Paradigm Academic Press
Law and Economy
ISSN 2788-7049
MAR. 2026 VOL.5, NO.1

A Legal Assessment of the Effectiveness of the Measures to Fight Against Scamming in Cameroon: The Case of Buea

Dr. NTOKO NTONGA Rene[1] & LIDVIN ADRAIN ZANGA[2]

[1] Money Laundering Legal Consultant, University of Buea, Cameroon

[2] Master's in Business Law Candidate, University of Buea, Cameroon

Correspondence: Dr. NTOKO NTONGA Rene, Money Laundering Legal Consultant, University of Buea, Cameroon.

doi:10.63593/LE.2788-7049.2026.03.009

Abstract

This study provides a comprehensive legal assessment of the effectiveness of anti-scamming measures in Cameroon, with specific focus on Buea. Scamming has emerged as a pervasive socio-economic challenge undermining public trust and causing significant financial losses across diverse sectors. The research critically examines the existing legal and institutional frameworks designed to prevent, detect, and penalize scam-related offenses, including relevant statutory provisions, enforcement mechanisms, and judicial practices. The primary objective is to evaluate how effectively these measures curb scamming activities within the Buea municipality and to identify gaps hindering optimal legal protection. The study adopts a mixed-methods approach, combining both qualitative and quantitative data. Data were collected through semi-structured interviews with key stakeholders — including law enforcement officers, legal practitioners, victims of scamming, and local government officials — to capture nuanced insights into the practical challenges of enforcement. Additionally, survey questionnaires were administered to a representative sample of residents in Buea to quantify public perceptions of scamming prevalence and the perceived efficacy of legal measures. Relevant legal documents, policy instruments, and case law were also reviewed as part of a documentary analysis to map the statutory landscape and enforcement patterns. Quantitative data from surveys were analyzed using descriptive and inferential statistical techniques to identify trends and correlations between demographic factors and perceptions of legal effectiveness. Qualitative interview data and documentary evidence were subjected to thematic analysis, enabling the identification of recurrent patterns, institutional strengths, and systemic weaknesses. Findings reveal that although Cameroon has enacted several legal instruments to combat scamming, enforcement remains weak due to limited resources, procedural inefficiencies, and low public awareness. The study concludes with recommendations for legal reform, enhanced institutional capacity, and community-based anti-scamming initiatives to strengthen the overall fight against scamming in Buea.

Keywords: legal assessment, effectiveness, measures, fight, scamming, Cameroon

1. Introduction

Scamming, particularly in the form of cyber-enabled fraud, represents one of the most pervasive and rapidly evolving threats to socioeconomic stability in Cameroon. Scamming activities, including phishing, identity theft, fraudulent investment platforms, and electronic payment fraud, have resulted in substantial financial losses for individuals, businesses, and the state. In 2025 alone, authorities reported that more than CFA 1.027 billion was lost to online scams, with 471 cases of scamming and phishing documented nationwide.[1] Scammers often

[1] StopBlablaCam. (2025, December 17). Cameroon loses over CFA 1 billion to cybercrime in 2025. Available at https://www.stopblablacam.com/society/1712-15499-cameroon-loses-over-cfa1-billion-to-cybercrime-in-2025. Accessed on 12/12/2025.

exploit digital platforms to impersonate trusted institutions, deceive users, and redirect funds into illicit channels, illustrating both the scale and sophistication of modern scamming operations in the country.[1]

In response, Cameroon has developed a legal framework aimed at combating cybercrime, including the scamming phenomenon. Central to this framework is Law No. 2010/012 on Cybersecurity and Cybercrime, which criminalizes a range of digital offenses and prescribes penalties intended to deter and punish offenders. For example, provisions such as Article 73 of the Cybercrime Law impose significant imprisonment terms and fines for fraudulent use of information systems or electronic communications for personal gain.[2] Despite these statutory measures, enforcement challenges persist. Judicial authorities and law enforcement agencies often face resource constraints, limited technical expertise, and procedural hurdles in investigating and prosecuting cyber-enabled scamming cases effectively.

The city of Buea provides a particularly relevant case study for analyzing the effectiveness of anti-scamming legal measures at the local level. As an urban Centre with a growing digital economy and active youth population, Buea experiences both traditional fraud and increasingly sophisticated online scams.[3] Moreover, the interaction between local law enforcement, judicial actors, and affected communities sheds light on the practical strengths and weaknesses of existing legal responses. Evaluating these dynamics is essential for understanding not only the formal legal framework but also how it functions in practice to deter, detect, and adjudicate scamming offenses within a Cameroonian context.

This study therefore undertakes a systematic legal assessment of anti-scamming measures in Cameroon, with a specific focus on Buea. It examines the scope and application of relevant laws, enforcement mechanisms, and key institutional actors involved. It also situates the legal framework within broader trends of cybercrime prevention, enforcement capacities, and community perceptions of scamming and justice. By doing so, this research contributes to ongoing discussions about legal reform, capacity-building, and strategies to enhance the effectiveness of anti-scamming efforts in Cameroon.

2. Overview of the Meaning and Nature of Scamming in Cameroon

Scamming generally refers to a form of fraud in which a person intentionally deceives another through false representations, misstatements, or dishonest schemes with the aim of obtaining an unlawful financial or material benefit. In legal terms, scamming is rooted in the broader concept of fraud (*escroquerie*), which involves the use of deceit to induce a victim to part with property, money, or rights.[4] Although Cameroonian legislation does not always employ the term *"scamming"* expressly, the conduct it describes is clearly captured under various statutory provisions addressing fraud and cyber-enabled criminal activities.

In Cameroon, scamming is primarily understood through Law No. 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality, which criminalizes fraudulent practices committed through information and communication technologies.[5] This law reflects an expanded legal understanding of fraud to include digital and electronic means, such as the manipulation of electronic data, impersonation, phishing, and fraudulent electronic transactions. Internationally, bodies such as the United Nations Office on Drugs and Crime (UNODC) describe scamming as a form of computer-related fraud involving the intentional input, alteration, or use of data to obtain economic advantage unlawfully.[6] This definition aligns closely with the Cameroonian legal position, particularly in the context of online and technology-driven scams.

Beyond cybercrime legislation, the traditional concept of fraud under the Cameroonian Penal Code also informs the meaning of scamming.[7] Fraudulent misrepresentation, abuse of confidence, and false pretences — long recognized under criminal law — constitute the legal foundation upon which modern scamming offenses are built. Thus, in the Cameroonian context, scamming may be understood as both a traditional criminal offense and

---

[1] *Ibid.*

[2] UNODC. (2010). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Article 73 [Law on cybersecurity and cybercrime]. United Nations Office on Drugs and Crime. Available at https://www.unodc.org/cld/fr/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/article_73/article_73.html. Accessed on 12/12/2025.

[3] Ibid.

[4] Federal Trade Commission. Glossary of Scams and Legal Terms. Available at https://www.ftc.gov/news-events/topics/glossary-scams-legal-terms. Accessed on the 12/1/2026.

[5] Cameroon. (2010). Law No. 2010/012 of 21 December 2010 relating to cybersecurity and Cybercriminality. Government of Cameroon.

[6] United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. UNODC.

[7] See Section 318 of Law No. 2016/007 of July 12, 2016, relating to the Penal Code, Cameroon.

a modern cyber-enabled phenomenon.[1]

3. Nature of Scamming in Cameroon

The nature of scamming in Cameroon is multifaceted, reflecting both technological developments and socio-economic conditions. Scamming occurs in both offline and online forms, though recent trends show a significant rise in cyber-enabled scams. Common manifestations include mobile money fraud, online investment scams, phishing emails, impersonation of public officials or institutions, fake job offers, and fraudulent online sales. These schemes often exploit weaknesses in digital literacy, high unemployment, and increasing reliance on electronic financial services.[2]

Legally, scamming in Cameroon is characterized by its intentional and deceptive nature, the presence of a victim who suffers economic loss, and the use of false representations as the principal means of execution. Under Law No. 2010/012, scamming frequently falls within the category of computer-related fraud, where information systems are used either as tools or targets of the offense. Articles dealing with unauthorized access, data manipulation, and fraudulent electronic payment systems illustrate how the law conceptualizes the nature of scamming as a technologically facilitated crime with serious economic consequences.[3]

From an enforcement perspective, the nature of scamming in Cameroon — particularly in urban and semi-urban areas such as Buea — is increasingly transnational and sophisticated. Many scams involve cross-border elements, anonymous digital platforms, and rapid movement of illicit funds, making detection and prosecution complex. This evolving nature has prompted Cameroonian authorities, including the National Agency for Information and Communication Technologies (ANTIC), to treat scamming not merely as isolated fraud but as part of a broader cybercrime ecosystem requiring technical expertise and coordinated institutional responses.[4]

Scamming in Cameroon is legally understood as a form of fraud grounded in both traditional criminal law and modern cybercrime regulation. Its nature is dynamic, technology-driven, and economically harmful, posing significant challenges to legal enforcement and victim protection. This dual character underscores the need for adaptive legal frameworks and effective implementation mechanisms, particularly at the local level in areas such as Buea.

4. Legal Framework Governing Scamming in Cameroon

The fight against scamming in Cameroon is anchored primarily in the country's cybercrime and cybersecurity legal regime, which criminalizes technological abuses such as electronic fraud, unauthorized access, and misuse of information systems. Although there is no standalone "anti-scamming law," the existing framework provides substantive and procedural tools for the detection, prosecution, and punishment of scam-related offences, particularly those conducted through electronic means.

4.1 Core Legislation: Law No. 2010/012 on Cybersecurity and Cybercrime

The cornerstone of Cameroon's legal architecture regulating digital offences — including scamming — is Law No. 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality. This statute establishes offences tied to the use of information and communication technologies and sets out sanctions for illegal acts against electronic systems and data. It has been described as the principal legislative instrument in the country's response to cyber-enabled wrongdoing.[5] The law governs the *security framework* of electronic communication networks and information systems. It defines and punishes cyber-related offences, including those that facilitate financial gain through fraudulent digital methods. It also provides for the protection of digital evidence and establishes the legal foundation for cooperation in cybercrime investigations.[6]

Article 65 criminalizes unauthorized access to electronic systems and interception of data without permission,

---

[1] *Ibid.*

[2] United Nations Office on Drugs and Crime. (n.d.). *Cybercrime and computer-related fraud*. UNODC.

[3] See the 2010 law on cyber security in Cameroon.

[4] National Agency for Information and Communication Technologies. (n.d.). *Cybersecurity and cybercrime in Cameroon*. ANTIC.

[5] Cameroon Government Certification Authority. (n.d.). Laws and regulations: Law No 2010/012 of 21 December 2010 relating to cybersecurity and the Cybercriminality in Cameroon; Law No 2010/021 of 21 December 2010 on electronic commerce in Cameroon. Available at https://www.camgovca.cm/en/regulation-policy/laws-and-regulations.html (camgovca.cm). Accessed on 13/12/2025.

[6] *Ibid.*

carrying penalties of imprisonment of 5–10 years and fines ranging from CFA 5 million to CFA 10 million.[1] Article 73 specifically addresses offences involving the falsification and use of counterfeit payment or credit cards through information systems — behaviours often linked to online scamming schemes — with prison terms of 2–10 years and fines from CFA 25 million to CFA 50 million.[2] Other provisions, such as those in Articles 66–72, prohibit interference with networks and the use of misleading software to execute unauthorized operations, a common technique in scam operations. Beyond specific offence provisions, the general sections of the law articulate its goal of building trust in electronic communication and protecting the integrity of information systems, which are essential for safe online transactions.[3]

4.2 Supporting Legal Instruments

While Law No. 2010/012 constitutes the core, other laws also contribute indirectly to regulating scam-related activity. For instance, Law No. 2010/021 on Electronic Commerce. This statute governs electronic transactions and commercial activities online, setting standards for legitimate ecommerce conduct, which helps differentiate lawful digital commerce from fraudulent schemes.[4] The Criminal Procedure Code (Law No. 2005/007) also provides procedural rules for investigation and prosecution, including provisions on evidence and extradition, which are crucial when scam cases cross borders or involve digital evidence. There is also Constitutional Guarantees as the Constitution, amended by Law No. 96-06, ensures privacy of communications, [5]underlining the legal basis for protecting individuals against unauthorized interception, a common tool in scamming offences.[6]

4.3 Institutional and Enforcement Framework

Implementing the legal framework requires robust institutions. In Cameroon, the *Agence Nationale des Technologies de l'Information* et de la Communication (ANTIC) plays a central role in coordinating cybersecurity efforts, including training judicial actors and law enforcement to detect and prosecute cyber offences effectively.[7]

At the local level, including in Buea, law enforcement and judicial authorities are increasingly required to apply these statutes to scam cases that often involve electronic transactions or social engineering tactics. The establishment of specialized cybercrime units within police forces and capacity-building initiatives aim to improve the handling of such offences, though challenges remain in resources and technical expertise.[8]

4.4 International Dimension

Cameroon has taken steps to engage with international frameworks, notably through accession processes related to the Budapest Convention on Cybercrime, which, once fully implemented, can strengthen cross-border

[1] United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Article 65 [Legislation database]. Available at https://www.unodc.org/cld/fr/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/article_65/article_65.html (UNODC. Accessed on 13/12/2025.

[2] United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Articles 66–72 [Legislation database]. Available at https://www.unodc.org/cld/en/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/articles_66-72/articles_66-72.html (UNODC). Accessed on 14/12/2026. United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Articles 84, 85 [Legislation database]. http://www.antic.cm/images/stories/data/IMG/pdf/cybersecurite/Loi_2010-012_cybersecurite_cybercriminalite.pdf (UNODC)

[3] Opt. cit. footnote 1.

[4] *Ibid.*

[5] Commission Nationale de la Communication (CNC). (n.d.). Loi n°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun [Electronic commerce law]. Available at https://cnc.gov.cm/lois/ (cnc.gov.cm). Accessed on 14/12/2025.

[6] See Law No 2005/007 of 27 July 2005 on the criminal procedure code. Available at http://minjustice.gov.cm/index.php/en/instruments-and-laws/laws/290-law-no-2005-007-of-27-july-2005-on-the-criminal-procedure-code. Accessed on 13/12/2026.

[7] National Agency for Information and Communication Technologies (ANTIC). (n.d.). Antic official website. Available at https://www.antic.cm/ (antic.cm). Accessed on 16/12/2025.

[8] National Agency for Information and Communication Technologies (ANTIC). (n.d.). La cybercriminalité – ANTIC [Cybersecurity regulation and activities]. Available at https://www.antic.cm/index.php/fr/cybersecurite/cybercriminalite/283-la-cybercriminalite.html (antic.cm). Accessed on 17/12/2025.

cooperation in tackling scam operations that inherently transcend national boundaries.[1] Cameroon's legal framework for regulating scamming is principally framed by its cybercrime and cybersecurity law, which defines and penalizes behaviours commonly associated with scams, especially when conducted through electronic means. Complemented by e-commerce rules, procedural codes, and institutional enforcement via ANTIC and judicial training, the framework provides statutory backing for prosecuting scam offences. However, practical enforcement, particularly in localities such as Buea, still faces implementation challenges that require continuous legislative refinement and capacity strengthening.

5. Effectiveness of the Measures to Fight Against Scamming in Cameroon

In Cameroon, scamming often classified as cybercrime, fraud, or advance-fee fraud poses a significant threat to societal stability and economic integrity. The regulation and combat of scamming are systematically addressed through a structured legal framework and proactive law enforcement mechanisms.

5.1 Practical Approach of the Fight Against Scamming in Cameroon

A. By the National Agency for Information and Communication Technologies

The National Agency for Information and Communication Technologies (ANTIC) is pivotal in regulating and combating scamming activities in Cameroon. ANTIC employs a multifaceted strategy that includes monitoring, public awareness, capacity building, and international collaboration[2].

1) Monitoring and Investigations

Since 2018, ANTIC has successfully identified over 6,650 fake social media accounts, primarily impersonating state dignitaries. Collaborating with platforms like Facebook, they have deactivated approximately 4,625 fraudulent accounts. Additionally, ANTIC has conducted over 8,500 investigations, unearthing the identities and locations of numerous cybercriminals. Since 2019, the agency has received more than 7,000 complaints related to scamming, demonstrating its proactive approach to addressing public concerns[3].

2) Capacity Building

ANTIC organizes training seminars and workshops to enhance the capabilities of public officials, law enforcement, and judicial authorities in understanding and combating cybercrime. These initiatives are crucial for equipping personnel with the necessary skills to tackle complex cyber issues effectively[4].

3) Public Awareness and Education

ANTIC has implemented various public awareness campaigns, including radio programs aimed at less tech-savvy communities, to educate citizens about cybersecurity risks. They have also targeted youth in secondary schools and universities, fostering vigilance and awareness of cybercrime[5].

4) Collaboration with International Bodies

ANTIC partners with international organizations, such as INTERPOL, to combat transnational cybercrime. A significant initiative, Operation Serengeti, conducted in late 2024, resulted in the arrest of over 1,000 suspects across 19 African countries, including Cameroon, highlighting the importance of international cooperation in addressing cyber threats[6].

5.2 Achievements in Combating Cybercrime in Cameroon

Cameroon has made significant strides in combating scamming, largely due to the concerted efforts of the judiciary, law enforcement agencies, and the National Agency for Information and Communication Technologies (ANTIC). These stakeholders have implemented various strategies that have led to notable successes in addressing the growing threat of cybercrime[7].

---

[1] United Nations, Cameroon. Cameroon and UNHCR: Building Durable Solutions Through Partnership, Solidarity and Innovation. Available at https://cameroon.un.org/en/308319-cameroon-and-unhcr-building-durable-solutions-through-partnership-solidarity-and-innovation. Accessed on 17/12/2026.

[2] National Agency for Information & Communication Technologies (ANTIC) - Cameroon.

[3] Cybersecurity: ANTIC claims it deleted 3,372 fake Facebook accounts out of 4,242 identified in 2020.

[4] ANTIC equips Constitutional Council staff with cybersecurity skills.

[5] ITU (International Telecommunication Union). (2020). Cybersecurity Index.

[6] INTERPOL. (2024). Operation Serengeti: A Global Effort to Combat Cybercrime.

[7] ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2022). Annual Report on Cybersecurity in Cameroon.

The Cameroonian judiciary has proactively addressed the increasing prevalence of cybercrime through the establishment of specialized courts. For example, the Yaoundé Court of First Instance was designated as a specialized cybercrime court in 2020[1]. This court focuses on handling cases related to fraud and scamming, resulting in a more efficient legal process. The establishment of such courts has increased the number of cases processed and raised the conviction rate for scammers. In one notable instance, a group of scammers who defrauded victims through fake investment schemes was sentenced to lengthy prison terms, illustrating the judiciary's commitment to punishing cybercriminals effectively[2].

Additionally, the judiciary has strengthened the legal framework surrounding cybercrime. The enactment of Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime has provided law enforcement with the necessary tools to prosecute offenders effectively[3]. This legislation has been pivotal in prosecuting cases of identity theft and online fraud. For example, in 2021, three individuals were convicted for creating fake identities to scam international victims, showcasing the judiciary's ability to adapt to the evolving nature of cybercrime[4].

Moreover, the judiciary has initiated public awareness campaigns within court settings, educating victims about their rights and legal recourse. This initiative aims to empower victims to come forward and report scams, thereby increasing the overall reporting rate of cybercrimes[5].

Also, the police force in Cameroon has significantly improved its response to cybercrime through specialized training and the establishment of dedicated cybercrime units. The Cybercrime and Digital Evidence Unit, created to focus specifically on online scams, has been instrumental in addressing the issue[6]. In 2022, this unit successfully dismantled a fraudulent network that was scamming individuals through fake online job offers, resulting in the arrest of ten suspects. This operation highlighted the police's enhanced capacity to investigate and respond to cybercrime effectively[7].

Additionally, the police have improved their forensic capabilities through partnerships with technology firms, allowing for better collection and analysis of digital evidence. For example, the introduction of advanced software tools for analyzing online communications has helped police trace scam operations back to their sources more effectively[8].

The Cameroonian police have also engaged in international collaborations to enhance their investigative capabilities. In partnership with INTERPOL, the police participated in Operation FALCON, which targeted online fraudsters across several African countries[9]. This operation led to the arrest of multiple scammers who were operating from Cameroon and defrauding victims globally. The success of such international collaborations underscores the importance of cooperation in tackling cybercrime, as many scams operate beyond national borders[10].

Furthermore, the National Agency for Information and Communication Technologies (ANTIC) has emerged as a key player in the fight against scamming by focusing on public awareness and education[11]. In 2021, ANTIC launched a nationwide campaign titled "Stay Safe Online," which included workshops, social media outreach, and informational materials distributed in schools and community centers[12]. This campaign successfully reached over 500,000 citizens, educating them about common scam tactics, such as phishing and lottery scams. The impact of this campaign is evident in the increased public awareness and vigilance regarding online fraud[13].

Furthermore, ANTIC has developed technological tools to monitor online activities for suspicious behavior. In

[1] Ministry of Justice, Cameroon. (2020). Press Release: Establishment of Specialized Cybercrime Court in Yaoundé.

[2] Yaoundé Court of First Instance. (2022). Annual Report on Cybercrime Cases.

[3] Judiciary of Cameroon. (2022). Combating Cybercrime through Specialized Courts.

[4] Cameroon Tribune. (2022). Cybercrime: Cameroonian Judiciary Cracks Down on Scammers.

[5] African Journal of Information and Communication. (2022). Cybercrime and the Role of Specialized Courts in Cameroon.

[6] Cameroonian Police Force. (2022). Annual Report on Cybercrime Investigations.

[7] INTERPOL. (2022). Operation FALCON: Global Effort to Combat Online Fraud.

[8] Ministry of Defense, Cameroon. (2022). Enhancing Cybercrime Response through International Cooperation.

[9] Police Chief, Cameroon. (2022). Combating Cybercrime: Challenges and Opportunities.

[10] African Police Journal. (2022). Special Issue on Cybercrime and Law Enforcement in Africa.

[11] ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2021). Stay Safe Online Campaign Report.

[12] ANTIC. (2022). Annual Report on Cybersecurity Awareness and Education.

[13] Ministry of Posts and Telecommunications, Cameroon. (2022). Combating Cybercrime through Public Awareness.

2022, the agency introduced a reporting hotline that received over 1,200 reports of scams within the first six months of its operation. This proactive measure allowed law enforcement to investigate several high-profile cases quickly[1]. For instance, a report led to the arrest of a group involved in a sophisticated online romance scam that defrauded victims of substantial amounts of money. The establishment of such reporting mechanisms has proven essential in facilitating timely responses to cyber threats.

Additionally, ANTIC has partnered with local universities to develop educational programs focused on digital literacy, aimed at teaching students how to navigate online spaces safely. These programs have equipped young people with the skills to recognize potential scams, further reducing the likelihood of victimization[2].

5.3 Failures in the Fight Against Scamming in Cameroon

Despite the notable successes in combating scamming in Cameroon, significant challenges and failures persist that hinder the overall effectiveness of these efforts. These failures stem from various factors, including resource limitations, a lack of public awareness, insufficient legal frameworks, and the evolving nature of cybercrime[3].

One of the primary challenges facing the fight against scamming in Cameroon is the inadequate allocation of resources to law enforcement and judicial bodies. Many police departments lack the necessary funding and technology to effectively combat cybercrime[4]. This limitation hampers their ability to conduct thorough investigations, gather digital evidence, and implement advanced forensic techniques. For example, several police units still rely on outdated equipment and software, which significantly slows down the process of identifying and prosecuting scammers. Consequently, this resource scarcity can lead to low conviction rates and a perception of impunity among cybercriminals[5].

Moreover, the judiciary faces similar resource constraints. Specialized cybercrime courts often operate with limited personnel and financial support, resulting in prolonged trial durations and backlogged cases. This inefficiency can deter victims from coming forward, as they may perceive the legal process as lengthy and ineffective[6]. The lack of training for judicial staff in handling complex cybercrime cases further exacerbates the situation, leading to inadequate legal responses and potentially unjust outcomes for victims seeking justice[7].

Another significant failure in the fight against scamming is the insufficient level of public awareness regarding the risks associated with online fraud. While campaigns have been launched to educate citizens, many individuals remain unaware of the latest scam tactics and how to protect themselves. A study conducted in 2022 revealed that a significant portion of the population still falls victim to common scams, such as phishing and advance-fee fraud, due to a lack of understanding of these threats[8].

Moreover, outreach efforts often target urban populations, leaving rural communities vulnerable to scams. This disparity in awareness can be attributed to limited access to information and resources in remote areas, where internet connectivity is often poor[9]. As a result, individuals in these communities may be more susceptible to scams, as they lack the knowledge and tools to recognize fraudulent activities. The failure to reach all demographics effectively undermines the overall impact of awareness campaigns[10].

The existing legal framework for addressing cybercrime in Cameroon, while improved, still has notable gaps that hinder effective prosecution. Laws can be vague or outdated, making it difficult for law enforcement to apply them to specific cases of scamming[11]. For example, the legal definitions of cyber offenses may not encompass newer forms of scams, such as those involving cryptocurrencies or sophisticated social engineering tactics. This lack of clarity can lead to challenges in prosecuting offenders, as lawyers may exploit these legal

[1] Cameroon Tribune. (2022). ANTIC's Efforts to Educate Citizens on Online Safety.

[2] Journal of Information Technology Education in Africa. (2022). Digital Literacy Programs in Cameroon: A Study on ANTIC's Initiatives.

[3] World Bank. (2022). Cybercrime in Africa: Challenges and Opportunities for Economic Development.

[4] World Bank. (2022). Digital Economy for Africa: Diagnostic Report on Cameroon.

[5] ITU (International Telecommunication Union). (2022). Global Cybersecurity Index: Challenges and Best Practices for Law Enforcement.

[6] Transparency International. (2022). Corruption Perceptions Index: Impact on Cybersecurity in Cameroon.

[7] UNODC (United Nations Office on Drugs and Crime). (2022). Strengthening Capacities of Law Enforcement Agencies to Combat Cybercrime in Central Africa.

[8] ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2022). Study on Public Awareness of Cybercrime in Cameroon.

[9] African Journal of Criminology and Justice Studies. (2022). Special Issue on Cybercrime and Justice Systems in Africa.

[10] ITU (International Telecommunication Union). (2022). Measuring Digital Literacy in Africa: Challenges and Opportunities.

[11] UNODC (United Nations Office on Drugs and Crime). (2022). Assessment of Cybercrime Legislation in Central Africa.

ambiguities to defend their clients[1].

Furthermore, the enforcement of existing laws is often inconsistent. Corruption within law enforcement agencies can impede investigations and lead to a lack of accountability for offenders[2]. Reports of bribery and collusion between scammers and officials have surfaced, undermining public trust in the system and discouraging victims from reporting incidents. This cycle of corruption and inefficiency not only hampers justice but also emboldens scammers to continue their activities with minimal fear of repercussions[3].

In addition, the rapidly evolving nature of cybercrime presents another significant challenge in the fight against scamming in Cameroon. Scammers are increasingly employing sophisticated techniques and technologies to circumvent detection and exploit vulnerabilities[4]. For instance, the rise of social media and digital communication platforms has provided scammers with new avenues to target unsuspecting victims. Techniques such as identity theft, deep fake technology, and phishing attacks have become more prevalent, making it difficult for law enforcement to keep pace with emerging threats[5].

Additionally, the global nature of cybercrime complicates efforts to combat scamming. Scammers often operate from different jurisdictions, making it challenging for Cameroonian authorities to apprehend offenders who may be located abroad[6]. The lack of international cooperation and legal frameworks to facilitate cross-border investigations further exacerbates this issue. As a result, many scammers remain at large, exploiting the weaknesses in both local and international systems.[7]

6. Conclusion

This study set out to assess the effectiveness of the legal measures put in place to combat scamming in Cameroon, using Buea as a case study. The analysis demonstrates that Cameroon has established a relatively comprehensive legal framework capable of addressing scamming, particularly through Law No. 2010/012 on cybersecurity and Cybercriminality, complemented by legislation on electronic commerce and relevant provisions of the Criminal Procedure Code. These laws provide a clear basis for the criminalization of scam-related activities, especially those carried out through information and communication technologies, and prescribe deterrent sanctions for offenders.

However, the findings of this study reveal that the existence of legal provisions alone does not automatically translate into effective protection against scamming in practice. In Buea, as in many other parts of Cameroon, the enforcement of anti-scamming laws is hindered by several challenges, including limited technical capacity among law enforcement officers, inadequate investigative resources, procedural delays, and difficulties in gathering and preserving digital evidence. Additionally, low levels of public awareness about scamming offenses and the applicable legal remedies further weaken the deterrent effect of the law, as many victims either fail to report incidents or lack confidence in the justice system.

The study also highlights the institutional role of agencies such as the National Agency for Information and Communication Technologies (ANTIC), which has made notable efforts in capacity building and awareness creation. Nonetheless, coordination between regulatory bodies, law enforcement agencies, and the judiciary remains insufficient, particularly at the local level in Buea. This gap reduces the overall effectiveness of the legal framework and allows scamming activities to persist, often in increasingly sophisticated forms.

In conclusion, while Cameroon's legal framework provides an adequate normative foundation for combating scamming, its effectiveness in Buea is constrained by enforcement and implementation challenges. Addressing these shortcomings requires not only legal reforms where necessary, but also sustained investment in institutional capacity, specialized training in cybercrime investigation, improved inter-agency cooperation, and enhanced public sensitization. Strengthening these areas will be crucial to ensuring that the law serves as a meaningful tool in the fight against scamming and contributes to greater public trust and digital security in Buea and Cameroon at large.

7. Recommendations

[1] Transparency International. (2022). Corruption Perceptions Index: Impact on Justice Systems in Africa.

[2] African Journal of Criminology and Justice Studies. (2022). Special Issue on Cybercrime Laws and Enforcement in Africa.

[3] World Justice Project. (2022). Rule of Law Index: Cameroon Country Report.

[4] Europol. (2022). Internet Organized Crime Threat Assessment (IOCTA).

[5] INTERPOL. (2022). Global Threat Assessment: Cybercrime Trends and Challenges.

[6] World Economic Forum. (2022). Global Risks Report: Cybersecurity and the Future of Work.

[7] Journal of Cybercrime Research. (2022). Emerging Trends in Cybercrime: A Global Perspective.

Based on the findings of the study on the legal appraisal of the enforcement of regulations against scamming in Cameroon, particularly in Buea, the following recommendations are proposed to enhance the effectiveness of the fight against cybercrime:

7.1 Increase Funding and Resources for Law Enforcement

To effectively combat scamming, it is essential to allocate increased funding and resources to law enforcement agencies. This funding should focus on acquiring advanced technological tools for digital forensics, training programs for officers, and improving overall operational capabilities. Enhanced resources would enable law enforcement to conduct thorough investigations, gather digital evidence, and respond more swiftly to reports of scams.

7.2 Strengthen Legal Frameworks

Efforts should be made to revise and strengthen the existing legal framework governing cybercrime. This includes updating laws to encompass new forms of scams, such as those involving cryptocurrencies and complex social engineering tactics. Clear definitions and guidelines will empower law enforcement to prosecute offenders more effectively and reduce ambiguity in legal interpretations.

7.3 Enhance Training for Judicial Personnel

Training programs for judges, lawyers, and legal practitioners should be implemented to improve their understanding of cybercrime laws and digital evidence. This will ensure that legal professionals are equipped to handle the complexities of cybercrime cases, leading to fairer and more informed rulings. Continuous professional development opportunities should be made available to keep legal personnel updated on emerging trends in cybercrime.

7.4 Expand Public Awareness Campaigns

Public awareness initiatives should be expanded to reach a broader audience, particularly in rural and underserved communities. Campaigns should focus on educating citizens about the various types of scams, how to recognize them, and the importance of reporting suspicious activities. Partnerships with local organizations, schools, and community groups can enhance outreach efforts and ensure that information is accessible to all demographics.

7.5 Establish Reporting Mechanisms

The establishment of user-friendly reporting mechanisms, such as hotlines and online platforms, should be prioritized. These mechanisms should be widely publicized to ensure that citizens know how to report scams easily and anonymously. Quick response teams should be formed to handle reports effectively and investigate incidents promptly.

References

African Journal of Criminology and Justice Studies. (2022). Special Issue on Cybercrime and Justice Systems in Africa.

African Journal of Criminology and Justice Studies. (2022). Special Issue on Cybercrime Laws and Enforcement in Africa.

African Journal of Information and Communication. (2022). Cybercrime and the Role of Specialized Courts in Cameroon.

African Police Journal. (2022). Special Issue on Cybercrime and Law Enforcement in Africa.

ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2022). Annual Report on Cybersecurity in Cameroon.

ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2021). Stay Safe Online Campaign Report.

ANTIC (Agence Nationale des Technologies de l'Information et de la Communication). (2022). Study on Public Awareness of Cybercrime in Cameroon.

ANTIC. (2022). Annual Report on Cybersecurity Awareness and Education.

Cameroon Government Certification Authority. (n.d.). Laws and regulations: Law No 2010/012 of 21 December 2010 relating to cybersecurity and the Cybercriminality in Cameroon; Law No 2010/021 of 21 December 2010 on electronic commerce in Cameroon. Available at https://www.camgovca.cm/en/regulation-policy/laws-and-regulations.html (camgovca.cm). Accessed on 13/12/2025.

Cameroon Tribune. (2022). ANTIC's Efforts to Educate Citizens on Online Safety.

Cameroon Tribune. (2022). Cybercrime: Cameroonian Judiciary Cracks Down on Scammers.

Cameroon. (2010). Law No. 2010/012 of 21 December 2010 relating to cybersecurity and Cybercriminality. Government of Cameroon.

Cameroonian Police Force. (2022). Annual Report on Cybercrime Investigations.

Commission Nationale de la Communication (CNC). (n.d.). Loi n°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun [Electronic commerce law]. Available at https://cnc.gov.cm/lois/ (cnc.gov.cm). Accessed on 14/12/2025.

Europol. (2022). Internet Organized Crime Threat Assessment (IOCTA).

INTERPOL. (2022). Global Threat Assessment: Cybercrime Trends and Challenges.

INTERPOL. (2022). Operation FALCON: Global Effort to Combat Online Fraud.

INTERPOL. (2024). Operation Serengeti: A Global Effort to Combat Cybercrime.

ITU (International Telecommunication Union). (2020). Cybersecurity Index.

ITU (International Telecommunication Union). (2022). Global Cybersecurity Index: Challenges and Best Practices for Law Enforcement.

ITU (International Telecommunication Union). (2022). Measuring Digital Literacy in Africa: Challenges and Opportunities.

Journal of Cybercrime Research. (2022). Emerging Trends in Cybercrime: A Global Perspective.

Journal of Information Technology Education in Africa. (2022). Digital Literacy Programs in Cameroon: A Study on ANTIC's Initiatives.

Judiciary of Cameroon. (2022). Combating Cybercrime through Specialized Courts.

Ministry of Defense, Cameroon. (2022). Enhancing Cybercrime Response through International Cooperation.

Ministry of Justice, Cameroon. (2020). Press Release: Establishment of Specialized Cybercrime Court in Yaoundé.

Ministry of Posts and Telecommunications, Cameroon. (2022). Combating Cybercrime through Public Awareness.

National Agency for Information and Communication Technologies (ANTIC). (n.d.). Antic official website. Available at https://www.antic.cm/ (antic.cm). Accessed on 16/12/2025.

National Agency for Information and Communication Technologies (ANTIC). (n.d.). La cybercriminalité – ANTIC [Cybersecurity regulation and activities]. Available at https://www.antic.cm/index.php/fr/cybersecurite/cybercriminalite/283-la-cybercriminalite.html (antic.cm). Accessed on 17/12/2025.

National Agency for Information and Communication Technologies. (n.d.). *Cybersecurity and cybercrime in Cameroon*. ANTIC.

Police Chief, Cameroon. (2022). Combating Cybercrime: Challenges and Opportunities.

StopBlablaCam. (2025, December 17). Cameroon loses over CFA 1 billion to cybercrime in 2025. Available at https://www.stopblablacam.com/society/1712-15499-cameroon-loses-over-cfa1-billion-to-cybercrime-in-2025. Accessed on 12/12/2025.

Transparency International. (2022). Corruption Perceptions Index: Impact on Cybersecurity in Cameroon.

Transparency International. (2022). Corruption Perceptions Index: Impact on Justice Systems in Africa.

United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Article 65 [Legislation database]. Available at https://www.unodc.org/cld/fr/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/article_65/article_65.html (UNODC. Accessed on 13/12/2025.

United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Articles 66–72 [Legislation database]. Available at https://www.unodc.org/cld/en/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/articles_66-72/articles_66-72.html (UNODC). Accessed on 14/12/2026. United Nations Office on Drugs and Crime (UNODC). (n.d.). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Articles 84, 85 [Legislation database]. http://www.antic.cm/images/stories/data/IMG/pdf/cybersecurite/Loi_2010-012_cybersecurite_cybercriminalite.pdf (UNODC)

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. UNODC.

United Nations Office on Drugs and Crime. (n.d.). *Cybercrime and computer-related fraud*. UNODC.

United Nations, Cameroon. Cameroon and UNHCR: Building Durable Solutions Through Partnership, Solidarity and Innovation. Available at https://cameroon.un.org/en/308319-cameroon-and-unhcr-building-durable-solutions-through-partnership-solidarity-and-innovation. Accessed on 17/12/2026.

UNODC (United Nations Office on Drugs and Crime). (2022). Assessment of Cybercrime Legislation in Central Africa.

UNODC (United Nations Office on Drugs and Crime). (2022). Strengthening Capacities of Law Enforcement Agencies to Combat Cybercrime in Central Africa.

UNODC. (2010). Loi No. 2010-012 sur la cybersécurité et la cybercriminalité: Article 73 [Law on cybersecurity and cybercrime]. United Nations Office on Drugs and Crime. Available at https://www.unodc.org/cld/fr/legislation/cmr/loi_no._2010-012_sur_la_cybersecurite_et_la_cybercriminalite/titre_iii/article_73/article_73.html. Accessed on 12/12/2025.

World Bank. (2022). Cybercrime in Africa: Challenges and Opportunities for Economic Development.

World Bank. (2022). Digital Economy for Africa: Diagnostic Report on Cameroon.

World Economic Forum. (2022). Global Risks Report: Cybersecurity and the Future of Work.

World Justice Project. (2022). Rule of Law Index: Cameroon Country Report.

Yaoundé Court of First Instance. (2022). Annual Report on Cybercrime Cases.