

The Impact of Spam and Privacy Concerns on Electronic Communication Users in Cameroon

Enow Godwill Baiye*

Abstract

This article is centered on spams and the violation of the right to privacy under Cameroonian electronic laws. The results of this work shows that spams have undoubtedly become a major source of violation of the right to privacy in Cameroon. This is attributed firstly, to the general and sparsely nature of the laws in this domain. Secondly, the lukewarm attitudes of electronic communication users who care less about such messages, gives spammers the opportunity to constantly send such messages with no fear of being punished by the law. From our findings, it was recommended that the 2010 cyber law that has existed for 12 years should be revised as it sparsely addressed the issue of spam. Also, more resources should be put at the disposal of ANTIC to enable them combat this digital evil. Electronic communication users should take the bull by the horn by enforcing their rights against spammers.

Keywords: Spam, spammers, privacy, users, cybercrimes, electronic communication

INTRODUCTION

Background and Justification to the Study

The advent of technology has facilitated the means by which people now communicate from distance. It has equally eased the means by which mails are transmitted. E-mail is one of the most popular internet services for instant and convenient message delivery today. Unfortunately, the problems associated with e-mails cannot be overemphasised. They have become a channel through which unsolicited and unwanted spam mails are spread [1]. Spam is a form of cybercrime [2]. The 2010 cybersecurity and cybercriminality law in Cameroon regulate cybercrimes. The issue of spam emails has become a globe problem. It affects users of both developed and developing countries with Cameroon not been an exception. According to ANTIC report, it was estimated that Cameroon lost 12.2 billion to cybercrime in 2021 [3]. Most advertising companies use spams because of its low operating costs when compared to normal emails [4].

The term “spam” has been defined differently by scholars. Spam is defined as unsolicited electronic mail, most of which takes the form of commercial advertising [5]. Spams are also taken to mean unsolicited bulk email. Spamming messages are not only found on spam emails. Other sources include instant messages spam, spam in blogs, mobile phone messages spam and internet forum spam [6]. From the definitions, the term “unsolicited” can be deduced to mean that they were never not demanded by the users and were sent without their permission. This therefore constitutes violation of one’s fundamental right to privacy as enshrined in international, regional and national legal instruments.

*Author for Correspondence

Enow Godwill Baiye
E-mail: enowgodwillbaiyebaiye@gmail.com

Ph.D. in English Private Law, University of Dschang,
Cameroon

Received Date: August 17, 2022
Accepted Date: August 29, 2022
Published Date: September 07, 2022

Citation: Enow Godwill Baiye. The Impact of Spam and Privacy Concerns on Electronic Communication Users in Cameroon. National Journal of Cyber Security Law. 2022; 5(1): 12–19p.

Research Questions

It is in the light of the foregoing problems that this work seeks to answer the following research questions:

- Are spams violation of the right to privacy under Cameroonian electronic laws?

- What are the impacts of spam on users of electronic communication in Cameroon?
- What are the hurdles to the criminalisation of spammers in Cameroon?

Research Objectives

The following objectives guide this study in order to address the aforementioned issues:

- To examine if spams constitute violation of the right to privacy under Cameroonian electronic laws.
- To examine the impacts of spam on users of electronic communication in Cameroon.
- To discuss the hurdles encountered in the criminalisation of spammers in Cameroon.

Research Hypothesis

This paper assumes the following:

- According to Cameroonian electronic laws, spam does not violate the right to privacy.
- There exist repercussions of spams on users of electronic communication in Cameroon.
- Criminalisation of spammers in Cameroon still remains an emerging challenge that the government is combatting with.

Research Methodology

This work uses the doctrinal method, consisting of primary and secondary data. Photographs constituted primary sources of data for the work. The sources of secondary data used for the development of this work were gotten from books, articles and websites. The content analyses of legal and institutional frameworks were used to analyse the data for the developing of this work.

CHARACTERISTICS OF SPAMS

Spams which now constitute a threat to many internet users has the following distinctive features:

- They are unsolicited by their users;
- Spammers send spam messages to large number of recipients;
- There are often missing or malformed message ID;
- The sending field is usually empty. A typical email must be send 'To';
- From: field is the same as the To: field;
- There is usually an inscription: why is this message in spam?
- There is also a message: report not spam
- Equally, spam messages have unique signs as seen in the pictures below:

PRIVACY AS AN OVERARCHING RIGHT

The study of privacy in the digital age is not new. The right to privacy is a fundamental universal right enjoyed by all irrespective of the persons' race, sex, and ethnicity. One of the ills with the digital age is that it came along with a new evil which is the violation of one's privacy through spams Figure 1. This section of the work is devoted to first of all look at the conceptual meaning of the right to privacy as a whole, followed by the legal basis of this right and at the end, established a concrete relationship between spamming and the right to privacy in Cameroon.

Conceptual Meaning of the Right to Privacy

The term "*privacy*" is not a new concept. It is a word that has existed in antiquity. For better understanding of the word, **Stone, E.F. & Gardner, D.G., [7]** purports that privacy is "the ability of the individual to control personal information about himself. Privacy also means freedom from unlawful interference of one's personal information. Similarly, Privacy means non invasion/intrusion of one's personal information without his permission. The concept of privacy as used in this work is limited to digitalised setting. Hence within the context of this work, we strongly affirm that the right to privacy is the right enjoyed by all human beings by which no personal information of his is to be accessed without his consent.

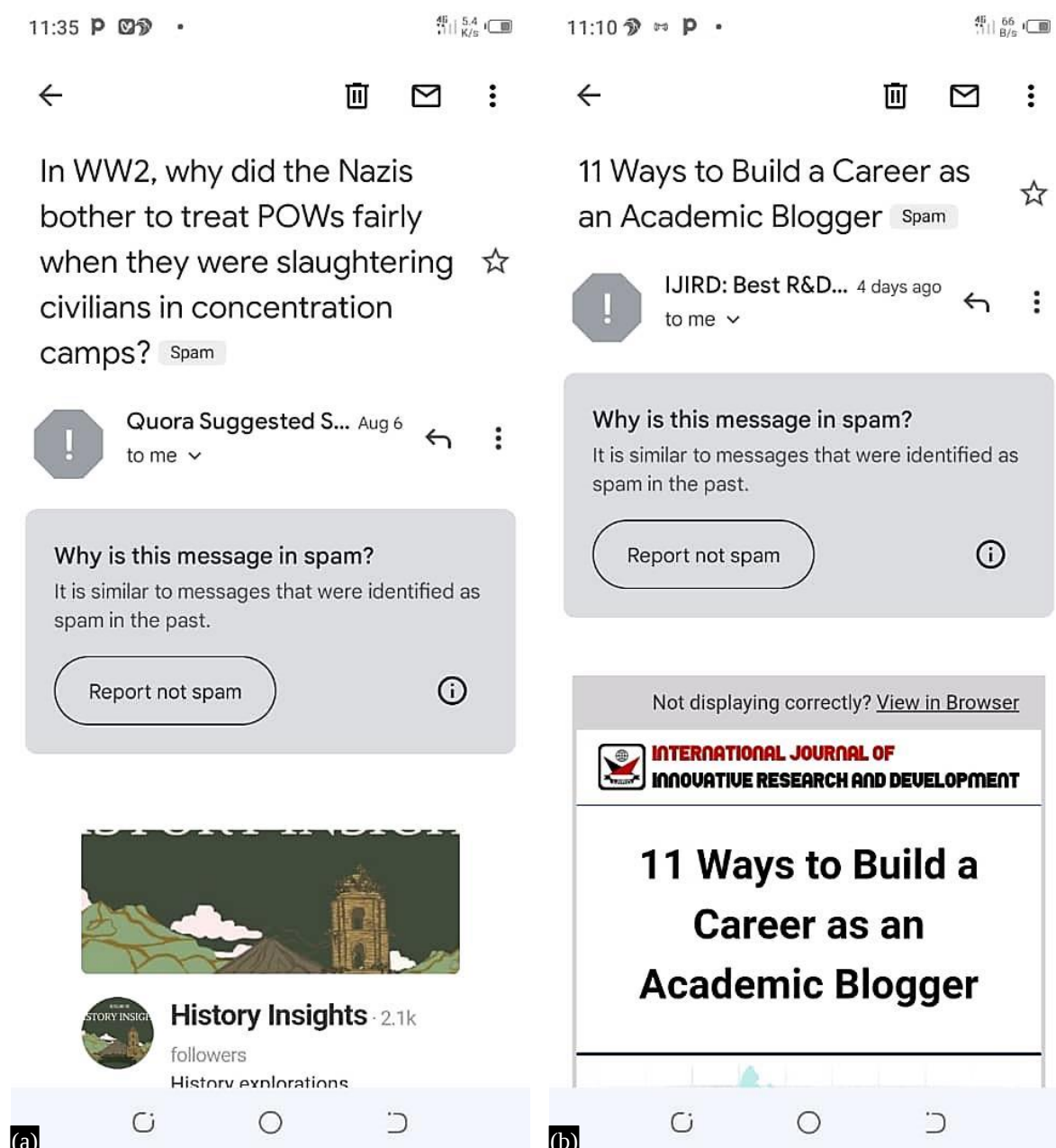


Figure 1. (a, b) Typical example of spam email.
Source: Personal spam email (2022)

The Legal Contour of the Right to Privacy in Cameroon

Though the concept of privacy has greatly evolved over the years, it remains a fundamental right that is embedded in several legal instruments. The Universal Declaration of Human Right (1948) strongly upholds this right [8]. The International Covenant on Civil and Political Rights Act (1966) [9] as well as in the International Convention on the Protection of Migrant Workers and Members of their Families, [10] the CEMAC Directive on the protection of the rights of users of the electronic communication in the CEMAC region are all legal instruments that recognises the right to privacy [11].

The right to privacy is a constitutional right embedded in the preamble of the Cameroonian Constitution [12]. The right to privacy for electronic communications users in Cameroon is equally regulated by the law on cybersecurity and cyber criminality in Cameroon. The law has as goal to

promotes trust in the use of electronic communication networks across the national territory as well information systems in Cameroon. The legal framework for digital evidence, security, cryptography, and electronic certification is well defined. Finally, the law protects basic human rights particularly the respect of the right to privacy [13]. Any content that infringes on human dignity, privacy, honour or national security are considered as illegal content as with the case of spam messages under the ambit of the law [14]. The law also contains provisions on the maintenance of confidentiality when it comes to electronic communication [15]. Section 41-48 of the law explicitly contains provisions on privacy in relation to electronic communication.

Similarly, the law holds content providers liable for data transmitted through their information system, particularly if such content involves an infringement of human dignity, injury to character, or invasion of privacy [16]. The law also prohibits sending electronic messages for prospecting purposes that conceal the sender's identity or don't contain a valid address to which the addressee may send a request to block such information. The sending of electronic mails while impersonating another user is strictly prohibited under the law [17].

Furthermore, the 2013 Decree on the modalities of the consumers' protection in the electronic communication sector provides inter alia that "*consumers in the electronic communication sector have the right in the consumption of technologies, goods and services in the electronic communication sector [18]*".

Measures in combatting spams to users

One of the measures used to fight spam emails in Cameroon is through criminal mechanisms. These are measures which are repressive in nature. They entail death sentences, imprisonment and payment of fines. The 2010 law contains repressive sanctions with the aim of punishing individuals and corporate bodies who violates one's right to privacy using electronic messages [19]. Persons who use illegal means to collect the personal data of another and thus violate their privacy are also subject to legal penalties [20].

Accessory and preventive sanctions are both measures aimed at reducing spam distribution to users. Sections 19 and 20 of the Cameroonian Penal Code govern them, respectively. The 2010 law expressly allows judges to impose such sanctions. To that end, the law states unequivocally that judges may use sequestration or seizure to prevent or end invasions of one's privacy [21], and seizure of the device used to commit the crime. The competent court's decision may also be published in any format [22].

As a state agency, ANTIC plays an administrative role in the fight against spam. The role of this body is well defined within the framework of Decree No. 2012/180 of April 12, 2012, on the organisation and operation of ANTIC. ANTIC's tasks on behalf of the state include regulating and monitoring activities related to the security of electronic communication networks and information systems within the confines of sections I and II of Chapter II. They also govern the application of electronic certification [23]. They are specifically responsible developing and implementing a national strategy for computer technology development [24]. ANTIC has the power to investigate, grant an injunction, implement coercive measures and repressive sanctions to enable them perform their job [25].

EFFECTS OF SPAMS

The effects of spam messages are as follows:

- They have the potential to spread viruses and other malware. Malware are set of instructions that runs on one's computer and can caused the system to be easily attacked [26].
- They have become channels to collect vital formations from users.
- Spams easily promotes frauds and can lead to the displacement of legitimate mail.

- It undermines the confidence users have on the use of emails.
- It constitutes threat to the privacy enjoyed by e-mail users consequently, affecting their welfare as much of their data will be used for receiving junk messages.
- Spam messaging constitute a common form of inconvenience to Internet users as they will constantly required to delete the unwanted messages manually. This is time sapping to the users.
- Indirectly, spams have resulted to mail harassment, child pornography, phishing, and deceptive marketing [27]. Mail harassment is clearly seen in photos showing from the researcher personal email gotten from his spam (Figure 2).

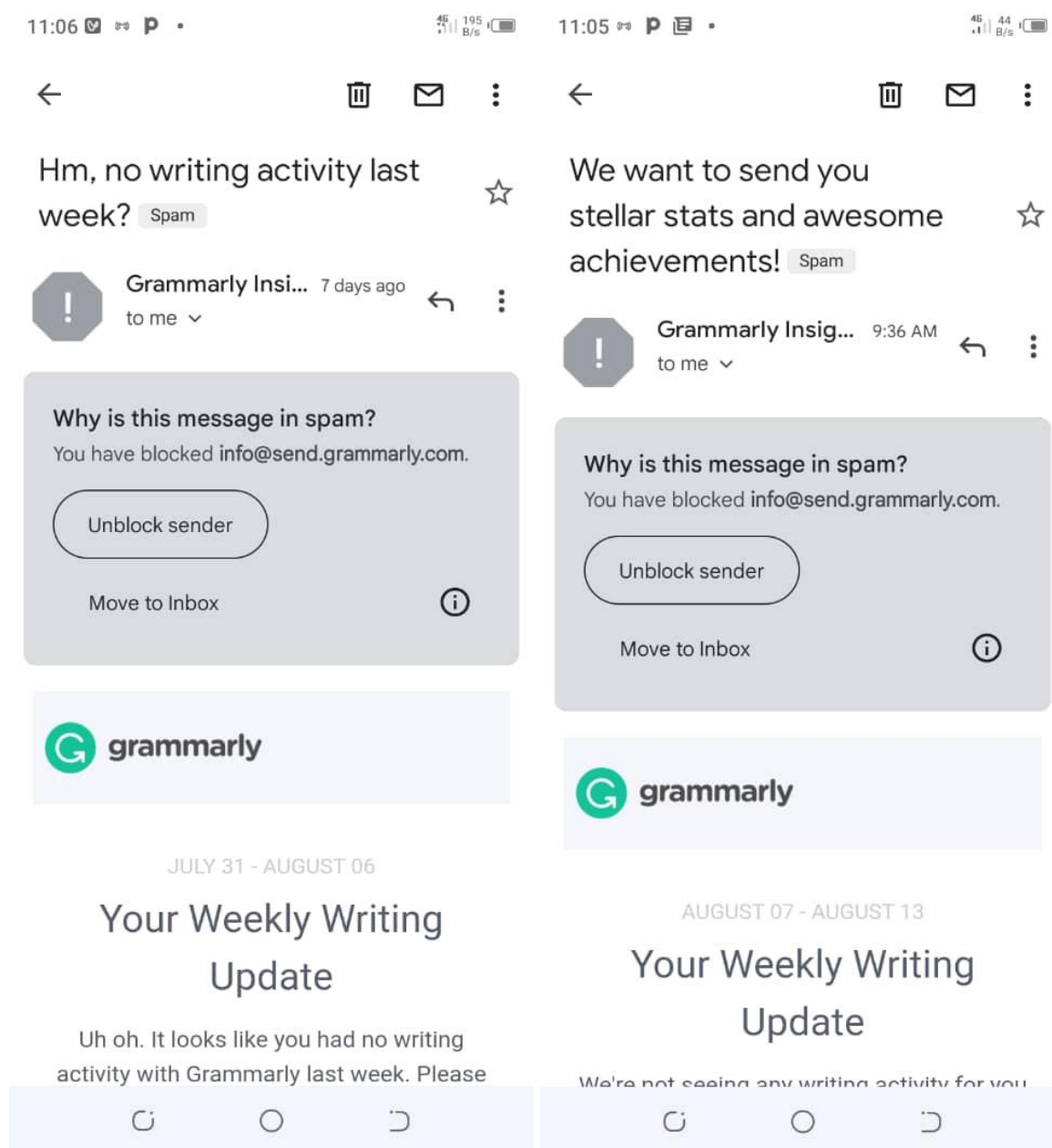


Figure 2. Constant repeated spam email from the same sender.

Source: Personal spam email (2022)

DILEMMA OF COMBATTING SPAMS IN CAMEROON

There are many limitations that have undermined the fight against spam mails to electronic communication users in Cameroon.

Inadequacy of the Laws

Cameroon like any other country has made considerable efforts to fight against cybercrimes. This effort was seen 12 years ago with the enactment of the 2010 law on cybercrimes in Cameroon. This was the first piece of legal framework that addresses issues relating to cybersecurity and cybercrimes within the national territory. However, this piece of legislation is not free from limitations. The law is too general and sparse. It fails to address issues of spamming. The law did not in any provision portrays spamming as a crime. This ambiguity gives room for electronic communication users to constantly receive unsolicited spam messages without their consent, hence amounting to violation of their right to privacy.

Persistent Infringement to the Right of Privacy

One thing the law ought to protect is one's right to privacy with the advent of technology. It is a common practice in Cameroon for electronic communication users to constantly receive junk spam messages in their mails and phones inspite of the existence of Decree no 2013/03399/PM of February 2013 which aims at protecting the electronic communications of consumers. This violated one's constitutional right to privacy. The government has not made this situation any better as they themselves violates one's rights to privacy through internet censorship. ANTIC [28] uses the state-of-the-art tools or cutting-edge tools to continuously watch social networks [29].

Illiteracy on the Part of Electronic Communication users

Most electronic communication users in Cameroon lacked the required knowledge in the operation of electronic gadgets. As a result of this, they do not know what spam messages are and even how to block the spammers. This gives spammers the opportunity to constantly send their unsolicited publicity or advertisement to their mails. At times, even those who have the basic knowledge in computing becomes lukewarm in enforcing their rights that have been violated.

Difficulties in Bringing Legal actions Against Spammers

Criminalising spammers remained one major debacle in combatting spamming and the right to privacy. Most of the spammers are multinational and foreign based companies. Suing these companies requires lots of money and legal expertise. The lack of these financial and human resources leaves users with no choice than to waive their rights. In addition, most of the spam emails do not carry the real identity of the senders.

CONCLUSION

Summarily, this paper has examined how spam constitute violation of one's right to privacy which advocates for unlawful interference with one's personal information without his consent. The paper provided an in-depth discussion of what spams are and the legal instruments protecting the right to privacy. The effects of spam mails were also examined in the course of our discussion. The outcomes of this paper points that though Cameroonian government has taken initiatives to enact laws in the domain of cybercrimes, the efforts still remain insufficient.

To improve in this area of the law, the following are recommended: the law on cybercrimes should be amended considering the fact that it was enacted 12years ago and fails to address succinctly the issues of spamming. New cyber offences must have evolved and are not addressed in the law. In addition, the repressive sanctions should be reconsider considering the danger spams possess to one personal information and electronic gadgets.

Sensitizing and educating consumers of electronic communication on the dangers of spams can also be a possible solution to the eliminate or reduce the spread of spam messages. They should be taught on how to block or black list spam emails or messages in general. ANTIC should therefore intensify their role in raising cyber threat awareness in Cameroon. The legal assistant department should be made known by the government to the general public to reduce the financial burden of those whose

right to privacy has been violated by spam but lack the financial and human resource to institute an action against defaulters.

REFERENCES

1. Neumann, P., and Weinstein, L., (1997), "Inside Risks: Spam, Spam, Spam! ," *Communications of the ACM*, Vol. 40(6), P. 112.
2. Cybercrimes as defined within the ambit of section 4 (32) of the 2010 law are: infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes.
3. Business in Cameroon, (2022) Stratline Limited.
4. Cyber security: spam, scams, frauds and Identity theft. Available at [https://mediasmarts.ca/digital-media-literacy/digital-issues/cyber-security/cyber-security-spam-scams-Frauds-Identity theft](https://mediasmarts.ca/digital-media-literacy/digital-issues/cyber-security/cyber-security-spam-scams-Frauds-Identity%20theft). (Lastly Accessed on the 17th of August, 2022).
5. Cournane, A., and Hunt, R., (2004), "An Analysis of the Tools used for the Generation and Prevention of Spam," *Computers & Security*, Vol. 23(2), P. 154.
6. Andreas Jacobsson, (2008), *Privacy and Security in Internet-Based Information Systems*, Blekinge Institute of Technology, Printfabriken, Karlskrona, Sweden, P.52.
7. Stone, E.F., Gardner, D.G., Gueutal, H.G., & McClure, S., (1983), "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*, Vol. 68(3), P. 459.
8. Article 12 of the 1948 UDHR. Strongly rebukes anyone who arbitrarily interferes with another's privacy, family home or correspondence.
9. Article 17 of the International Covenant on Civil and Political Rights Act.
10. Article 14 of the International Convention on the Protection of Migrant Workers and Members of their Families.
11. Article 3 of CEMAC Directive N0. 07/08-UEAC-133-CM-18 laying down the Legal Framework for the Protection of the Rights of Users of the Electronic Communication in the CEMAC Region.
12. The preamble of the Cameroonian Constitution affirms that the privacy of all correspondence is inviolate. No interference may be allowed except by virtue of decisions coming from the judicial power
13. Section 1 & 41 of Law N° 2010/012 of 21 December 2010 relating to Cybersecurity and Cyber Criminality in Cameroon.
14. *Ibid*, Section 4(26).
15. *Ibid*, Section 4(24) provides that there shall be maintenance of the confidentiality of information and transactions to prevent unauthorized disclosure of information to non-recipients enabling the reading, listening, intentional or accidental, illegal copying during storage, processing or transfer.
16. *Ibid*, Section 43.
17. *Ibid*, Section 48(1)(2).
18. Decree No. 2013/0399/PM of 27 February, 2013 on the Modalities of the Consumers' Protection in the Electronic Communication Sector.
19. Section 74(1) of the 2010 Law on Cybersecurity and Cyber Criminality punishes persons with imprisonment from 1 to 2 years and a fine from 1,000,000 to 5,000,000 CFA francs who uses any device to receive the privacy of another person by attaching, recording or transmitting private or confidential electronic data without the consent of the persons
20. With imprisonment from 6 months to 2 years or a fine from 1 000,000 to 5,000,000 CFA francs or both of such fine and imprisonment.
21. *Ibid*, Section 41.
22. *Ibid*, Section 64(4).
23. Article 4 of Decree no 2012/180 of 12 April 2012 on the organisation and functioning of ANTIC
24. *Ibid*, Article 5; Other specific functions are: to identify software and computer equipment that will be relevant for public service needs; contribute in the harmonization of technical standards as well as proposing technical repositories, to promote interoperability between information system;

coordinate the implementation and monitoring of websites ,intranet and extranet of the state and public bodes; contribute to the technical training to train universities, colleges, high schools colleges; to put in place measures to ensure internet security amongst others.

25. Ibid, Article 7.

26. Skoudis (2004), *Malware- Fighting Malicious Code*, Prentice Hall PTR, Upper Saddle River, NJ.

27. Andreas Jacobsson, (2008), *Privacy and Security in Internet-Based Information Systems*, Blekinge Institute of Technology, Printfabriken, Karlskrona, Sweden, P.58.

28. National Agency of Information and Communication Technologies.

29. Ngaundje D., Leno, (2021), “An Appraisal of the Law on Consumer Protection in Cameroon with Respect to Technology Products”, *International Journal of Science and Research (IJSR)*, Vol. 10 (2), PP. 828-835.