IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Critical Analysis of Cybersecurity Law in Cameroon.

Ashu Pauline Manyi, Ph.D.[1]

[1] Senior Lecturer, Department of English Law, Faculty of Laws and Political Science, University of Maroua – Cameroon.

ABSTRACT

The importance of cybersecurity is on the rise in Cameroon. Fundamentally, our society is more technologically resilient than ever before and there is no sign that this trend will slow down. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like mobile money codes, social security numbers, credit card information and bank details are now stored in cloud storage services like drop box or google drive. The vulnerability of our computers, information systems and networks have exposed individuals, businesses and the government at risk of being targeted by cyber criminals. The impact of cybercrimes is one which the government of Cameroon cannot claim a blind eye to. Stamping it out looks almost impossible and it leaves us asking if there are any steps taken to realize its complete eradication. Amidst these challenges, Cameroon enacted Law No 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality (hereinafter referred to as the Cyber law) to regulate and monitor electronic security activities; electronic certification and electronic signatures; electronic documents; protection of electronic communication networks, information systems and privacy, etc. This study is undertaken to critically analyze cybersecurity law in Cameroon. For this study, a qualitative method of research was used. Materials were collected from secondary sources, such as books, websites, reports, articles, dissertations, theses, conventions, etc . We also found out some challenges faced in implementing cybersecurity law. To redress these, some recommendations have been proposed which will go a long way informing and ensuring compliance of the Law.

Key Words: **Critical Analysis, Cybersecurity Law, Cameroon.**

1. INTRODUCTION

Over the years, Cameroon has experienced a rapid increase in information and Communication Technology (ICT) and Internet usages. As years go by, internet users have doubled making the country one of the African countries in the lake Chad with the highest growth in internet access. This has increased the flow and exchange of personal data between public and private actors, individuals, associations, and companies. It has also led to the rapid growth in businesses, education, e-services, social media use and high penetration of mobile services and this has gone a long way to improve the quality of life, efficiency, and productivity[2].

The government of Cameroon has long identified ICTs as a strategic tool in its economic development plans, including a strategic vision to lead the central African sub-region's telecommunications industry to be an ICT hub in the sub-region. In its "*Strategic Plan for Digital Cameroon by 2020"*[3], the government promised to integrate and promote the use of ICTs in all sectors of the economy, thereby transforming Cameroon into a digital economy. In addition, it promised to improve the regulatory framework by ensuring that the legislative and regulatory frameworks are adapted to the market and technology trends. As the vision gets implemented and as the society depends more and more on digital technologies, security of the information infrastructure of the country has become a major concern, especially the critical ones.

Notwithstanding these benefits, internet access and technological developments have exposed users to numerous potential risks, such as scamming, phishing, skimming, SIM-box fraud, defacement, unauthorized disclosure, identity theft, etc[4]. Report of millions of dollars lost by businesses and individuals to cybercrime are becoming a common feature in the media. However, besides the financial losses, the systems and networks providing critical services to societies are also at risk of attack and sabotage[5]. Knowing the different point of attack or threat, attacks surface and the readiness of organizations in preventing such attacks is a first step in improving the security posture of any cyber infrastructure. To this effect, the Law of 2010 regulating cyber security and cyber-crimes has been put in place to regulate and monitor electronic security activities; electronic certification and electronic signatures; electronic documents; protection of electronic communication networks, information systems and personal privacy in Cameroon.

2. FIELDS OF PROTECTION UNDER 2010 CYBERSECURITY LAW

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyberattacks. It is made up of two words, one is *cyber* and the other is *security*[6]. Cyber is related to the technology which contains systems, networks and programs or data. Whereas security related to the protection includes systems security, network security and application, and information security [7].

Cybersecurity in Cameroon governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon. The law on cybersecurity also seeks to build trust in electronic communication networks and information systems; establish the legal regime of digital evidence, security, cryptology and electronic certification activities; protect basic human rights such as the right to human dignity, honour and

[2] Boraine A. & Ngaundje L., (2019). "Fighting Cybercrime in Cameroon" *International Journal of Computer* (IJC), Vol. 3, No 1, ISSN 2307-4523, Pp 87-100. Also, Situational Analysis of Digital Security in Cameroon, P. 1.; Tomslin Samme-Nlar, (2021). "Cybersecurity in Cameroon Enterprises: What we Learnt", GEFONA Digital Foundation.

[3] http://www.minpostel.gov.cm/index.php/en/les-grand-chantiers/138-cameroon--digitalstrategic-plan-2020. Accessed 11/03/2025.

[4] Boraine, (2019). "Situational Analysis of Digital Security in Cameroon". Retrieved at: Cameroon_Digital_Security _Situational _Analysis.pdf. p. 2.

[5] Mohammad Talid, (2012). "Cyber Forensics: Computer Security and Incident Response", *International Journal of New Computer Architectures and Their Applications (IJNCAA)*, 2(1): 127137, ISSN: 2220-995. P. 127.

[6] Cyber Security Lecture Notes, B Tech III-Year, 2020-2021, Department of CSE, Malla Reddy College of Engineering and Technology, India, Pp 1-37.

[7] *See ibid.*

respect of privacy, as well as the legitimate interests of corporate bodies[8]. The intensification of information and communication technology usages in all facets of life has exceedingly amplify the call for security and to avoid incidents of information security breaches, such as cybercrimes, frauds, commercial crimes, cyber laundering, etc. However, the government of Cameroon requires a well - developed approach to tackle these incidents in order to realize legally defensible digital security[9]. In this paper, we would be making a critical analysis of cyber security Law in Cameroon.

2.1. ELECTRONIC DOCUMENTS

Electronic document is one of the areas of protection by the 2010 law. The law has put in place measures necessary to protect documents that are signed electronically. To this effect, the law provides that any person wishing to affix an electronic signature to a document can do so by creating document using a reliable device whose technical characteristics shall be determined by the instruments defined by the Minister in charge of telecommunications[10]. The law has also provided that any person using an electronic device must take minimum precautions fixed by the minister in charge of telecommunications in order to avoid any illegal use of the encoding elements or personal equipment related to its signature; inform the certification authority about any illegitimate use of his signature; and to ensure the authenticity of all the data he declared to the electronic certification service provider and to any person he requested to trust his signature[11].
However, in the event of failure to respect these commitments, the holder of the signature shall be responsible for any act or injury caused to others[12].

2.2. ELECTRONIC COMMUNICATION NETWORKS, INFORMATION SYSTEMS AND PERSONAL PRIVACY

The 2010 law on Cybersecurity has equally put in place security measures that are aimed at protecting electronic communication networks, information systems of private individuals, companies, the government of Cameroon in general, as well as protecting privacy.

2.2.1. ELECTRONIC COMMUNICATION NETWORKS

An electronic communication network (ECN) is a type of computerized system used for buying and selling securities, and is an alternative to stock exchanges. It is also where we buy and sell orders for securities from different market participants are directly matched, eliminating middlemen like brokers[13]. It allows brokerages and investors in different geographic locations to trade without a third-party involvement, offering privacy for investors[14].
The 2010/012 law on cybersecurity has also put in place measures where electronic communication networks operators and E C service providers must take all necessary technical and administrative measures to guarantee security of the services provided in order to protect the communication network system. For this measure to be implemented, the network operators and service providers of the network operator are bound to inform users about the risk of using their networks; the existence of techniques to ensure the security of their communication; the specific risks of security violation, especially denial of services distributed, abnormal rerouting, traffic points, traffic and unusual ports, passive and active listening, intrusion and any other risk[15].

[8] Section 1 of Law no 2010/012 of 21 December 2010 relating to Cybersecurity and Cyber Criminality in Cameroon.
[9] Mohammad Talid, (2012). *Op cit*, p. 127.
[10] Section 21 of the 2010 law on Cybersecurity (*supra*).
[11] Section 22 *(ibid*).
[12] Section 23 (*ibid).*
[13] Adam Hayes, (2022). "Electronic Communication Network (ECN): definition and Examples", Investopedia.
[14] See *supra.*
[15] Section 24 of the 2010 Law on Cybersecurity *(supra*).

The law further provides that EC network operators and service providers shall be bound to conserve traffic connection data for a period of ten (10) years. They shall equally set up mechanisms for monitoring the traffic data of their networks, which are made accessible during judicial inquiries, and they shall also be liable where the use of the traffic data undermines the individual liberties of users[16].

2.2.2. INFORMATION SYSTEMS

The 2010 Cybersecurity law has further put in place measures to protect information systems in Cameroon. Here, operators of information systems; Corporate bodies; electronic communication networks and information systems content providers have been assigned to ensure the protection of the information systems which are examined below.

2.2.2.1. INFORMATION SYSTEMS OPERATORS

Operators of information systems play a great role as provided by the cybersecurity law to protect the information systems by carrying out various tasks:

- take every technical and administrative measure to ensure security of services offered by having some standardized systems which at all times identify, assess, process or manage any risk relating to the security of the information systems of services provided directly or directly[17];
- set up technical mechanisms with the approval and visa of the agency to avoid any hitches that may be prejudicial to the steady functioning of systems, their integrity, authentication, non- repudiation by third party users, confidentiality of data and physical security[18];
- Protect information systems platforms against any radiation or intrusion that may impair the integrity of data transmitted and any other external attack especially through intrusions detection system[19].

Information systems operators have to inform users of the prohibition of using electronic communication networks for publishing illicit content or any other acts such as designing of misleading viruses, spywares, desirable software or any other device leading to fraudulent practices that is likely to affect the security of networks or information systems[20].

Information system operators are also bound to conserve connection and traffic data of their information systems for a period of ten (10) years; set up mechanism for monitoring and controlling access to the data of their information systems which shall be accessible in the course of judicial inquiries; installations of operators of information systems may be subject to search and seizure order by a judicial authority as provided by the laws and regulation in force[21].

They shall also assess and revise their security systems and where necessary, make appropriate modifications to their security practices, measures and techniques according to technological change; operators and users may cooperate mutually with a view to implementing security practices, measures and techniques for their systems[22].

2.2.2.2. CORPORATE BODIES

Corporate bodies are also in charge of providing access to information system as per the 2010 law on cybersecurity. They have asA obligation to provide users with information about the dangers associated with the use of unprotected information systems for private individuals; the need to install parental control devices; specific security especially, generic of viruses; the existence of permanent technical means to restrict access to certain services and propose at least one of such means such as, the use of most recent operating systems, the

[16] Section 25 of 2010 Law (*ibid*).

[17] Section 26 (1) of the 2010/012 Law (*supra*).

[18] Section 26(2) (3) *(supra).*

[19] Section 26 (4) (*ibid)*.

[20] Section 28 (1) (2) of 200 Law*(supra*).

[21] *See ibid.*

[22] See *supra.*

use of anti-viruses against the activation of personal firewalls, intrusion detection systems and activation of automatic updating.[23]

2.2.2.3. ELECTRONIC COMMUNICATION NETWORKS AND INFORMATION CONTENT PROVIDERS

They also play a great role in the protection of electronic communication networks as provided by the 2010 law on cybersecurity. Electronic communication networks and information systems content providers shall be bound to carryout tasks such as ensuring the availability of material, as well a data stored in their installation; and they are bound to set up filters in order to avoid any attacks that may be prejudicial to personal data and the privacy of users[24]; shall be subject to a regime of compulsory and periodic auditing of their security systems by the agency; undertake security audit and severity scale rating each year or as required by the prevailing circumstances[25]; all audit reports shall be confidential and shall be addressed to the Minister in charge of Telecommunication; and the Minster shall also fix conditions for rating the severity scale[26].

2.2.3. PRIVACY

Privacy is a fundamental human right which is very difficult to define. Nevertheless, different countries have different views as to its definition. Generally speaking, privacy includes the right to be free from interference and intrusion. The right includes privacy of communications (telephone calls, correspondence, etc); privacy of home and office, health, etc [27]. It can also be defined as the right to be left alone and to keep certain matters secluded from public view[28]. However, the law of 2010 on cybersecurity seeks to protect privacy, which is the right to dignity, honour, reputation and respect through electronic communication[29]. As part of modern technologies, electronic communications pose a serious threat to the privacy of individuals. The law has laid emphasis on the protection of privacy and the punishment thereto in case of violation[30]. Glaring examples of violation of privacy is found in the landmark cases of ***Yomba Madeleine v. Les Brasseries du Cameroun***[31] and the case of ***Mfopa Mama born Ntouo Sabiatou v. Societe Nestle Cameroun S.A and Societe Ocean Central Africa SA***. In both cases, the individuals' photos were unlawfully used for advertisement purposes without their consent, constituting violation of their image's rights. To this effect, the courts ruled in their favour and they were compensated. Also, in the case of ***Mbock Frankline Junior v. Les Films Terre Africaine and Les Brasseries du Cameroun*** *(unpublished)*, a contract stipulated for the use of an individual's image within a specific period of two years was violated through the broadcasting of the advertising spot beyond the agreed term. This constituted a violation the individual's right to image. It was held at the final judgment that mere evidence of the invasion of one's privacy gives rise to compensation, and that there is therefore no need to established that they suffered some damages[32].

The increased use of digital platforms requires the collection and storage of a wide range of personal data. However, some websites, commercial companies, public entities, health care establishments, banks and others often hold valuable information in digital form, on their customers or users[33]. To this effect, the law provides that operators of electronic communication and network information system shall ensure the confidentiality of

[23] Section 27 of the 2010/012 law (*supra).*

[24] Section 31 (1) (2) of the 2010 Law of Cybersecurity (*op cit*).

[25] See *Supra.*

[26] Section 32 (3) (4) i*bid.*

[27] European Convention on Human Rights and the Human Rights Act 1998, Article 8.

[28] *See ibid.*

[29] Section 41- 48 of the 2010 law (*ibid*). Electronic communication is the emission, transmission or reception of signs, signals, writings, images or sounds through electronic means, and includes e-mail, facsimile transmission, internet, telex, telegraph, telecopy, telephone communication confirmed by writing.

[30] *See supra.*

[31] Supreme Court of Cameroon, Judgment No 61 of May 1976.

[32] D. Moukouri, (2020). "Data Protection Overview in Cameroon", *LEXAfrica.* Available at: lexafrica.com/2020/03/data-protection-overview-in-Cameroon. Accessed 20/03/2025.

[33] Cameroon Data Protection Overview. Available at: https://www.dataguidiance.com.ca. Accessed 09/03/2025.

information channeled including traffic data[34]. Also, where content may entail infringement of human dignity, injury of character and invasion of privacy, the content providers shall be responsible for data transmitted through their information systems networks[35].

Also, the 2010 law has equally laid down a number of actions, which if carried out will be considered as violation of privacy, which include, to listen, intercept or store communications and traffic data related thereto, which can be used for other means such as interception or monitoring without the user's consent[36].

Furthermore, electronic communication networks and information system content providers are bound to conserve content and store data in their installation for a period of ten years and they also have to set up liters in order to contain any attack that may be prejudicial to the personal data in privacy of users[37]. It is important to reiterate that, a copy of data violating an individual's privacy can be seized and destroyed[38]. Its destruction must be ordered by the State Counsel. Only objects, documents and data used as evidence may be kept under seal and this must be authorized by the State Counsel. If the data or information has been transformed or modified, the State Counsel, Examining Magistrate or Court may request that a clearer version of the data be obtained. This can be done by experts such as qualified natural persons or companies having technical capacity to do so[39].

2.3. ORGANS IN CHARGE OF REGULATING AND MONITORING OF ELECTRONIC SECURITY ACTIVITIES.

The 2010 law has put in place the National Agency for Information and Communication Technologies, in its French acronym "ANTIC", together with the Telecommunication Regulatory Agency (TRA), to regulate electronic security activities in Cameroon[40].

2.3.1. NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES (NAICT)

This organ came into existence by virtue of 2012 decree[41], which relates to its organization and functioning. In French, it is referred to as "ANTIC" which is the acronym used throughout this paper. "ANTIC" is an independent body put in place by the 2010 law, whose main mission is to follow up government actions in the domains of ICTs, ameliorate the way of life of the local population, and to put in place measures to reduce the cost of electronic communication within Cameroon[42]. It is also responsible for implementing a national cybersecurity strategy, policy and roadmap[43]. "ANTIC" was assigned new missions to regulate electronic security activities and Internet in Cameroon[44].

"ANTIC" is also vested with powers to supervise, carryout forensic investigation, grant injunction and sanction.[45] To this effect, this institution has as duties to submit its employees to take an oath in the discharge of their duties[46]. They carry out certain functions such as bringing awareness of all cybernetic offences which

[34] Section 42, *op cit*.

[35] Section 43 (*supra).*

[36] Section 44 *(supra)*

[37] Section 46(1) and (2) (*ibid).*

[38] Section 41 of the 2010 law on cybersecurity and cybersecurity.

[39] Vigiline Tise, (2021). "Privacy Protection in Electronic Communication Under Cameroon Law", Nico Halle & Co Law Firm.

[40] Section 7(1) of 2010 Law (*supra*).

[41] Decree No. 2012/180/PR of 10 April, 2012 relating to the organization and functioning of the National Agency for Information and Communication Technology (NAICT).

[42] Sylvie Siyam & Serge Daho, (2014) "The Stammering of Cameroon's Communications Surveillance", *Global Information Society Watch*, available at: www.protegeqv.org/ . Accessed 09/03/2025.

[43] Cyberwellness profile Cameroon, United Nations Statistics Division, December 2012. More information is available on ITU website at : http://www.itu.int/en/ITU- /Cybersecurity/pages/default.aspx. Accessed 07/03/2025.

[44] Sylvie Siyam & Serge Daho, (2014). (*Supra).*

[45] Section 2, Chapter 2 of Decree No. 2012/118O *(ibid*).

[46] These duties include accession into local, field work and even professional transportation to collect copies, request by convocation or on the spot inquiries and justification.

can be identified through system control; request information on the financial status; they also solve litigations between certification authorities, network on the one hand and system information security service providers and its consumers on the other hand; they inflict or propose sanctions on certification authorities, security service providers, security auditors and editors of security logistics which does not conform to the law in force; and undertake conservatory measures necessary to ensure the continuity of service and protect the interest of users[47].

However, ANTIC has played a great role in securing Cameroon's cyberspace through four key activities which include.

2.3.1.1. COMPUTER INCIDENCE RESPONSE TEAM (CIRT)

CIRT is one of the organs of "ANTIC" that has been put in place by the 2010 law. An officially recognized national CIRT was established in December 2010[48]. The 'CIRT' is a pillar body responsible for enhancing trust and confidence over the Cameroonian cyberspace by fighting cybersecurity among others. Cameroon responded to cybercrime by establishing CIRT in 2014. Urged to work proactively toward this role, CIRT has made it a priority to create information security awareness and to continuously monitors and controls critical infrastructures[49]. CIRT has the current status of threats and provides valuable information for developing mechanisms to prevent and combat threats among civil, business and public stakeholders, particularly those that are in Key Infrastructures of the country[50].

Also, CIRT's second mission is on vulnerability scanning. It does this by critically identifying the types of vulnerabilities and the percentage at which they appear on the websites. Thirdly, it handles cybercrime incidents and ensures faster and more effective responses to major attacks. It receives reports from cybercrimes or incidents from SED, Interpol, E-mail box (alert@antic.cm) and also carryout forensic investigation and the punishment of cyber criminals[51].

CIRT has organized seminars in order to enforce cybersecurity. For example, a seminar on Internet Governance Forum (IGF) was held in Bamenda on the theme "*Securing the Cameroonian Cyberspace through CIRT".*[52] By virtue of Article 7 of the 2010 law[53], ANTIC has been delegated and authorized to control all activities related to information security. This is to ensure that the system has its latest patches, and monitoring critical infrastructure in real time. CIRT also investigates and resolves computer security incidents. Participants were also drilled at the seminar to use some best practices to avoid attacks by cybercriminals, such as always updating software and systems in used, avoid using pirated versions of software, installation of parental control tools, avoid putting personal information to unknown websites, etc[54].

Also, another seminar was held in Yaoundé on July 2015 [55]to sensitize the population on "*Cybercrime and its consequences in Cameroon".* In this seminar, participants were drilled on the types of cybercrime in Cameroon such as Scamming, phishing, web defacement, skimming, hacking, malware, sim-box and sim swap frauds. Some measures were taken such as cybersecurity watch, sensitization and training, security audit, regulation of internet resources, digital certification. All these are to secure our cyberspace and to fight against cyber-criminality in Cameroon[56].

---

[47] *See supra*.

[48] Cyberwellness Profile Cameroon, United Nations Statistics Division, December 2012. (*supra*).

[49] Cameroon Computer Incidence Response Team Cybersecurity Annual Report 2014.

[50] Ashu Pauline M., (2022*).* "Fighting Cybercrime Threats in Africa: A Legal Appraisal", L*' Harmattan,* Tome 3, p. 359.

[51] See *supra,* see also*,* CIRT Cybersecurity 2014 Annual Report, p. 8, Table 10.

[52] Internet Governance Forum (IGF) that was held from the 18 -20 June 2014, at the University of Bamenda, Bambili.

[53] Chapter II Article 7 (1) – (3) of Law No. 2010 /012 on Cybersecurity and Cyber-criminality in Cameroon.

[54]See *supra.*

[55] Seminar on "Cyber-Criminality and its Consequences in Cameroon", held in Yaoundé, 8th July 2015. Presented by Besong John Ebot, Telecommunication Engineer.

[56] See *supra*.

2.3.1.2. PUBLIC KEY INFRASTRUCTURE (PKI)

The 2010 Law has put in place another organ known as the Public Key Infrastructure, which is in charge of controlling electronic certification system[57]. The National Public Key Infrastructure (PKI) is under the auspices of "ANTIC"[52]. This organ is also in charge of putting security in the system, in order to electronically secure services. Also, this organ assists to secure cyberspace and fight against cyber-criminality by providing electronic certificates to users of Internet services which can as well produce the same legal effects to users over the globe[58]. Moreover, PKI provides users rights to confidentiality, integrity, authentication and non- repudiation of their transactions[59].

Furthermore, the PKI system monitors and controls system infrastructures day by day to see if existing software are updated and free from viruses. They do this through "control bulletin" to know the vulnerability in the system[60].

2.3.1.3. SECURITY AUDIT OF ELECTRONIC COMMUNICATIONS NETWORK AND INFORMATION SYSTEMS

This is another organ of "ANTIC'' that helps in the protection of electronic communication networks and information systems as provided by the 2010 law[61]. It is in charge of auditing security systems to see that they conform to the laws and conventions that are put in place. It also gives recommendations and follows up to ensure they are appropriately implemented. Information security audit provides electronic certificates and issues signature, which is aim at securing those doing business online to make sure the parties they are dealing with are the rightful parties. This signature is created using a protected device and each modification shall be detected[62].

Security audit has been put in place to help secure Cameroon's cyberspace. To this effect, seminars on security audit are necessary in insecure environment. The seminar was aimed at enlightening various participants on the importance of security audit by ensuring compliance of information systems with security standards to this domain. It equally seeks at improving the security of Cameroon's cyberspace by reducing risks caused by malicious acts that could endanger the sustainability of Information systems [63].

2.3.1.4. DIVISION OF CO-OPERATION AND NORMALISATION

This is an organ under the auspices of "ANTIC" that is in charge with the management of Internet resources at the national level. Since cybercrime is not only a national issue and in order to secure the cyberspace, this division has to work with other corporations or international bodies like "IMPACT", which helps train people on how to secure the cyberspace in "*real time fighting*". For example, focal pointers, technicians to increase the technological system. This organ has also put in place norms that must be followed by all[64].

The above four organs and activities of "ANTIC" did not only reflect a framework of active involvement, but a commendable effort not only to fight cybercrimes and put in place security network systems.

---

[57] Electronic certificate is an electronic card which contains your personal credentials, and if login it opens. This certificate is mostly use as signature in banks to carry out transactions. In case an offence is carried out, it easily identifies the culprit. [52] Section 8 and 9 of 2010 law.

[58] Chapter VII, Section 20 (1) of Law No. 2010/012 of 21 December 2010 relating to Cybersecurity and Cyber-criminality in Cameroon.

[59] *See supra.*

[60] Vulnerability are those weaknesses that are found in a system (infrastructure) it is like a "back door" in which hackers and scammers used to exploit and commit crimes.

[61] Section 9 on 2010 Law (*supra*).

[62] Chapter VI Section 18 of the 2010 Law *(ibid).*

[63] Seminar of 12 November, 2011 held at the Yaoundé Conference Hall on Cybersecurity in Cameroon.

[64] See *op cit.*

2.3.2. TELECOMMUNICATION REGULATORY BOARD

The Telecommunications Regulatory Board is an independent body put in place by the 2010 law on cybersecurity that is in charge of regulating and monitoring electronic security activities in Cameroon[65]. TRB is regulated by Decree No 2012/ 2013 of 21 April 2012 which deals with its organization and functioning. Since its creation, the TRB has been acting as the driving force of the telecommunication sector which is today very active and prosperous[66].

- It has some daily activities such as the instruction on license applications, agreements, and accreditations of equipment, regulations control;
- It equally does the entry into service of an eight to nine digital numbering plan in 2007 and 2010 respectively, which has greatly increased the numbering capacity;
- TRA has as a mission to ensure the regulation, control and monitoring of the activities of providers and operators of the telecommunications sectors and also sees to the respect of equity of users[67];
- The methodical approval of interconnection catalogues of mobile telephone operators which favoured a substantial reduction in tariffs of telecommunications and services;
- Planning and conditions of exploitation of frequency bands and the acquisition of a spectrum control mobile stations; the publication of a universal telephone directory and customer sensitization; and
- Impartial and conciliatory rules of disputes amongst operators[68].

However, in order to regulate, or ease the setting up of a competitive attractive market, the TRB is looking for every possible initiative to find solutions to the problems arising from the ongoing economic and technological progress.

3. CHALLENGES FACED BY THE 2010 CYBERSECURITY LAW

The telecommunications sector in Cameroon has grown significantly over the years, with the advent of new technologies and the increasing demand for connectivity. However, the growth has also brought about new challenges, particularly in the area of cybersecurity. In this part of our paper, we would be examining some of the challenges or shortcomings of the 2010 law on cybersecurity in Cameroon.

3.1. LACK OF AWARENESS AND UNDERSTANDING OF THE CYBERSECURITY LAW

The 2010 law has put in place cybersecurity law which is very essential to ensure the smooth functioning of the cyberspace and to protect the interests of consumers, businesses, and the government. Notwithstanding, this law is facing some challenges and one of them is the lack of awareness and understanding of cybersecurity among the stakeholders, including customers, businesses, and government agencies. Many people are not aware of the risks associated with cyber threats and do not take adequate measures to protect themselves and their data. The lack of awareness is compounded by the lack of cybersecurity skills and expertise in Cameroon, which makes it difficult to develop and implement effective cybersecurity strategies[69]. It is on this note that there have been so many data breaches and identity theft in Cameroon without the victims being aware. For example, the National Social Insurance Fund in Cameroon (NSIF) face data breached in 2024 by a notorious hacking group "*Space bears"* which infiltrated the institution's systems exposing 10GB worth information which exposed personal data of over 1.5 million Cameroonians without knowledge of the institution.

[65] Section 7 (1) 2010 law (*supra).*

[66] Jean Lois Beh Mengue, General Manager "Regulating is Facilitating" TRB 2016.

[67] Cameroonweb (*supra)*

[68] *See supra*.

[69] Cybersecurity in Cameroon's Telecommunications sector: challenges and solutions, 2023. ISP. Page 2. Available at https://isp.page>news. Accessed 14/03/2025.

3.1. NO SPECIFIC DATA PROTECTION LAW

The 2010 law on cybersecurity provides that electronic communications and information systems content providers shall be bound to conserve such content and stored data in their installations for a period of ten (10) years. This is a challenge because there is no specific data protection law and as such, there is no specific data protection commission which has been put in place to follow-up or to make sure that the data collected should be preserve or protected.

3.2. SATURATED TELECOMMUNICATION NETWORKS

The saturated telecommunication markets force operators to launch cheaper subscriptions and promotions thereby encouraging SIM Box fraudsters. For example, simbox[70] fraudsters become more and more sophisticated using high –tech equipment incorporating the least new features to hide their activities[71]. This type of fraud is persistent and unavoidable in that the fraudsters use prepaid sim cards in which their ownership and address are much harder to trace compared to the easily traceable post-paid Sims. This problem is serious particularly in Cameroon and in other countries where the incoming inter traffic rates are high and controls tax in terms of availability of Sims and law enforcement[72].

Also, the issue of subscriber chun rate between operators in the market. The telecommunication industry operates in a low customary loyalty environment, so, fraudsters usually take advantage of cheap packages including bundles offer which earn lower per- minute revenue to the operator than the interconnect rate they can earn from the Inter carriers. Due to this highly competitive market and low customer, the loyalty phenomenon, the cost of all- inclusive bundles is driven down. Fraudsters are smart technologically aware and know how to outbox local operators. Experts are masking themselves; they host their equipment where their calls can reach multiple cell sites and get widely dispersed, and they send out artificial SMS messages or accept a few incoming calls. This is to mask their true intent. This significantly causes operators to lose revenues on calls and also see degraded call quality which prevents them from meeting SLAS for mobile hobbling traffic[73]. Here, machines that housed simcards redirect the illegal VOIP trafficking on the networks. Fraudsters effectively 'bypass' the interconnect toll charging points to exploit the different between the high interconnection rates and the low retail price for on-network calls, thus avoiding payment of the official termination fee of an operator or MVNO[74].

3.3. THE COMPLEX NATURE OF THE LAW

The 2010 law allows criminal and investigation officers to gain access to users' data from Internet Service Providers (ISP) and ICPs without limitation to time and circumstances. Also, ISP and ICPs are bound to store contents and data for a period of 10 years, but the exact data that must be stored are not clearly defined[75]. However, this makes the prosecution and punishment of cybercrimes problematic.

---

[70] A simbox is also called a "simbank". It is one of the hardware modules of ANTRAX solution for GSM terminat -ion. A simbox device holds a bundle of simcards separately from VOIP/ GSM gateway in order to minimize the maintenance, expenses and reducing the sim blocking issue. A simbox is a set up in which fraudsters install simboxes with multiple low cost prepared Simcards. The fraudsters then can terminate international calls through local phones in the respective country to make it appear as if the call is a local call. With this, fraudsters bypass all inter- connection charges.

[71] For more details see Info@keynote-sigos.com. Also see Nemesy Co. Ltd.support@nemsysco.com/bizdev@nemesysco.com.

[72] Ashu Pauline M., (2019). "Formation of Online Contracts in the Digital Age and Established Common Law Principles: Prospects and Challenges", Ph.D Dissertation, University of Yaoundé II – Cameroon, p. 286.

[73] Ashu Pauline M, (2019). S*upra,* p 287. See also, 2013 Report on Communications Fraud Control Association (CFCA). Available at: https://www.xintec.com/fraud-mangement/what-is-simbox-fraud-and-why-is-it-so-hard- to-beat. Accessed 08/03/2025.

[74] See s*upra.*

[75] Internet Governance Forum (IGF)- Cameroon, "Securing the Cameroonian Cyberspace
Through the Computer Incident Responsible Team (CIRT), presented by Besong John Ebot at University of Bamenda – Bambili, 18-20 June, 2014, available at www.igf.cm. Accessed 11/03/2025.

4. RECOMMENDATIONS

Since the security of cyberspace is very important to a country like Cameroon, there is need to address the challenges that are encountered in the implementation of the 2010 law.

4.1. INCREASE AWARENESS AND UNDERSTANDING OF CYBERSECURITY.

Increase awareness and understanding cybersecurity among stake holders is one of the recommendations that has been put in place. This can be achieved through public education campaigns, training programs, and workshops that provide information on the risks associated with cyber threats and the measures that can be taken to protect against them[76].

4.2. ORGANISATIONAL POLICY

Organizations need to realize that today and future network architectures which take advantage of cloud technologies and Internet of Things (IoT) require security at every point where mobile phone, laptop, sensor or API makes contact with the network. This could even be from within, not the perimeter in its traditional sense. So, a little bit of more training and awareness is perhaps required. Also, the practice of using other IT personnel like engineers or application developers to take on the role security specialists has as impact on the organization's readiness to fight cyber-attacks. Without the right cybersecurity skills, the infrastructure and applications will not be adequately protected against attacks.

4.3. INFORMATION SECURITY STANDARDS

Most organization implement international information security standards and technology (NIST) framework. In Cameroon however, it was found that focus is on ANTIC's regulations as spelled out in the 2010 law on Cybersecurity and Cybercriminality where organizations are made to pay huge penalties of up to fifty million (50.000.000) FCFA if they do not comply with certain requirements of the law[68]. Nevertheless, it requires that operators of information systems should take every technical and administrative measures to ensure the security of services offered.

4.4. POLICY RECOMMENDATION

Generally, the 2010 existing law seem to have a positive impact on the cybersecurity posture of Cameroon due to the hefty fines meted out in the laws, especially for organizations not taking all necessary steps to secure their infrastructure. However, the laws do not consider that some smaller companies who operate an information system in order to provide their services and products to their customers may not have the large investment and budget usually required to properly secure information systems. This might be where a national strategy on cybersecurity might help define how the go plans to encourage and incentivize the private sector to comply with the passed cybersecurity laws and regulations. Tax incentives or other ideas of how small companies may afford security solutions to protect their information systems should be an important aspect for such a strategy.
Also, it might be helpful to classify companies into different structures and into different categories. This will clearly indicate which sectors, systems and infrastructure which are critical and which are not. It is unreasonable to expect a hotel that uses and operates information systems to run their telecommunications company or a hospital classifying information system is either critical or non- critical infrastructure would make the regulation less of a financial burden to those sectors that are not considered critical.

[76] Cybersecurity in Cameroon's Telecommunications Sector: Challenges and Solutions, 2023. ISP. Page 3. At https://isp.page>news. Accessed 14/03/2025.

5. CONCLUSION

In conclusion, the 2010 law on cybersecurity is very important because it protects all categories of data from theft and damage, protects health, personal information, intellectual property, etc. Nevertheless, the importance of this law cannot be over-emphasized because of the challenges it faced. But, some recommendations have been put in place for smooth cybersecurity law in Cameroon.

REFERENCES

1. 2006 E- Crime Watch Survey", p. 1, available at: http://www.cert.org/archive/pdf/crimesurvey06.pdf. Accessed 06/03/2025.
2. 2013 Report on Communications Fraud Control Association (CFCA) https://www.xintec.com/fraud-mangement/what-is-simbox-fraud-and-why-is-it-so-hard- to-beat/. Accessed 08/03/2025.
3. Adam Hayes, (2022). "Electronic Communication Network (ECN): definition and Examples", Investopedia.
4. Ashu Pauline M., (2019). "Formation of Online Contracts in the Digital Age and Established Common Law Principles: Prospects and Challenges", Ph.D Thesis, University of Yaoundé II – Cameroon.
5. Ashu Pauline M., (2022). "Fighting Cybercrime Threats in Africa: A Legal Appraisal", L*' Harmattan,* Tome 3, Pp 345-367.
6. Boraine A. (2019). "Situational Analysis of Digital Security in Cameroon". Retrieved at: http://Cameroon_Digital_Security_Situational_Analysis.pdf . Accessed 04/08/2025 : (Pp 1-14).
7. Boraine A. and Ngaundje L., (2019). "Fighting Cybercrime in Cameroon" International Journal of Computer (IJC), ISSN 2307-4523 (Print & Online), Vol. 3, No 1, Pp 87-100.
8. Cameroon Computer Incidence Response Team Cybersecurity Annual Report 2014.
9. Cameroon Data Protection Overview. Available at: https://www.dataguidiance.com.ca. Accessed 09/03/2025.
10. CameroonWeb, Telephones and Communications, (2014-2016). Available at: http://www.cameroonweb.com/cameroonHomePage/Privacy_Policy.php. Accessed 08/03/2025.
11. CIRT Cybersecurity 2014 Annual Report, p. 8, Table 10.
12. Cyber Security Lecture Notes, B Tech III-Year, 2020-2021, Department of CSE, Malla Reddy Col (2019) Lege of Engineering and Technology, India, Pp 1-37.
13. Cybersecurity in Cameroon's Telecommunications Sector: challenges and solutions, 2023. ISP. Page 2. Available at https://isp.page>news. Accessed 14/03/2025.
14. Data Encryption, Parliament office for Science and Technology No. 270, 2. No. 2, April 2012.
15. Decree No 2013/0399/PM of 27 February 2013 on the Modalities of Consumers' Protections in the Electronic Communication.
16. Decree No. 2002/092/PR of 8th April 2002 which Facilitates and Accelerates the uptake of ICTs in Cameroon.
17. Decree No. 2012/180/PR of 10 April, 2012 relating to the organization and functioning of the National Agency for Information and Communication Technology (NAICT).
18. D. Moukouri, (2020). "Data Protection Overview in Cameroon", *LEXAfrica.* Available at: https://www.lexafrica.com/2020/03/data-protection-overview-in-Cameroon . Accessed 20/03/2025.
19. European Convention on Human Rights and the Human Rights Act 1998.
20. Gefona Statement to United Nations Informal Multi-Stakeholder cyber Dialogue on Cyber Capacity Building, 2020, available at: https://www.antic.cm/images/stories/laws/law%20relating%20to%20cybersecurity%20andcybercriminality%20cameroon.pdf. Accessed 11/03/2025.
21. Law No 2010/013 of December 21, 2010 relating to Electronic Communications in Cameroon.
22. Law No 2015/006 of April 20, 2015 regulating electronic Communication in Cameroon.
23. Law No. 2010 /012 on Cybersecurity and Cyber criminality in Cameroon.

24. Law No. 98/014 of July, 2010 to regulate telecommunications in Cameroon. 24. Mohammad Talid, (2012). Cyber Forensics: Computer Security and Incident Response, International Journal of New Computer Architectures and Their Applications (IJNCAA), 2(1): 127-137, ISSN: 2220-995.
25. Nemesy Co. Ltd.support@nemsysco.com/bizdev@nemesysco.com.
26. Perspectives : Cryptography. Available at: http://www.terrorismcentral.com/library/treasers/Flamm.html. Accessed 07/03/2025.
27. Seminar of 12 November, 2011 held at the Yaoundé Conference Hall on Cybersecurity in Cameroon.
28. Seminar on "Cyber-criminality and its Consequences in Cameroon", held in Yaoundé, 8th July 2015. Presented by Besong John Ebot, Telecommunication Engineer.
29. Sylvie Siyam and Serge Daho, (2014) "The Stammering of Cameroon's Communications Surveillance", Global Information Society Watch. Available at: www.protegeqv.org/ . Accessed 09/03/2025.
30. Tomslin Samme-Nlar, (2021). "Cybersecurity in Cameroon Enterprises: What we Learnt", GEFONA Digital Foundation.
31. U k, 2006, p. 3. Available at: http://www.parliament.uk/documents/upload/postpn270.pdf. Accessed 02/03/2025.
32. Vigiline Tise, (2021). "Privacy Protection in Electronic Communications Under Cameroon Law", Nico Halle & Co Law Firm. Available at: https://www.hallelaw.com/privacy. Accessed 16/03/2025.