[22]. T.Danziger and C.Danziger. "Art and Law"Art news (Jul. 17, 2018), 2.

[23]. European Commission. "EU Data Protection Reform: Better Data Protection Rights for European Citizens". Internet: europa.eu/dataprotection,May.12, 2011 [May. 12.2019].

[24]. Section 39, Cyber Law.

[25]. 23 March 1976.

[26]. Cameroon Constitution of Law No. 96-06 of 18 January 1996 to amend the Constitution of 2 June 1972 and the Law of 2010 on Cyber Security and Cyber Criminality.

[27]. Advocate General Sharpston described the case as involving two separate rights: the 'classic' right to the protection of privacy and a more 'modern' right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71. 5. S

[28]. Ibid.

[29]. The Preamble, Cameroon Constitution.

[30]. Sections 152, 305 and 280-281 of the Penal Code criminalise actions of contempt or assault against anyone.

[31]. Section 42,Cyber Law states that 'The confidentiality of information channelled through electronic communication and information systems networks, including traffic data, shall be ensured by operators of electronic communication and networks information systems'.

[32]. Section 3 (24), Cyber Law.

[33]. A-G v Guardian Newspaper Ltd (No. 2) 13 October 1988, 85.

[34]. Section 45, Cyber Law.

[35]. Section 61, Cyber Law.

[36] Section 44 (1), Cyber Law.

[37]. Section 47, Cyber Law.

[38] Section 39 (1), Cyber Law.

[39]. Ibid, section 52 (1).

[40]. See sections 57-126 of Law No. 2005/007 of 27 July 2005.

[41]. Ibid, Section 82.

[42] Section 74 (1), Cyber Law punishes with imprisonment from one to two years and a fine from one to two million.

[43]. Section 74 (4), Cyber Law punishes with imprisonment from six months to two years or a fine from one to five million CFA francs or both of such fine and imprisonment.

[44]. Section 78 (1) punishes with imprisonment from six months to two years or a fine from five to ten million CFA francs or both of such fine and imprisonment.

[45]. Court of First Instance of Buea (CFIB)/017b/2015 unreported.

[46]. CFIB/015f/2012 unreported.

[47]. Section 72, Cyber Law.

[48]. Court of First Instance of Buea/011A/2013 unreported.

[49]. Section 73 (2), Cyber Law provides 'Whoever deliberately accepts to receive electronic communications payment using a forged or falsified payment, credit or cash withdrawal card shall be punished in accordance with Subsection 1 above'.

[50]. Section 8 (1), Cyber Law provides "… ANTIC shall be the Root Certification Authority (2) … ANTIC shall be the Certification Authority of the Public Administration."

[51]. Section 16, Cyber Law.

[52]. Sections 13 and 32 (2), Cyber Law.

[53]. Sections 32 (3), Cyber Law. It is left for the experts to define the conditions and terms for the conduct of security audit.

[54]. Section 13 (2), Cyber Law. See Decree No.2012/1643PM of 14 June 2012 on the Conditions and Modalities of Security Audit of Electronic Communication and Information Systems Networks for the conditions for the conduct of audit.

[55]. Section 14, Cyber Law.

[56]. Section 6 (1), Cyber Law.

[57]. Section 24, Cyber Law.

[58]. Sections 25 31 and 46, Cyber Law.

[59]. Ibid.

[60]. 33, Cyber Law. The risks which users are to be informed of are not known by users.

[61]. Section 3 (41), Cyber Law. Processing is carried out in good faith and entails in particular the collection, storage, use, revision, disclosure, archiving and destruction of data, regardless of the means applied and procedure

[62]. Section 3 (41), Cyber Law.

[63]. Ibid, Section 53.

[64]. Ibid, Section 3 (42) defines Connection data as 'data relating to the access process in an electronic communication'.

[65]. Ibid, Section 3 (43) defines Traffic data as 'data relating to an electronic communication indicating the origin, destination, route, time, date, size and duration or type of underlying service'.

[66]. Decree No. 2002/092 of 8th April 2002.

[67]. Section 7(1), Cyber Law.

[68]. Ibid.

[69]. See Decree No. 2012/180/PR of 10th April 2012.

[70]. The seminars were organized differently. In Buea, it was organized on the 16 of September 2017,

Douala, 4-5 of May 2017 and Bertoua from the 25-27 May 2017.

[71]. The Seminar was organized in the month of November of 2012.

[72]. http://antic.cm/index.php/en/component/k2/item/348, [Feb.10, 2018].

[73]. Voa.com. "Cameroon urged to Act against cybercrime". Internet: https://www.google.com/amp/151740.htm, Feb. 10, 2011 [Feb.10, 2018].

[74]. Section 73 (1), Cyber Law.

[75]. The Budpast Convention of 23rd November 2001.

[76]. See <www.antic.com> accessed 12 August 2018.

[77]. CFIB/015f/2012 unreported.

[78]. In cracking down on cyber crime, the government created in 2015 a center for digital forensic and cyber security under the University of Buea in partnership with the Ministry of Post and Telecommunication and university of Bloomsburg in the U.S. according to the director of the centre, Joan Waka, their mission is to "train young Cameroonians on how to protect the country's cyberspace".

[79]. CFIB/015f/2012 unreported.

[80]. An interview conducted with a scammer in my neighbour in Limbe.

[81]. E. Akuta and J.Ongloa. (2011, Oct). "Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy and Practice."J Peace Gender and Development studies. [On- line]. Pp129-137.

[82]. Interview conducted on the 12 of July 2018.

[83]. Section 6 (1), Cyber Iaw.

[84]. The duty of information and communication operators to conserve data for 10 years is repeated in various sections of the law, that is, sections 25, 35, 42 and 46. The repetition of these sections brings the law to 90 sections.

[85]. Africa.ICT. "Full text in English: cyber security& cyber criminality law". Internet: www.afrlct.com, [Sept. 23, 2019].

[86] C. Michael. Scene of the Cybercrime. Location: Syngress Publishing Inc, London, 2008, pp35.

[87]. Ibid.