Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences

Anoumbuandem Benvolio Lekunze
University of Buea, Buea, Cameroon

Keywords

Cameroon,
cybercrime,
digital technologies,
e-commerce,
fraud,
justice,
law,
scamming,
security,
transactions

Abstract

Objective: to examine the impact of cybercrimes on e-commerce related transactions in Cameroon and evaluate the effectiveness of the legal provisions in force that counteract cyberthreats.

Methods: The research is based on the utilitarian, transaction cost and the rational choice theories. It adopts the qualitative research methodology with the use of the doctrinal method. The author conducted a comprehensive analysis of Cameroon's legal acts in the field of cybersecurity and e-commerce. A survey was carried out between January to April 2025 at Molyko in Buea where 250 sample responses were obtained. Judicial precedents and statistics of the Cameroon Ministry of Posts and Telecommunications were investigated.

Results: It was found that cybercrimes have caused loss of trust and confidence in e-commerce transactions within Cameroon and a declining rate at which people are willing to carry out e-commerce transactions in Cameroon. More than 60% of young persons between the ages of 16 to 35 years in some major Cameroonian cities are either involved in e-commerce related cybercrimes or suffered from them. It was also observed that there is an increase in the rate at which female persons are involved in e-commerce related cybercrimes. The main types of cybercrimes were identified: scamming, phishing, and bank card skimming.

Scientific novelty: it consists in a comprehensive interdisciplinary analysis of the impact of cybercrime on e-commerce in the context of the developing African economy. For the first time, an empirical study of the scale of cybercrime in a specific region of Cameroon was conducted, including

a quantitative assessment of youth involvement in illegal activities. The author has developed a theoretical model that combines the utilitarianism, transaction costs, and rational choice concepts to explain the motivation of cybercriminals. Specific socio-legal factors contributing to the growth of cybercrime in the context of the socio-political crisis were identified.

Practical significance: The study results are of great practical significance for improving the legal, technological, social and economic mechanisms for countering cybercrime in Cameroon. The proposed recommendations include reforming procedural legislation, expanding the powers of specialized agencies, introducing a system of home addresses and social security numbers, raising the minimum wage, and integrating courses on cybersecurity into educational programs. The data obtained can be used by government agencies, the judicial system, educational institutions and international organizations to develop effective strategies to combat cybercrime and develop a secure digital economy.

For citation

Lekunze, A. B. (2025). Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences. *Journal of Digital Technologies and Law, 3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

Contents

Introduction

Crimes are frequent occurrences in every human society, old as the creation of humans, and operate as a core concept in modern society (Chris et al., 2005). The introduction of the internet to the public on January 1, 1983[1] has facilitated the commission of some crimes through online communication portals that were not initially foreseen by the legislator. The first recorded history of cybercrime was in 1834 when the French telegraph system was hacked, and access gained to financial markets through stolen data[2]. The act of committing cybercrime involves different elements, tools and processes as opposed to conventional crimes that may not raise many issues of jurisdiction and proof. This is because cyberspace is vast and unlimited to a geographical region or country (Yokotani & Takano, 2022; 2021).

Cybercrime can be defined as a wide range of criminal activities that are carried out using digital devices and networks (Alhadidi et al., 2024; Arroyabe et al., 2024; Edwards & Hollely, 2023; Gupta et al., 2025; Higgs & Flowerday, 2025a)[3]. It is also a collection of criminal activities that include offences against computers and computer systems (Payne, 2020). A computer can be the object of commission or a target. Cybercrime can also be any criminal activity that uses a computer as either an instrumentality, or a means for perpetuating further crimes. It can take the form of cyber theft or other related illegal activities targeted on humans and property (Garner, 1999). This article focuses on the impact of cybercrimes in electronic commerce (e-commerce) transactions in Cameroon because available literature on the impact of cybercrimes n oe-commerce in Cameroon is limited. Examples of cybercrimes include but not limited to, hacking, cyber stalking, defamation, email bombing, data diddling, salami attacks, denial of service attack, virus and worm attacks, internet time thefts etc. E-commerce transactions as the name signify operates in cyberspace by peer-to-peer electronic data interchange (EDI) (Garner, 1999) and not always void of crimes.

---

1 January 1, 1983 is considered the official birthday of the Internet. Prior to this, the various computer networks did not have a standard way to communicate with each other. A new communications protocol was established called Transfer Control Protocol/Internetwork Protocol (TCP/IP). This allowed different kinds of computers on different networks to «talk» to each other. ARPANET and the Defense Data Network officially changed to the TCP/IP standard on January 1, 1983, hence the birth of the Internet. https://clck.ru/3QEh9u

2 Blue Voyant. https://clck.ru/3QEh97

3 Cybercrimes it should be noted are common in the domain of commercial transactions than others.

E-commerce can take the forms of engaging in online shopping, mobile apps conversational commerce via live chat, chatbots, and voice assistants[4]. It can be through Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C) and Customer to Business (C2B). It is also defined as the practice of buying and selling goods and services through online consumer services on the internet. It is one of the ways in which companies and individuals carry out business in order to maximize profits within a short time frame while reducing fixed cost over a broad range of assets and transport costs from central business districts[5].

There are several advantages associated to e-commerce, but despite these advantages, cybercrimes have hampered the smooth functioning of e-commerce and have led to loss of profits, trust and confidence amongst business counterparts. There are efforts in Cameroon to combat cybercrimes through legislation and technology but this has not so far seen a significant impact in commercial transactions because of lack of new technologies, weak digital rights management system[6], ease to circumvent technology, convenience, and speed at which cybercrimes are committed. This is more so because of the benefits and satisfaction that perpetrators acquire by committing cybercrimes in e-commerce transactions the very technologies meant for protection.

Cybercrimes and related offences in commercial transactions have in the past years experienced a rise in Cameroon due to an increase in the proliferation of the internet, low cost of procuring electronic devices, global economic crisis, lockdowns due to the COVID-19 pandemic coupled with the introduction of numerous social media platforms. Cybercrimes became popular in Cameroon around 2005 before the enactment of the 2010 laws on cyber criminality and electronic commerce. This can be demonstrated by the earlier cases of; The People v. Obi Roland[7], The People v. Nfang Macknight[8], The People v. Mbah Valery[9], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[10],

4 VentureBeat. (2025, March 15). How to prepare your products and brand for conversational commerce. https://clck.ru/3QEhWE

5 This can be explained by the Von Thunen Theory of agriculture that was developed by Johann Heinrich in 1826. This model predicts human behaviour in terms of landscape and economy based on meticulous mathematical calculations and observations. It explains transport cost from the geographical location of farms to a central business district (CBD). Although it is a theory in agriculture, it relates to e-ecommerce today because the principal objective of e-commerce is to minimize transaction costs from where goods and service originate to where a consumer is located.

6 It refers to technical ways of securing data with the use of passwords, cryptography and steganography.

7 CFIB/55C/2008(Unreported).

8 CFIB/76C/2009(Unreported).

9 CFIB/255/2010(Unreported).

10 (2014) 2 SLR.

The people of Cameroon & another v. Tita Njina Kevin Ndango[11]. All these cases preceded the 2010 Laws on cyber criminality and electronic commerce in Cameroon although some of these cases were reported later. It can be observed in these cases that the civil parties were hardly present in court reason why it shall later be observed in this article that this aspect has caused a surge of cybercrimes in Cameroon.

The first legislations on cybercrimes and e-commerce in Cameroon were enacted in December 2010 following frequent occurrences of cyber criminality cases in Cameroon that related mostly to commercial transactions with the use of online platforms through false pretenses[12] in the guise of legitimate business transactions[13]. That is why the cyber criminality law and the electronic commerce laws in Cameroon were enacted in the same year.

This article therefore treats the impact of cybercrime together with e-commerce transactions in Cameroon for this reason. The cyber criminality law in Cameroon provides the legal framework for investigating and prosecuting cybercrimes alongside the Cameroonian Penal Code and the Criminal Procedure Code (CPC). It elaborates on the types of cybercrimes including unlawful interception, hacking, computer related fraud, offences relating to child pornography etc. The law is not only adjectival but also procedural because it provides rules for investigating and prosecuting cybercrimes with international co-operation.

The 2010 law on electronic commerce in Cameroon on the other hand laid the foundation of e-commerce in Cameroon[14]. This was due to the rapid emergence of e-commerce platforms that followed world trends. The law equally provides substantive elements and procedures to investigate and prosecute allegations of malpractices in e-commerce transactions.

Cybercrimes in Cameroon exist not only in e-commerce transactions but also in other criminal acts like defamation, false pretense, theft, cyberstalking and hacking. Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon criminalizes cybercrimes jointly with law N° 2016/007 of 12 July 2016 relating to the Penal Code[15]. While Law N° 2010/021 of 21 December 2010 on electronic commerce in Cameroon establishes offences and punishments for violating the provisions of e-commerce rules. The impact of cyber criminality on e-commerce is huge in Cameroon coupled with the fact that a majority of the country's citizens are not computer savvy and

11 (2010) CCLR 1-126

12 Section 318 of Law N°2016/007 of 12 August 2016 on the penal code.

13 Cybercrimes in Cameroon were officially recognized as a legal issue with the enactment of law N°2010/012 of December 2010 which defines cybercrime offences and provided penalties. Before this law, many instances of cybercriminality were addressed under the penal code.

14 Law N° 2010/021 of 21 December 2010.

15 Section 219 of the Penal Code.

cannot afford internet connections to do research on electronic commercial platforms. This has led to some legal problems like breach of confidence and trust, loss of profit margins in both the micro and macro-economic levels, increased bribery and corruption and a general increase in crime wave since the illicit proceeds acquired from such crimes are often used to perpetuate further offences.

1. Statement of the problem

The introduction of e-commerce in Cameroon and the advent of cyber criminality has had devastating consequences on digital based businesses. This has been compounded by the fact that a vast majority of the Cameroonian population live below the minimum wage level coupled with no official home addresses in the country and no social security numbers attributed to citizens. The lack of digital home addresses and social security numbers makes investigations, the execution of summonses and arrests strenuous because deliveries[16] are usually at the post offices or in other locations on call, or payments are posted to bank accounts that cannot be linked to specific addresses of account owners. Loss of confidence and trust is more nowadays in electronic based commercial transactions in Cameroon because many payments are unsecured[17]. There are huge losses in profit margins and an increase crime wave across the country because illicit profits derived from cybercrimes are sometimes used in furtherance of other crimes like drugs abuse, bribery, corruption, crimes of moral integrity, public drunkenness etc. Cybercrimes have also led to high levels of arbitrary arrests and torture especially on the youths without tangible evidence since some police and judicial officers rely on allegations of scamming due to lifestyles even without any official complaint. Most of these officers hardly prosecute cybercrime in e-commerce cases but prefer to enrich themselves by collecting bribes and freeing suspects. This is compounded by the fact that most victims hardly lodge official complains against the perpetrators. There is also a low level of attention and international co-operation to combat e-commerce related cybercrimes in Cameroon due to inadequate technical infrastructures, personal financial gains and proper follow-up. This has led to an increase in the rate of e-commerce related cybercrimes within the country with most offenders preferring to bribe out their way and turning to other victims to recover their losses[18]. There is also a general atmosphere of fear to file official complaints against cybercriminals because of shame and dire consequences since most victims are accomplices with the perpetrators to indulge

[16] Although controlled deliveries can be done at the post offices to apprehend suspects, this is hardly done in Cameroon.

[17] Return policies are highly ineffective in Cameroon and are hardly embodied in commercial contracts. So the aspect of fear creeps into customers' minds.

[18] It can observed that most cyber offenders under e-commerce hardly stop their acts even after enriching themselves. They mostly perfect their skills.

in illegal transactions form the onset. All of these problems have been escalated by lack of sufficient powers attributed to agencies like the National Financial investigation agency (NFIA) and the National Agency for information and communication technologies (NAICT) to prosecute cybercrimes in Cameroon. Their roles are limited to filing complaints, carrying out investigations and making recommendations with no proper follow-up.

2. Theoretical and Conceptual frameworks

This article is based on several theories.

2.1. The utilitarianism theory

This theory was propounded by John Stuart Mill in 1861. He believed that happiness was the only thing humans do and should desire for their own sake. He believed that because happiness is the only intrinsic good, and since more happiness is preferable to less, the goal of ethical life is to maximize happiness. Jeremy Bentham and John Stuart Mill called it 'the principle of utility' or 'the greatest-happiness principle'. In the context of this article, cybercrimes in e-commerce satisfy the cravings, wellbeing and the happiness of the perpetrators. Therefore, the drive to satisfy personal egos and happiness by offenders may make them desire the benefits of defrauding others by way of committing cybercrimes under e-commerce transactions to gain pleasure and satisfaction. This theory aligns with the Resourceful Evaluative Maximizing Model theory that views individuals as rational actors who are always seeking to maximize their own utility or wellbeing within a given set of constraints. It shows that individuals always strive to find the best possible outcome due to constraints in their resources (Wartiovaara, 2011).

2.2. Transaction cost theory

This theory was introduced by John R. Commons in 1931 (Williamson, 2008). It is cost incurred when carrying out trade. These costs are associated to those in running the economic system of a company and the total costs of carrying out a transaction. It also includes the cost of planning, deciding, changing plans, resolving disputes, and after-sales costs. According to the author, the determinants of transaction costs are frequency, specificity, uncertainty, limited rationality, and opportunistic behaviour. One of the objectives of e-commerce is to significantly reduce transaction costs by way of electronic data interchange (EDI). The Transaction Cost Theory (TCT) focuses on minimal effort on resources and the cost required parties to exchange their goods and services. The objective of this theory is to maximize transaction performance while minimizing costs which is the main objective of e-commerce. This theory can be compared

to the Von Thunen model that dwells on transaction cost like transportation of crops from farms to a central business district. The sales price is mostly determined according to the distance between the central business district and where the farm produce is sold. This theory is related to e-commerce because of the distances between where goods and services are located, where negotiations take place and where they are delivered. E-commerce in consideration to this model leads to reduced cost, irrespective of where the goods are manufacture and where they are delivered, as opposed to transactions that are concluded in a manner where the parties have to travel over long distances to carry out negotiations and carry out shopping in real world.

2.3. Rational choice theory

This theory was propounded by Adam Smith in 1776 and later articulated by the sociologist George Homans in 1961. The theory is based on behavioral psychology. The theory involves achieving a goal using the most cost-effective method without reflecting on the worthiness of that goal. The goals may be self-regarding, selfish, or materialistic (Snidal, 2013). The theory gives guidelines that help to understand economic and social behaviour and used in criminology. It helps to predict the outcome and pattern of choice and assumes that individuals are self-interested when decisions are based on optimizing preferences by balancing costs and benefits. This phenomenon is common in e-commerce where many options are available in online shopping where different choices may be made in preference to others. The goals of cybercriminals in e-commerce are usually self-centered without regards to the consequences caused to their victims after depriving them of their wealth. The theory is also related to crime where an individual can decide to commit an offence and be caught or takes risk to commit and offence and go free while benefiting. This is a typical phenomenon in e-commerce related cybercrimes where it is difficulty to catch perpetrators the act.

3. Related Literature

Some authors have written independently in the areas of cybercrime and e-commerce and have made little connection between cybercrimes and e-commerce. While few authors have highlighted the impact of cybercrime on e-commerce transactions, they have not critically examined the relation between the two, which is metaphoric. This is because the same sanctions that exists in conventional crimes under commercial transactions exist under cybercrimes in electronic commerce transactions. What happens offline is the same as what happens online with the difference being the mode and interface used in carrying out the same act with the same act.

Reyns et al. (2011) dwells on the fears caused by cybercrimes because of victimization. The author examines the relationship between risk in cyberspace for fear of being a victim

of cybercrime. His analysis is based on information collected from undergraduate students at the University of Cincinnati. The major finding in his research shows that many people are worried to become victims of cybercrimes. He further emphasizes on the category of offenders and their behavioral pattens in relation to status and gender. His work examines behavioural frequencies that have great effects on the levels of fear because of cybercrime victimization. He agrees that fear and victimization in cyberspace are based on perceived risks. His work doesn't analyze how these fears can be allayed to encourage e-commerce.

Böhme и Moore (2012) dwell on cybercrimes in online shopping and how to prevent them. Their main finding was that cybercrimes have led to the reduction in the rate of transactions like; online banking, online shopping which has caused huge negative effects. The paper concluded that people who do not know about cybercrimes are more likely to engage in e-commerce transactions like online shopping. Their work is mostly limited to online shopping meanwhile e-commerce is broader.

Y. Abubakari (2020) demonstrates how people lose many opportunities for fear of being scammed. The author shows the reasons, impacts and limitations of cybercrime policies in Anglophone West Africa. He also demonstrates how cybercrime perpetrators lose focus in education and that the reason for the growth of cybercrimes is associated with economic strains and corruption at the governmental level. The author considers hindrances in cybercrime policy because of corruption, government interference, ineffective implementation of cybercrime laws and inconsistencies in the content of cybercrime policies. His research focused on Ghana, Nigeria, and Sub-Saharan Africa as a representative sample for Anglophone West Africa because the prevalence of internet fraud in West Africa is centered around the Anglophone West African counties like; Ghana, Nigeria, Liberia, Sierra Leone, Gambia and part of Cameroon, with Nigeria and Ghana being the most notorious.

André Boraine and Ngaundje Leno Doris (2019) wrote on the fight against cybercrime in Cameroon. They focused mainly on the conflict in the Anglophone regions of Cameroon and showed a link between the conflict and the increased rate of cybercrimes due to the conflict. They examine the role of the government of Cameroon in the fight against cybercrimes and analyzed some of the legal provisions used to combat cybercrimes in Cameroon. Their paper examined why cybercrimes are prevalent in Cameroon and recommend measures that can be put in place to combat cybercrimes in Cameroon. They did not show the direct impact of cybercrimes on e-commerce transactions in Cameroon. Their paper raises awareness and contributes to knowledge in data protection rules, especially among investigating officers, students, specialists, and non-specialist legal practitioners.

Most available literature as examined above is focused on either cybercrime or e-commerce. This article shows the direct impacts that cybercrimes have on e-commerce transactions in Cameroon and makes recommendations.

4. Common types of e-commerce related cybercrimes in Cameroon

Cybercrimes in e-commerce transactions in Cameroon caused an approximate loss of 12.2. billion francs CFA in 2021 with scamming and phishing accounting for approximately half the amount[19]. There are different types of e-commerce related cybercrimes that affect Cameroon and the world. It may be observed that the nature of cyberspace communications does not limit cybercrimes to particular geographical territories. A person may be in a country and commit cybercrime across different countries with different systems of law. Therefore, there is need for international co-operation to combat cybercrimes, especially e-commerce related cybercrimes. This same reason accounts for the absence of complainants in legal proceedings and the growth of cybercrimes[20]. The types of cybercrimes associated to e-commerce include but not limited to: spamming, salami attacks, virus bombarding, cyber defamation etc. The common types in Cameroon are scamming[21], phishing[22] and bank card skimming[23]. Most of these crimes in Cameroon are oriented towards financial gains and occur in e-commerce at inter personal level.

4.1. Scamming

Scamming originates from the word scam. It is a dishonest plan to make money or getting an advantage especially by tricking people. It becomes a scheme if the plan is in a large scale. Scheming is relatively rare in Cameroon[24]. Scamming is also a confidence trick to defraud a person or group after gaining their trust by taking advantage of a combination of factors like the victim's naivety, compassion, vanity, confidence and greed (Orbach & Huang, 2018). In Cameroon, according to a 2021 report of the Ministry of Post and Telecommunications (MINPOST), the rate of scamming was 60 % in Yaounde, Douala, Buea and Noun amongst unemployed young people aged between 16 and 35 years[25].

Scamming is not a new phenomenon but has grown with the proliferation of ICT tools and the internet. In ancient Greece, cups and balls trick were used as forms of deception and in same Greece, a 'confidence man' called Thompson who was a swindler asked

---

19 2021 report of the Ministry of Post and Telecommunications. Note 30. https://clck.ru/3QMjCH

20 One of the reasons behind lack of will in Cameroon to prosecute cybercrimes is because the victims are sometimes citizens of foreign countries and lack interest to prosecute in Cameroon due to some legal challenges, cost and fear. This aspect permit bribery and corruption since the victims are not usually available in Cameroon.

21 It is false pretence with the use of electronic communication protocols.

22 To behave as a trusted person to gain access to sensitive information.

23 A method to obtain bank card information while they are used on an automatic teller machine.

24 2021 report of the Ministry of Post and Telecommunications. Note 6 p. 1346. https://clck.ru/3QMjCH

25 Ibid.

his victims to express confidence in him by giving him money rather than gaining their confidence in a more nuanced way. He was not successful and was arrested in July 1849[26]. E-commerce related cybercrimes became noticeable in Cameroon in 2005 before the enactment of the 2010 law on cybersecurity. Before then, courts relied mostly on the Penal Code[27] to adjudicate such cases as was seen in the case of The People v. Obi Roland[28]. This was a case of scamming that was heard by the Court of First Instance Buea in 2008 before the enactment of the 2010 laws on cybersecurity and electronic commerce law. Section 318 of the Cameroonian Penal Code was used as basis of the judgement. The accused was found guilty and sentenced to six years imprisonment. This was the same position held by thesame court in The People v. Nfang Macknight[29], where the accused was found guilty by the same court for similar reasons.

Even though the courts have often found the accused persons guilty, surprisingly many of such cases hardly get to Cameroonian courts. The procedure in determining cyber cases is often riddled with incompatibilities like the violation of rights under sections 3 and 8 of the CPC that have led to the discharge of some accused persons as was seen in the cases of The People v. Mbah Valery[30], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[31]. It can be observed that because of the high level of bribery and corruption in e-commerce related cybercrime cases like scamming, courts are hardly seized nowadays in Cameroon to adjudicate on such cases. The scammers and investigating officers prefer to collude to bribes for their freedom. This may be however difficult in situations where a complainant decides to follow up prosecution by filling a civil claim before a competent court. This was so in the case of The people of Cameroon & another v. Tita Njina Kevin Ndango (Jansson & von Solms, 2011) where the Court of First Instance Buea found the accused guilty of all the counts in the charge because the complainant travelled from Switzerland to attend the hearing.

4.2. Phishing

It refers to a type of scamming where victims are tricked to reveal sensitive information or by installing a malware that may contain salami attacks, viruses, worms, that can mirror a targeted website (Jansson & von Solms, 2011). It may be done in a manner that there is a slight alteration in the spelling or numerals of a website to resemble the original website such that a victim may not know that he is dealing with a fake website.

---

26 2021 report of the Ministry of Post and Telecommunications. Note 29. https://clck.ru/3QMjCH

27 Law N°2016/007 of 12 July 2016 on the penal code of Cameroon.

28 CFIB/55C/2008(Unreported).

29 CFIB/76C/2009(Unreported).

30 CFIB/255/2010(Unreported).

31 (2014) 2 SLR.

Phishing is commonly used in Cameroon on mobile networks where victims are called or sent text messages from a cell phone or smartphone to deliver a bait message. The fake messages are usually on grounds of erroneous financial deposits into the victims' mobile money accounts. The perpetrator meanwhile has logged the telephone number of the victim into the mobile operator's version of desktop application (APP). The perpetrator then tricks the victim to verify his mobile account details by entering his passcode for a refund with a promise of reward. If the victim request a mobile money service on his account and enters his passcode on his device, it is simultaneously communicated to the perpetrator's desktop app where he gains access to withdraw or transfer funds. This aspect is notorious in Cameroon and almost all mobile telephone users in Cameroon have experienced this phenomenon with a majority falling for the trick. This aspect not only generate fear but also distorts the idea of e-commerce carried out by mobile telephone companies as one of the ways that the telephone operators use to conduct their businesses online. Some cases of this nature have been successful before the laws courts because it is possible to track the number of the perpetrator although, the criminals are at times smart enough to register the withdrawing account number in the names of different individuals who are based in different geo-locations.

4.3. Bank Card Skimming

This is when technology devices are installed on or inside automatic teller machines or at other sales points where perpetrators can capture card details and replicate them[32]. It is also a tactic that criminals use to obtain sensitive information from a debit or credit card. These devices capture and store data that fraudsters later use to make purchases or withdrawals at different times[33]. Bank card skimming is not very common in Cameroon because of the scarcity of the technological devices used and because most ATMs and sales points are secured with cameras and guards. Although it is still possible for skimmers to physically steal card details when they are left carelessly.

4.4. Socio-legal impacts of cybercrimes on e-commerce transactions in Cameroon

Cybercrimes have many negative consequences on businesses and e-commerce users ranging from loss of confidence to bankruptcy of businesses and other social ills across the countries (Luu et al., 2025; Higgs & Flowerday, 2025b; Lee et al., 2023; Holt, 2022; Hornuf et al., 2025). Cybercrimes related to e-commerce has social and legal consequences and creates the fear of victimization on potential users willing to pay

[32] Federal Bureau of Investigation. Skimming. https://clck.ru/3QEhzV

[33] BrightBridge Credit Union. https://clck.ru/3QEi7p

for goods and services through online platforms. Fright is an element that affects the physical and psychological dispositions of every human being. It erodes confidence and pushes people to do cost benefit analysis with some results that lead people to prefer cash payments on the spot[34].

The proliferation of cybercrimes in e-commerce transactions can be explained under the utilitarian and the rational choice theories[35] where human nature tends to situate people in a position that maximizes their satisfaction even if it means to engage in irrational choices that at times may achieve a positive goal without fear of the consequences. The utilitarian view considers satisfaction as a factor that can overshadow rational behavior. This explains why a majority of youths and young people in Cameroon in some places like Buea and Bamenda have picked up scamming as a trade within the Molyko and Bambili neighborhoods respectively. E-commerce related cybercrimes have also grown rapidly in these areas because of the socio-political conflict in the English-speaking regions of Cameroon. This situation is further aggravated by a high unemployment rate amongst the youths, a low minimum wage level across the country[36] and a general low salary scale in Cameroon. Most of the youths in these areas in Cameroon especially the females open fake online shops purporting to do e-commercial transactions through social media platforms to mask the illicit sources of their income. E-commerce related cybercrimes were mostly committed in the past by males who engage in deceptive tricks by electronically producing rare images of objects and animals that do not exist to entice their victims.

Due to the introduction of modern ICT infrastructures and easy access to the internet at affordable costs in Cameroon, Scamming and phishing are nowadays common in most populated cities. A survey carried out by the author between January to April 2025 at Molyko in Buea where 250 sample responses were obtained from random participants revealed that at least 60 % of the youths in Molyko are involved in e-commerce related cybercrimes. The data collected also revealed that 10 % of the perpetrators were females while 50 % were males ranging from the ages of 16 to 35 years. It was also observed that most of the victims are people residing in Molyko and know their victims. A few victims were unknown by the perpetrators while some of the victims resided in different cities of Cameroon and abroad.

---

34 Many purchasers in Cameroon prefer to buy and do spot payments in cash for products that they can see and fill. This is the reason why most people in Cameroon move with cash despite the attendant risks.

35 See the Rational theory supra.

36 The minimum wage in Cameroon is 46,939frsCFA less than what obtains in other neigbhouring African countries.

The survey also found out that the illicit financial benefits derived from these cybercrimes vary significantly in amounts with few perpetrators making huge amounts almost on regular basis while some just barely make pocket money for the day. The activities of the perpetrators involved mostly scamming and phishing. The survey concluded that most of the youths in Molyko get involved because of the need to satisfy their ego for money, competition, peer pressure, strain and the insignificant number of prosecutions because of corrupt practices. It was also concluded that most perpetrators are still actively involved in cybercrimes related to e-commerce transactions while still perfecting their skills.

It was also discovered that many youths have dropped out of school as observed by Yushawu Abubakari in his article in 2020 (Abubakari, 2020). While some youths who have been submerged by cybercrimes paid others out of their illicit gains to sit for their school examinations[37].

Occult practices[38] are also common with dire consequences amongst cybercriminals in Cameroon because most youths with low intellectual capacity are lured to believe that their successes are dependent on such practices to convince their victims. These practices have led to some fatalities and the emergence of organized gangs of fraudsters who at times jointly contribute bribes to 'make a way out' for their counterparts in trouble. The levels of these occult practices extend to other social aspects like homosexuality, Lesbianism incest and sexual activities under the same roof[39].

All these factors as earlier observed have contributed to a high level of school dropouts thereby increasng the level of illiteracy amongst the youths in Cameroon. Meanwhile the Cameroonian government has despite this sacrificed to educate its youths by subsidizing primary, secondary and university education throughout the country.

4.5. The Proliferation of other offences due to e-commerce related cybercrimes

Illicit wealth derived from cybercrimes related to e-commerce in Cameroon has led to the proliferation of other offences like drugs abuse, prostitution, public drunkenness, impersonation in examinations, sexual offences, defamation, violence, corruption, identity theft, assault, battery reckless driving etc. Unexpected wealth can lead to psychopathic tendencies especially amongst youths whose mental capacities are still developing. This was also observed in the survey conducted.

---

37 Some of the cases of impersonation have been detected during disciplinary board sessions by authorities of universities based in Molyko.

38 Occultism describes various practices and beliefs related to the study of manipulation of supernatural forces. It involves a wide range of practices including divination, magic, alchemy, astrology and spiritualism.

39 Although there are human rights activists today in Cameroon who carry out the activiies aimed at protecting the rights of lesbians, gays, bisexuals, transgender and queer people (the international movement of LGBTQ is recognized as extremist and banned in the territory of the Russian Federation).

4.5.1. Loss of trust and confidence by e-commerce users

It is common today to see most youths in Cameroon who are living a flamboyant lifestyle while riding cars of a particular mark without any proof of their financial means. This attitude is directly linked to the high rate of e-commerce related cybercrimes and corrupt practices. Cameroon's corruption index according to transparency international in 2024 was 26 points /100, far higher than most countries in the world[40]. These results can be partially attributed to cybercrimes in e-commerce and the accompanying frivolous investigative practices that are laden with bribery and corruption with little follow up at the level of the International Police Organization (INTERPOL)

The Cameroonian 2010 law on cybersecurity attributes the jurisdiction and authority of investigative officers[41] who should abide by the rules of criminal procedure as captured by the 2005 Criminal Procedure Code[42]. But unfortunately, most of these officers collude with the perpetrators for personal gains and so most cybercrime cases hardly go to court for proper determination[43]. It is common to find cases where a suspected cyber offender is arrested because of his suspicious financial activities by police and gendarme officers even without a complaint, who accompany the suspect to ATM machines to collect their own purported share of ill-gotten money. These offices at times force the suspects to transfer money from their mobile money accounts to their own phones before letting them go. It is common to see the accomplices of suspects contributing bribes for the release of one of theirs in trouble. Some cyber offenders have made it a habit to put some officers on their pay roll who have always shielded them from any possible eventuality. Suspects who fail to co-operate with the officers have more often been subjected to arbitrary arrest and detention with torture. This raises an issue of due process and failure by the officers to maintain the rule against torture as enshrined in the ICCPR, ACHPR and other national legislations.

All these negative aspects put together has eroded trust and confidence on the country's citizens to a greater extent both home and abroad. Many opportunities to carry out legitimate e-commerce transactions in Cameroon with foreigners has been compromised for lack of trust. It may be noted that many Cameroonians residing abroad are well known for cybercrimes that has led to the incarcerations with some serving long prison sentences in foreign countries. The phenomenon of hiding cyber criminals for a bribe is experienced today in many African countries (Sarefo et al., 2023; Matias, 2025). Most investigative officers prefer to take a bribe than to prosecute perpetrators before the law courts because of their ego.

---

40 Transparency International. https://clck.ru/3QEjAB

41 Section 52(1) of Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon

42 Sections 59 and 60 of Law N°2005 of 27 July 2005 on the Criminal Procedure Code.

43 Some of the bribes are taken most often from the suspects by force and coercion.

Loss of trust and confidence in commercial transactions is experienced at the interpersonal levels of relationships, corporate bodies and sovereign states (Wright & Kumar, 2023; Yi et al., 2024; Porcedda, 2023; Sarkar & Shukla, 2024; Tok et al., 2025; Onwuadiamu, 2025). As noted by B. Rainer and Tyler Moore (2012), most individuals who have been victims of cybercrimes in online commercial transactions end up never engaging in it again for fear of victimization while those who do not know about cybercrimes are more likely to engage in online commercial transactions. The impact of cybercrimes on e-commerce has therefore discouraged many foreigners from engaging in e-commerce transactions with Cameroonians in general. This loss of confidence is linked not only to Cameroonians but also to the neighboring West African citizens, as examined by Yushawu in his paper (Abubakari, 2020).

Significant financial losses have been experienced in Cameroon due to e-commerce related cybercrimes because there is a great latitude of choice and freedom in cyberspace[44], prospective e-commerce users prefer to deal with other nationals for fear of being victimized on Cameroonian e-commerce platforms. The estimated losses on the economy of Cameroon caused by e-commerce related cybercrimes in 2021 was revealed by the Ministry of Post and Telecommunication which is the competent ministry that deals with communication issues in Cameroon. The ministry's report estimated according to ANTIC and ANIF[45] that Cameroon lost approximately 12.2 billion francs CFA in 2021 due to scamming and phishing.

4.5.2. Arbitrary arrests and detentions due to e-commerce related cybercrimes

Arbitrary arrests and detention for suspicion on e-commerce related cybercrimes without any complain in violation of due process are frequent in the major cities of the Northwest and Southwest regions of Cameroon with Buea, Bamenda and Limbe being notorious. The preamble of the Cameroon constitution[46] is clear that no person shall be arrested or detained except in the manner determined by law. The law that determines such arrest in Cameroon is the Criminal Procedure Code[47]. Contrary to the constitutional and procedural provisions on arrest and detention, most cybercrime suspects are arbitrarily arrested without arrest warrants nor under the flagrante delicto procedure[48] as prescribed by the CPC. This can be attributed to the fact that the persons conducting such arrest are aware that they could make quick income through bribes that some cybercriminals are willing to pay as trade-off for their freedom.

---

44 Lawrence Lessig puts it as democracy in cyberspace.

45 2021 report of the Ministry of Post and Telecommunications. Note 24 and 25. https://clck.ru/3QMjCH

46 Law N° 96-6 of 18 January 1996 (as revised)

47 Section 30 of Law N° 2005 of 27 July 2005 on the Criminal Procedure code.

48 Section 31.

Due process is a fundamental aspect of legal proceedings that seeks to protect civil rights. Breaching it may lead to the nullification of an entire case[49]. In the cases of The People v. Mbah Valery[50], and the people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[51], the Court of first Instance Buea acquitted and discharged the accused persons for violating some procedural aspects of criminal procedure that included illegal arrests and detention. The trial court held in the latter case that although the character of the accused persons was doubtful, they should walk away from the court as free people. This was because of serious procedural errors that violated the provisions of sections 3 and 8 of the Criminal Procedure Code. The decision was not meant to encourage the actions of the accused but went a long way to show the importance of protecting fundamental human rights[52]. It therefore becomes problematic when suspects are intercepted by the forces of law and order in violation of their constitutional and legal rights under the pretext of enforcing the law. Most of the victims of such arrest are not only tortured at times but their financial resources are also extorted by coercion. This justifies the purported "good will" of some police officers to fight cybercrimes in Cameroon.

Arbitrary arrests and detention without due process ought to be discouraged because it violates the fundamental principles of civil liberty enshrined in most international conventions and domestic laws. Article 9 of the International Covenant on Civil and Political Rights (ICCPR) 1966 prohibits arbitrary arrest and detention while article 6 of the African Charter on Human and People's Rights (ACHPR)1987 guarantees the right to liberty and clearly articulates that the deprivation of this freedom must be for reasons and conditions laid down by the law. These legal provisions are applicable in Cameroon pursuant to article 45 of the 1996 constitution as revised[53].

Cases of illegal arrests and detentions due to e-commerce related cybercrimes are common in the Northwest and Southwest regions of Cameroon as compared to other regions of the country (Abubakari, 2020). This has partially been attributed to the socio-political crisis plaguing the two regions (Boraine & Leno Doris, 2019). The crisis has contributed to an increase in e-commerce related cybercrimes meanwhile the officers who have been deployed to these regions have seized the opportunity to unlawfully arrest and detain suspect for their personal benefits under the pretext of economic crimes. This has invariably led to a fragrant disregard of the legal provisions that guarantee civil liberties.

---

49 See sections 3 and 8 of the CPC dealing with absolute and relative nullity. See also the decision of Lord Denning in the case of United Africa Company Limited (U.A.C) v. Macfoy dealing on nullity.

50 CFIB/255/2010(Unreported).

51 (2014) 2 SLR.

52 See ICCPR and the ACHPR.

53 Article 45 of Law N° 96-6 of 18 January 1996 on the Cameroonian Constitution.

4.6. Economic impacts on e-commerce caused by cybercrimes

The growth of e-commerce related cybercrimes in Cameroon has led to financial losses and profits on individuals and corporate bodies, leading low incentives to engage in e-commerce transactions. This is because fears caused by cybercrimes due to victimization have a greater impact in cyberspace because many people are worried of becoming victims of cybercrimes (Yokotani & Takano, 2021). This invariably has a nexus with the demand for e-commerce transactions, and may significantly reduce turnover and output because of loss capital and profits due the actions of cybercriminals. Some financial losses because of e-commerce related cybercrimes may lead to bankruptcy. The amount of financial loses for instance as observed above cause due to cybercrimes in 2024 was about 12.2 billion francs CFA. This has a huge impact on the economy and besides the illicit financial gains made from e-commerce related cybercrimes are not taxable.

All of the above distorts the smooth functioning of e-commerce in Cameroon. One of the purposes of e-commerce is to achieve fast turnover. With the proliferation of cybercrimes in Cameroon, there is a huge challenge as the demand for e-commerce services dwindle. Loss of trust and confidence due to cybercrimes in e-commerce has also significantly destroyed the economy of the country in different ways increasing inflation[54], money laundering and currency counterfeiting.

Conclusion

This article has examined the impacts of Cybercrimes related offences on e-commerce in Cameroon and has observed that most cybercrimes in Cameroon are targeted towards fake e-commerce transactions. It has been found out that the economic situation of Cameroon, the easy access to ICT tools, the conflict in the Southwest and North west regions of Cameroon and the need to live flamboyant live styles are some of the contributing factors in Cameroon that have led a high rate of e-commerce related cybercrimes. It was found out that there are socio-legal and economic impacts and the proliferation of other crimes as a result. The high rate of cybercrimes related to e-commerce transactions in some major cities of Cameroon are mostly perpetrated by youths with the number of potential future offenders on the rise. This was demonstrated by the results of a survey carried out and the reports of the Ministry of Post and Telecommunication. It was also discovered that the role of the institutions charged with combatting cybercrimes in Cameroon is limited. The findings also reveals that e-commerce related cybercrimes in Cameroon has led to loss of trust and confidence with arbitrary arrests and detentions in violation of some international treaties, constitutional and criminal procedure provisions. It has

[54] It can be observed that the prices of basic commodities in Buea is high as compared to other cities in cameroon because of illegal wealth that is used in Buea by mostly youths who are scammers.

been observed in this article that most suspect are hardly brought before the competent law courts because police officers prefer to take bribes and set the suspects free. The findings further show that cybercrimes in e-commerce related transactions has tarnished the reputation of Cameroonians at home and abroad and most foreigners have lost trust and confidence to conduct online businesses with Cameroonians. This loss of trust and confidence is attributed to lack of proper home address systems and social security numbers attributed to Cameroonians.

It is therefore recommended that legal, technological, social and economic reforms should be instituted in Cameroon to resolve the issues identified. The legislations in force should be improved upon by specifically addressing the procedural rules to follow at the investigative and litigation stages on cases of e-commerce related cybercrimes. The law should empower the National Financial investigation agency (NFIA) and the National Agency for information and communication technologies (NAICT) to prosecute cases of e-commerce related cybercrimes. The forces of law and order should be trained regularly on arrest and detention on cybercriminal while providing them with incentives for successful e-commerce related cybercrime prosecutions. Serious sanctions should also be applied in cases of corruption and bribery under cybercrimes. The minimum wage level and the salary scale of Cameroon should be improved while creating new jobs to absorb idle youths. Schools should introduce cybersecurity and e-commerce lessons in their curriculum from the elementary level up to the universities. A proper home address system and social security numbers should be instituted in Cameroon for easy identification. Digital rights management systems and tracking technology should be improved.

References

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Author information

Lekunze Anoumbuandem Benvolio – PhD, Lecturer, Department of English Law, University of Buea
Address: PO Box 63, Buea, Cameroon
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 27, 2025
Date of approval – May 9, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия

Анумбуандем Бенволио Лекунзе

Университет Буэа, Буэа, Камерун

Ключевые слова

безопасность,
Камерун,
киберпреступность,
мошенничество,
право,
правосудие,
транзакции,
фишинг,
цифровые технологии,
электронная коммерция

Аннотация

Цель: проанализировать влияние киберпреступности на операции электронной коммерции в Камеруне и оценить эффективность существующих правовых механизмов противодействия киберугрозам.

Методы: исследование базируется на теориях утилитаризма, транзакционных издержек и рационального выбора. Применена методология качественного исследования с использованием доктринального метода. Проведен комплексный анализ правовых актов Камеруна в сфере кибербезопасности и электронной коммерции. Выполнено социологическое обследование с получением 250 выборочных ответов от жителей района Молико в городе Буэа в период с января по апрель 2025 г. Исследованы судебные прецеденты и статистические данные Министерства почты и телекоммуникаций Камеруна.

Результаты: установлено, что киберпреступления привели к потере доверия к операциям электронной коммерции в Камеруне, что отражается на снижении желания граждан осуществлять онлайн-транзакции. Выявлено, что более 60 % молодежи в возрасте от 16 до 35 лет в крупных городах Камеруна либо вовлечены в киберпреступления, связанные с электронной коммерцией, либо пострадали от них. Зафиксирован рост числа женщин среди киберпреступников. Определены основные виды киберпреступлений: мошенничество, фишинг и хищение средств с банковских карт.

Научная новизна: комплексный междисциплинарный анализ влияния киберпреступности на электронную коммерцию в контексте развивающейся африканской экономики. Впервые проведено эмпирическое исследование масштабов киберпреступности в конкретном регионе Камеруна с количественной оценкой вовлеченности молодежи в противоправную деятельность. Разработана теоретическая модель, объединяющая концепции утилитаризма, транзакционных издержек и рационального выбора для объяснения мотивации

киберпреступников. Выявлены специфические социально-правовые факторы, способствующие росту киберпреступности в условиях социально-политического кризиса.

Практическая значимость: результаты исследования имеют важное прикладное значение для совершенствования правовых, технологических, социальных и экономических механизмов противодействия киберпреступности в Камеруне. Предложенные рекомендации включают реформирование процессуального законодательства, расширение полномочий специализированных органов, введение системы домашних адресов и номеров социального страхования, повышение минимальной заработной платы и интеграцию курсов кибербезопасности в образовательные программы. Полученные данные могут быть использованы правительственными структурами, судебной системой, образовательными учреждениями и международными организациями для разработки эффективных стратегий борьбы с киберпреступностью и развития безопасной цифровой экономики.

Для цитирования

Лекунзе, А. Б. (2025). Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия. *Journal of Digital Technologies and Law*, *3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

Список литературы

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Сведения об авторе

Лекунзе Анумбуандем Бенволио – PhD, преподаватель, кафедра английского права, Университет Буэа
Адрес: Камерун, г. Буэа, а/я 63
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 27 апреля 2025 г.
Дата одобрения после рецензирования – 9 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.