International Journal for Research Trends in Social Science & Humanities
Volume 4, Issue 2
Mar-Apr 2026, PP 1-19

Digitalization and Cyber Space Regulations in Cameroon: Challenges and Opportunities

Sokem Assoua Riccardo, Betana Kholbert Mbimbe
Faculty of laws and Political Science,
The university of Buea, Cameroon

Abstract- The regulation of cyberspace in Cameroon is increasingly critical as the country navigates the complexities of advanced digitalization. However, With the on-going Anglophone crisis in the two English-speaking regions of Cameroon, individuals, businesses and the government are increasingly becoming at risk of being targeted by cyber criminals. Amid this challenge, Cameroon has enacted a law relating to Cyber Security and Cyber Criminality and trained personels to fight cybercrime. In spite of these measures, cybercrime is still rampant and the question is why?. As internet usage increases, so does exposure to cyber threats such as hacking, data breaches, and online fraud. This paper's aim is to investigate the extent to which effective cyber space regulation can be achieved in Cameroon to support safe digitalization. By employing the theory of Digital Sovereignty as its theoretical construct while adopting advocacy for liberation as it's philosophical framework, this paper argues that, the proliferation of internet and volume of digital transactions does not correlate significantly with the evolution of national cyber security regulations in Cameroon The paper however strongly recommends, the development of a centralized monitoring digital and evaluation framework to track the progress of digitalization efforts and assess their impact.

Keywords- Digitalization, cyberspace, regulation, cybercrime.

I. Introduction

The information age is increasingly mobile with ever finer webs of potential connectivity overlaying the physical spaces we inhabit. While commentators have long argued that cyberspace can only be understood in reference to material places (Zook, 2000:75). In fact, we argue that services such as Google, Local engender a type of hybrid space (Couclelis, 1996), which we term DigiPlace, in which digital data and physical places are continually re-combined into lived, subjective space as one negotiates through time, space and information. Particularly novel factors behind the construction and experience of DigiPlace are: the ability to access it in real time and on the move, and the impact of this electronic visibility on perceptions of physical accessibility.

Apparently, The Internet has witnessed substantial growth over the past three decades, leading to the conceptualisation of a new communication dimension as a representation of cyberspace, considered the most significant achievement of modern man (Amant et al., 2017). Gibson (1984) first coined the phrase 'cyberspace' in the novel Neuromancer, where the author viewed it as a graphical representation of data obtained from the memory banks of all computers present in the human system. As such, cyberspace can be explained as a new communication medium emerging from globally interconnected computers. Cyberspace can further be delineated as the virtual

environment developed by computing systems and the users who interact within it (Schatz et al., 2017).

The Internet Utilisation Statistics (IUS) reported that the number of users has grown by 444.8% since 2000. Asia possesses the highest number of users (42%), followed by Europe (24.2%) and North America (13.54%). The rest of the users are distributed between Latin America/the Caribbean (10.4%), Africa (5.6%), and Oceania/Australia (1%). (Gomez-Diago, 2012:90). Cyberspace comprises a pivotal aspect defining modern life as it empowers communities and individuals to organise and connect themselves in and through it (Boyle, 2017).

The period between 2000 and 2010 witnessed an expansion in global Internet usage from 360 million to over 2 billion people. As this expansion of Internet usage continues, cyberspace culture is anticipated to continually grow and become interwoven in the daily life of individuals across the globe. Furthermore, given that a significant proportion of the population does not play any role in cyberspace, the advancement of wireless communication technologies is facilitating the emergence of interactive communication within horizontal networks. As a result, this enables different people to share synchronous and asynchronous messages through e-mails, chats, SMS, blogs, vlogs, podcasts, and wikis (Hunter, 2017).

For many years, women have occupied a significant portion of cyberspace at the behest of different motivations. For instance, in 2000, a study by the Pew Internet Institute revealed that women used cyberspace to maintain and establish relationships. In a separate study, Solis (2009) reported that platforms such as Facebook, Flickr, FriendFeed, myspace.com, and Twitter were utilised more by women than by men. As people enjoin themselves in networks, they access a wide range of available content on the Internet and can share both information and ideas concerning different situations (Dohr et al., 2010). Additionally, online access empowers individuals to complete diverse activities, such as shopping, completing online studies, or searching for jobs. These facilities further enable the human population to enjoy greater autonomy, in turn influencing their performance and empowering them to handle diverse issues. Women living in isolated regions can now also access opportunities and information they would be unable to access otherwise.

Cyberspace was recently defined as a world-changing domain characterised by the interlinked utilisation of the electromagnetic spectrum and electrons, the target of which is to construct, modify, exchange, use, share, save, and dispose of information and disrupt physical resources (Mayer et al., 2014). Today, communication between humans is becoming increasingly computer mediated and, over time, ubiquitous. Computers have become connected through high-speed networks both local and wide using wireless technologies. Interaction over high bandwidth is also boosting the speed of communication and offers the ability to transmit images, voices, and sound as well as data in a text format (Gungor et al., 2011). Computer-based technologies are thus empowering the creation of entirely new interaction interfaces between humans and machines, along with a completely new virtual space for human–human interaction (Beck, 2014).

Collectively, these new and different communication spaces are referred to as cyberspace. Cyberspace comprises several elements including; Telecommunications devices and physical infrastructures empowering the interconnection of networks of communication and technological systems, computerised systems and the associated software ensuring that domains operate and connect as required, networks linking computer systems together, networks that link the computer networks linking computer systems, access nodes for users and intermediaries that route nodes; and data residing in the systems (Smirnov, Levashova and Kashevnik, 2019).

A common school of thought posits that culture is associated with the past as well as the conservation and relaying of traditions in a particular community (Morin, 2016). However, a different cultural face is directed towards the future namely, the forward-facing outlook of culture, comprising creation rather than a conservation of focus on memory and imagination. The ability to discern new and unexpected scenarios to induct people into computer-mediated environments is required in the new environments they inhabit (Rouse and Dionisio, 2018). Nonetheless, despite the wide spread of computer systems, Rouse and Dionisio's understanding of functions as mediation tools remains relatively poor. Individuals can often feel disconnected in a technology-based world that appears strong and powerful in its physical presence while remaining hidden and difficult in another sense namely, the understanding of the human experience they portray (Burda and Harding, 2013:45). Subsequently, understanding the present situation requires cultural imagination that involves speculating and affirming the likelihood of other forms of life that differ from the commonplace experiences to which users are accustomed in a natural manner as it shapes the mind through cultural transmission processes (Shweder et al., 1998).

According to Gomez-Diago (2015), cyberspace culture embraces the set of attitudes, thought processes, values, and practices that grow together with cyberspace. By referencing the interaction between the different concepts, associations between culture and technology can be clearly identified. The lack of boundaries, whether nationally or locally in the environment, also encourages and enhances conversations between individuals drawn from diverse cultures (Gomez Diago, 2012). Higher education cyberspace culture is delineated as an intellectual space culture to which users gain access via computers and which empowers users in the context of higher educational to collaborate with virtual reality, avatars, and text (Saunders et al., 2009). In this cyberspace culture, educators and students are provided with a unique opportunity to undertake a wide range of computer-accessed learning, both planned and unplanned.

Cyberspace security and threats represent a concern for all stakeholders, not just the government, public authorities, commercial enterprises, or individuals (Caton, 2012). Therefore, Digitalization which refers to how the technological revolution is transforming value chains in revolutionary ways and opening new opportunities for value addition and structural change has the potential to support economic growth throughout the world (Digital Economic Report 2019)

However, Cameroon has witnessed significant growth in internet penetration over the past decade. According to the International Telecommunication Union (ITU), internet usage in Cameroon increased from approximately 10% in 2010 to over 50% by 2023

(ITU, 2023). This surge is attributed to the expansion of mobile networks and affordable smartphones, which have made access to digital services more widespread. The digital economy is becoming increasingly important for economic growth, with e-commerce and online services gaining traction among citizens.

Moreover, Cameroon has made strides in establishing a legal framework for cybersecurity and data protection. The Cybersecurity Law, enacted in December 2010, was one of the first steps toward addressing cyber threats. However, this law is now considered outdated due to rapid technological advancements and the emergence of new cyber threats. Additionally, Cameroon has recently promulgated Law No. 2024/017, which focuses on personal data protection. This law emphasizes informed consent, data accuracy, and cross-border data transfers but lacks provisions specifically addressing AI governance or automated decision-making processes.

Digitalization presents substantial opportunities for economic development in Cameroon. The World Bank highlights that digital technologies can enhance productivity and create new markets (World Bank, 2022). For instance, small and medium-sized enterprises (SMEs) can leverage online platforms to reach broader audiences beyond their localities. E-commerce platforms like Jumia have emerged as vital players in facilitating trade within the region. Digital tools also offer prospects for improved governance and public service delivery. E-governance initiatives can enhance transparency, reduce corruption, and increase citizen engagement (UNDP, 2021). By digitizing public services, the Cameroonian government can streamline processes such as tax collection and permit issuance, making them more efficient.

The rise of social media platforms has fostered greater connectivity among citizens. Platforms like Facebook and WhatsApp enable individuals to communicate freely and share information rapidly. This connectivity can empower civil society organizations by providing them with tools for advocacy and mobilization (Freedom House, 2023).
Finally, regulating cyber-space in Cameroon amidst advanced digitalization presents a dual-edged sword offering numerous opportunities for economic growth and improved governance while simultaneously posing significant challenges related to cybersecurity threats, misinformation dissemination, and inadequate regulatory frameworks.

Statement of the Problem

In recent years, Cameroon has witnessed a surge in internet usage, with millions of citizens gaining access to online platforms for communication, commerce, education, and social interaction. This digital transformation presents numerous opportunities for economic growth, innovation, and improved governance. However, it also raises pressing concerns regarding cybersecurity, privacy rights, misinformation, and the overall integrity of digital spaces.

With the on-going Anglophone crisis in the two English-speaking regions of Cameroon, individuals, businesses and the government are increasingly becoming at risk of being targeted by cyber criminals. Amid this challenge, Cameroon has enacted a law relating to Cyber Security and Cyber Criminality (hereinafter referred to as the Cyber law) and trained personels to fight cybercrime. In spite of these measures, cybercrime is still rampant and the question is why?. As internet usage increases, so does exposure to

cyber threats such as hacking, data breaches, and online fraud. The African Union's Agenda 2063 emphasizes the need for robust cybersecurity frameworks across member states (African Union, 2022).

However, Cameroon faces challenges in developing comprehensive cybersecurity policies due to limited resources such as Limited Infrastructure, Domestic and foreign investment in technology remains low, limiting the resources available for developing comprehensive regulatory frameworks, Existing laws often suffer from poor enforcement due to inadequate institutional capacity and limited public awareness about rights related to data privacy, a significant portion of the population lacks awareness regarding their digital rights and how to protect themselves against cyber threats (Digital Literacy Gap) and limited expertise. The digital space has also become a breeding ground for misinformation and hate speech. The spread of false information can incite violence or unrest; thus, regulatory measures must balance freedom of expression with protecting public order (Reporters Without Borders, 2023). The challenge lies in creating laws that effectively address these issues without infringing on individual rights. Cameroon's existing legal framework regarding cyber regulations is still evolving. While laws such as the Law on Cybersecurity and Cybercrime were enacted in 2010 to address some issues related to digital activities (Government of Cameroon, 2010), enforcement remains inconsistent. There is a pressing need for updated legislation that reflects current technological realities while ensuring compliance with international standards.

This paper, by intending to throw more light on challenges and opportunities pertaining to digitalization and cyberspace regulations in Cameroon, aims to examine the extent to which the proliferation of internet and volume of digital transactions correlate with the evolution of national cyber security regulations.

II. Literature Review

The literature review attempts to discuss the various literature related to the regulations of the cyberspace in Cameroon in the age of advanced digitalization. The discussion also identifies gaps left by other researchers of similar studies. However, this paper attempts to fill those gaps so that the write-up can contribute to a new body of knowledge in the academic world. Through this review, literature is re-packaged and analysed as a way of bringing new insights into the problem studied.

Conceptual Review

- **Cyberspace**

The phrase 'cyberspace' was coined in 1982 by a Canadian science fiction author, William Gibson, in an article that appeared in the Omni magazine, and thereafter in his novel Neuromancer (Jahshan, 2007). In his definition, Gibson conceptualised cyberspace as a virtual world created by computer networks and inhabited by intelligent beings. An excerpt from Gibson's novel describing cyberspace delineated the concept as 'a graphic representation of data abstracted from the banks of every computer in the human system' (Gibson, 1984:51). As such, the author advanced the idea of a space in the digital realm that could be inhabited and explored.

Examining the root definition of the term 'cyberspace' further reveals a similarity in concept to the connotation made by Gibson. According to Berdayes and Murphy (2000), cyberspace is constructed of two root words: 'cyber' and 'space'. Cyber derives from the Greek word for 'pilot', thereby advancing the idea of steering, controlling, or piloting. Space, meanwhile, appears in the English language with diverse meanings, such as a time lapse or duration or a physical expanse (Van Manen and Adams, 2009:56). A philosophical view of space by Hobbes connoted the idea of an unbounded continuum void of matter (Berdayes and Murphy, 2000). Therefore, cyberspace communicates the idea of control and unboundedness, or concretion and abstraction. Gibson shared the same view by conceptualising cyberspace as an imaginary space in the digital landscape where intelligent beings are free to explore and engage creatively.

Based on this understanding, it can be argued that the conceptualisation of cyberspace can be traced back to the early WWII period, when allies were investigating how electronic technology could be employed to improve radar signals and developing machines that could compute complicated radar messages (Kaisler, 2016). While computers were not yet fully developed during this era, a different school of thought argues that there existed computing devices that created virtual platforms where allies could engage with one another. Axelord (2014) further highlighted that technological disruptions have been catalysing cyberspace since their inception during the WWII period. A particular disruption concerned the creation of the Advanced Research Projects Agency network (ARPAnet) by the United States Department of Defence in the 1960s (Liu and Albitz, 2009:10).

The ARPAnet connected research organisations and government agencies in the U.S., allowing them to share scarce computing resources. By the mid-1970s, educational institutions and the government developed an interconnection of computers via networks to share information and messaging. For instance, the UCLA and the Stanford Research Institute (SRI) were interconnected using the ARPAnet through packet-switching technology (Liu and Albitz, 2009). By the mid 1980s, the observed increase in network interconnectivity led to a technological gold rush and effectively brought about the creation of new fortunes and the unprecedented demise of older regimes; a new economy thus began to be developed by enthusiastic engineers and venture capitalists, leading to the creation of a new venture in the Information Super Highway (Brown, 2014:34).

In 1990, a new innovation was developed by Tim Berners-Lee, a computer programmer working at the Conseil Européen pour laRecherché Nucléaire (CERN) in Switzerland. Lee created a system that could empower individuals in a network to access research materials (Brown, 2014). Similarly, they could also share documents across different computer platforms without necessarily having to reformat them. By 1991, Lee had created the first browser, later named the World Wide Web (WWW; Brown, 2014). As such, the Internet boom experienced during the 1990s led to the development of a new system (cyberspace) and a culture associated with it (cyberspace culture).

- **Cyber-security**

Cyber-security can be described as consisting of controls, technologies, and processes designed to protect data, networks, and systems from cyber-attacks (Dorsey et al.,

2017). Lindsay (2015) highlighted that when cyber-security is effective, it lowers the likelihood of cyber-attacks and further ensures that an organisation and its individuals remain protected from the threat of unauthorised exploitation of their technologies, systems, or networks (Lindsay, 2015). An effective cybersecurity approach comprises several protection layers spread across programmes, computers, networks, or data that a user intends to secure. In organisations, the technology, people, and processes ought to complement one another so as to develop effective defences against cyber attacks (Altner and Servi, 2016:32).

- **Definition of Cyberspace**

Gibson's previously discussed definition of cyberspace connoted the idea of a virtual landscape created by computer networks and inhabited by intelligent beings (1984). However, in order to clearly comprehend the term, it is expedient to examine it from the views of other scholars and industry practitioners. It is also important to highlight that the term has since gained significant interest from the non-academic community, including technological strategists, security and military professionals, and medical leaders, together with users of the technology domain (Dawson and Thomson, 2018).
In a literal sense, cyberspace can be described as the interconnection of different forms of technology. This assertion stems from the fact that the Internet backbone comprises three main types of technologies: hardware, software, and protocols (Baldauf and Stair, 2011). While hardware refers to the physical cables and devices that carry data, software describes the different programmes allowing users to interact with the Internet in order to access services and information. Protocols, meanwhile, describe the rules governing the established connections in networks (Bangia, 2005). Different arguments further consider cyberspace to refer to the utilisation of technology in computing environments. This view derives from the understanding that computers have represented an integral part of human culture since the early 1990s. As such, this represents a domain used to refer to the integration of different forms of technology in human beings' everyday life (Li et al., 2017:25).

The combination of emerging trends in cyberspace, including computer technology and the Internet, has been defined as cyberspace culture (Khin et al., 2016). Lévy (2001) further described cyberspace culture as the set of intellectual and material technologies, attitudes, values, and modes of thought that have developed simultaneously with the growth of cyberspace. In contrast, the author defined cyberspace itself as the material infrastructure of digital communications, the diverse information contained within it, and the intelligent beings that navigate and nourish it.

With this insight, it becomes easier to comprehend cyberspace culture as an ongoing trend in the current world that involves including computer and modern Internet technologies in various aspects of a country, such as health, education, infrastructure, and research. The contribution of this Internet and computer technology cannot go unnoticed, and considerable research has accordingly been conducted on this subject (Safa et al., 2018). The majority of such publications examine this contribution in general, and they have proven vital for understanding cyberspace culture.

Cyberspace, as a concept of the Internet, implies that cyberspace usage is not limited solely to global sharing of information in large numbers, but also includes other relevant

aspects, such as distributed creation of information and materials, social networking and network marketing, real time streaming of information from the Internet, mass collaboration of people in the online space to achieve common goals and objectives, collaborative assessment of information shared and distributed online, social bookmarking, and cloud computing, which involves sharing and storing information on the Internet through cloud-storage services for real-time access and retrieval (Chase et al., 2002:67).

All these services encourage commitment and participation in the online space, thus further encouraging the participation of more people. As a result, this contributes to shaping individual lives, including how people talk, their different communities, and even their identities. Bell (2001) expressed a similar view by postulating that the association between technology and society is two-way; as such, computers not only give form to ideas, experiences, and metaphors, but are also shaped by these aspects as well.

The evaluation of different definitions leads to the authors' definition of cyberspace as a virtual platform, wherein interactions occur between technology and individuals residing in the given space. This insight is important for advancing the discussion of the interrelation between cyberspace and culture.

- **Empirical review**

As digital technologies evolve, they create new opportunities and risks. The proliferation of data, the rise of artificial intelligence (AI), and the expansion of the Internet of Things (IoT) have led to significant concerns regarding privacy, security, and ethical use of technology. According to a study by Zuboff (2019), the commodification of personal data has raised questions about consent and individual autonomy in a digital economy.

One major challenge is the pace at which technology evolves. Regulatory frameworks often lag behind technological advancements, making it difficult to implement effective regulations. A report by the European Union Agency for Cybersecurity (ENISA) highlights that existing regulations may not adequately address emerging threats such as deepfakes or AI-driven cyberattacks (ENISA, 2020).

Cyberspace transcends national borders, complicating regulatory efforts. Different countries have varying laws regarding data protection, cybersecurity, and online content moderation. A comparative analysis by DeNardis (2020) emphasizes that this fragmentation can lead to regulatory arbitrage, where companies exploit less stringent regulations in certain jurisdictions.

Regulators face the challenge of fostering innovation while ensuring security and privacy. A study by Binns et al. (2021) discusses how overly stringent regulations can stifle innovation in tech industries, while too lenient approaches can expose users to risks. Empirical studies suggest that collaborative governance models involving multiple stakeholders governments, private sector entities, civil society organizations can enhance regulatory effectiveness. For instance, a framework proposed by Kettunen

et al. (2021) advocates for public-private partnerships to share information on cybersecurity threats and best practices.

Regulatory frameworks should be adaptive to keep pace with technological changes. Research by Scott et al. (2022) indicates that flexible regulations that allow for periodic review and adjustment based on technological advancements are more effective than static rules. International cooperation is essential for addressing cross-border cyber issues effectively. Studies show that treaties like the Budapest Convention on Cybercrime provide a foundation for international collaboration but require further strengthening to adapt to new challenges (Council of Europe, 2020).

One of the most significant regulatory frameworks is the General Data Protection Regulation (GDPR) implemented by the European Union in May 2018. The GDPR aims to protect individuals' personal data and privacy in an increasingly digital world. A study by Kuner et al. (2020) highlights how GDPR has influenced global data protection practices, leading to stricter compliance requirements worldwide (Kuner et al., 2020).

In the United States, the California Consumer Privacy Act (CCPA) serves as a model for state-level data privacy regulations. Research conducted by Zuboff (2019) indicates that CCPA has set a precedent for other states considering similar legislation, emphasizing consumer rights regarding personal data usage and transparency (Zuboff, 2019:45).

One of the primary challenges in regulating cyberspace is keeping pace with rapid technological advancements. A report by McKinsey & Company (2021) emphasizes that regulators often struggle to understand emerging technologies such as artificial intelligence and blockchain, which complicates effective oversight and governance (McKinsey & Company, 2021). A comparative analysis by Bennett et al. (2021) reveals that while some countries have robust regulatory frameworks in place, others lag behind due to lack of resources or political will (Bennett et al., 2021). This disparity can lead to regulatory arbitrage where companies exploit weaker regulations in certain jurisdictions.

The proposed Digital Services Act aims to create a safer digital space within the EU by establishing clear responsibilities for online platforms regarding harmful content and user safety. An analysis by Cohen & Sundararajan (2022) discusses how this act could reshape platform accountability and enhance user protections against misinformation and hate speech online (Cohen & Sundararajan, 2022).

China's Cybersecurity Law, enacted in June 2017, mandates strict controls over data localization and cybersecurity measures for network operators. A study by Liang & Zhang (2023) examines how this law reflects China's approach to maintaining control over information flow within its borders while promoting national security interests (Liang & Zhang, 2023).

As of 2025, Africa is experiencing rapid digital transformation, with increasing internet penetration and mobile connectivity. According to the International

Telecommunication Union (ITU), internet usage in Africa grew from 11% in 2010 to over 40% by 2023 (ITU, 2023). This growth presents both opportunities and challenges, particularly concerning cybersecurity, data protection, and privacy.

One significant study by Kshetri (2022) examines various cybersecurity frameworks implemented across African nations. The study highlights that countries like Kenya and South Africa have developed national cybersecurity strategies aimed at protecting critical infrastructure and enhancing public-private partnerships. However, Kshetri notes that many African countries still lack comprehensive legal frameworks to address cybercrime effectively.

Another critical area of focus is data protection. A study by Moyo et al. (2023) analyzes the implementation of data protection laws across several African countries. The authors found that while some nations, such as Nigeria and South Africa, have enacted robust data protection regulations (e.g., Nigeria's Data Protection Regulation of 2019), enforcement remains a significant challenge due to limited resources and awareness among citizens about their rights.

Research by Muthoni (2024) delves into internet governance issues in Africa, emphasizing the need for multi-stakeholder approaches involving governments, civil society, and private sectors. Muthoni argues that effective governance can enhance trust in digital services but requires transparency and accountability mechanisms to prevent misuse of power. A report by the African Union (AU) indicates that inadequate infrastructure hampers effective regulation efforts. Many regions still face issues related to electricity supply, internet access, and technological literacy (AU, 2023). These limitations hinder the ability of regulatory bodies to monitor online activities effectively.

Political interference poses another significant challenge. Research conducted by Oduor et al. (2023) reveals that government censorship and control over digital spaces often undermine regulatory efforts aimed at promoting freedom of expression and access to information. The authors argue for a balanced approach where regulations protect citizens without infringing on their rights. Capacity building is essential for improving regulatory frameworks. A study by Ndung'u (2024) emphasizes training programs for law enforcement agencies and judicial officials on cyber laws and digital evidence handling as crucial steps toward enhancing regulatory effectiveness. Regional cooperation is vital for addressing cross-border cyber threats. The East African Community's initiatives towards harmonizing cybersecurity laws illustrate how collaborative efforts can lead to more robust regulatory environments (EAC Report, 2024).

Cameroon has seen a substantial increase in internet penetration, which was reported at approximately 60% as of early 2023 (World Bank, 2023). This growth has necessitated the development of regulatory frameworks to manage online activities effectively. The government has implemented various laws aimed at cybersecurity, data protection, and online content regulation.

Law No. 2010/012: This law addresses cybercrime and establishes penalties for offenses such as hacking, identity theft, and online fraud (Cameroon Ministry of Posts and Telecommunications, 2010).

Law No. 2016/012: This legislation focuses on the protection of personal data and privacy rights within the digital space (Cameroon National Assembly, 2016).
These laws are part of a broader strategy to create a safer online environment while promoting digital innovation.Several empirical studies have been conducted to analyze the effectiveness and implications of these regulations:

A study by Ngoh et al. (2022) examined the impact of cybercrime on businesses in Cameroon. The researchers found that over 70% of surveyed companies had experienced cyber incidents, leading to financial losses averaging around $15,000 per incident. The study highlighted that inadequate enforcement of existing laws contributed significantly to this issue. Another critical analysis by Tchouakeu & Nguimkeu (2023) focused on the implementation challenges associated with data protection laws in Cameroon. The authors noted that while legal frameworks exist, there is a lack of awareness among citizens regarding their rights under these laws. They also pointed out that enforcement mechanisms are weak due to limited resources allocated for monitoring compliance.

A survey conducted by Fokou & Ndong (2023) assessed public perception regarding government regulations in cyberspace. The findings revealed that approximately 65% of respondents felt that current regulations were insufficient to protect them from online threats. Furthermore, many expressed concerns about potential government overreach and censorship.

The studies indicate several challenges faced by Cameroonian authorities:
Limited Resources: Enforcement agencies often lack the necessary tools and personnel to effectively monitor and respond to cyber threats.
Public Awareness: There is a significant gap in public knowledge about cybersecurity measures and personal data rights.
Technological Advancements: Rapid technological changes outpace regulatory frameworks, making it difficult for laws to remain relevant.

From the empirical literature provided above, the study is guided by the following hypotheses
H1 1:$\mu \neq K$, i.e., The proliferation of internet and volume of digital transactions does not correlate significantly with the evolution of national cyber security regulations.

Theoretical framework
The paper adopted the Theory of Digital Sovereignty by J. M. Balkin, 2016. The theory posits that nations must assert control over their digital environments to protect their citizens' rights and maintain national security. Balkin argues that as digital technologies evolve, so too must the legal and regulatory frameworks that govern them. This theory is particularly relevant to Cameroon as it navigates issues related to internet governance, data privacy, and cybersecurity.

The strength of the theory of digital sovereignty lies in its ability to address the complexities and challenges posed by the digital transformation of society, emphasizing the need for states and individuals to reclaim control over their digital environments. Digital sovereignty emphasizes the necessity for states to reassert their authority over digital infrastructures and technologies. As governments face challenges from powerful multinational corporations that dominate the digital landscape, this theory provides a framework for states to protect their citizens' rights, privacy, and security in an increasingly interconnected world.

The Theory of Digital Sovereignty is highly relevant to studying "Digitalization and cyberspace regulations in cameroon" as it provides a framework for understanding how Cameroon can assert control over its digital landscape while addressing issues related to data privacy, national security, economic development, cultural identity preservation, and international relations.

III. Methodology

This paper's focus is the Buea municipality of Cameroon where Antic (National agency for information and communication technologies) branch is found. For the purpose of this study, descriptive research design was used. The descriptive design describes phenomena as they exist. It issued to identify and obtain information on the characteristics of a particular problem or issue. Descriptive research design was selected because it has the advantage of producing good amount of responses from a wide range of people. Also, this design provides a meaningful and accurate picture of events and seeks to explain people's perception and behaviour on the basis of the data collected. The advantage with this design is that it helps to find views as they are in their natural setting and because it is effective, less costly and easily accessible for collecting data from the target population (Schwab, 2005). The target population of this study included the Government officials in Buea, Law enforcement officers, cyber security experts, ISPs, Businesses, General public internet users across various demographics and academics / researchers involved in cybersecurity issues.

In this study, a sample of 120 respondents were used by answering questionnaires for the purpose of getting the findings of the study. A sample of 120 respondents were selected because they were considered to represent and having vital information for the study by virtue of their positions. (Sekaran.,2010:56) stated that, in research investigations involving several hundreds or thousands of elements, it would be practically impossible to collect data from, or test, or examine every element. Even if it were possible, it would be prohibitive in terms of time, cost and other human resources. That's why sampling makes a research feasible.The paper adopted a philosophical framework where primary and secondary data were collected with the aid of Questionnaire ,interview and observations through stratified random sampling method.this method was appropriate as it enabled the researcher to choose a population of interest that would provide answers to the research questions (Kothari,2004).

International Journal for Research Trends in Social Science & Humanities
Volume 4, Issue 2
Mar-Apr 2026, PP 1-19

IV. Presentation and discussion of findings

In this study, the return was 83.3%. majority of the participants were males 64 (63.0%) and majority were within the age group 31-40 37(37.0%).Also, majority of the participants had secondary school certificates 44(44.0%) while majority 41(41.0%) had worked with their organization for 4-7 years..Lastly,44(44.0%) of the respondents in this research were other career oriented.

Table 4.1. Rate of return of questionnaires

Object	Sample population (SP)	Return rate (RR)	SP%	RR%
Total	120	100	100	83.3

Source: field survey 2025

In this study, A total of 120 questionnaires were administered which constitute 100% and a total of 100 questionnaires returned to the researcher which is 83.3%.

Table 4.2 Distribution related to the extent to which the proliferation of internet and volume of digital transactions correlate with the evolution of national cyber security regulations.

	Issues raised	Perception of Respondents						
		SA	A	D	SD	N	SA &A	SD &D
	the extent to which the proliferation of internet and volume of digital transactions correlate with the evolution of national cyber security regulations							
1	The increasing number of internet users directly correlates with the need for more comprehensive cybersecurity regulations.	0 00%	20 20%	24 24%	48 48%	8 8%	20 (20)	72 (72)
2	The rise in digital transactions has significantly influenced the scope and complexity of national cybersecurity laws.	2 2%	26 26%	34 34%	34 34%	4 4%	28 (28)	68 (68)
3	The volume of data generated and transmitted online has necessitated the creation of new cybersecurity regulations.	48 48%	24 24%	22 22%	4 4%	2 2%	72 (72)	26 (26)
4	The evolution of cybersecurity regulations has been primarily driven by the growth of e-commerce and online financial activities.	58 58%	30 30%	8 8%	2 2%	2 2%	88 (88)	10 (10)
5	The proliferation of social media platforms has created a	32 32%	44 44%	14 14%	6 6%	4 4%	76 (76)	20 (20)

	need for specific cybersecurity regulations to address data privacy and security concerns.							
6	The increasing sophistication of cyber threats has led to more stringent cybersecurity regulations.	24 24%	8 8%	38 38%	24 24%	6 6%	32 (32)	62 (62)
7	The development of cloud computing and related services has significantly impacted the focus of national cybersecurity regulations.	20 20%	36 36%	12 12%	22 22%	10 10 %	56 (56)	34 (34)
8	The expansion of the Internet of Things (IoT) has necessitated new regulations to address the security of connected devices.	44 44%	32 32%	18 18%	2 2%	4 4%	76 (76)	20 (20)
9	The globalization of digital transactions has led to international cooperation in the development of cybersecurity regulations.	54 54%	36 36%	4 4%	4 4%	2 2%	90 (90)	8 (8)
10	Cybersecurity regulations are evolving at a pace that is commensurate with the growth of the internet and digital transactions.	70 70%	18 18%	2 2%	6 6%	4 4%	88 (88)	8 (8)
11	The effectiveness of national cybersecurity regulations is directly proportional to the volume of digital transactions occurring within a country.	64 64%	30 30%	0 0%	4 4%	2 2%	94 (94)	4 (4)
	Total	416	304	176	156	48	720	332
	Percentage	37.8 %	27.6 %	16%	14.2 %	4.4 %	65. 4	30. 2

Source: Field survey, 2025

4.2.1 Distribution showing total respondents view according to various questions

Types of response	Cumulative frequency	Total percentage (%)
SA	416	37.8
A	304	27.6
SD	156	16.0
D	176	14.2
N	48	4.4
Total	1100	100

Source: Field Survey 2025

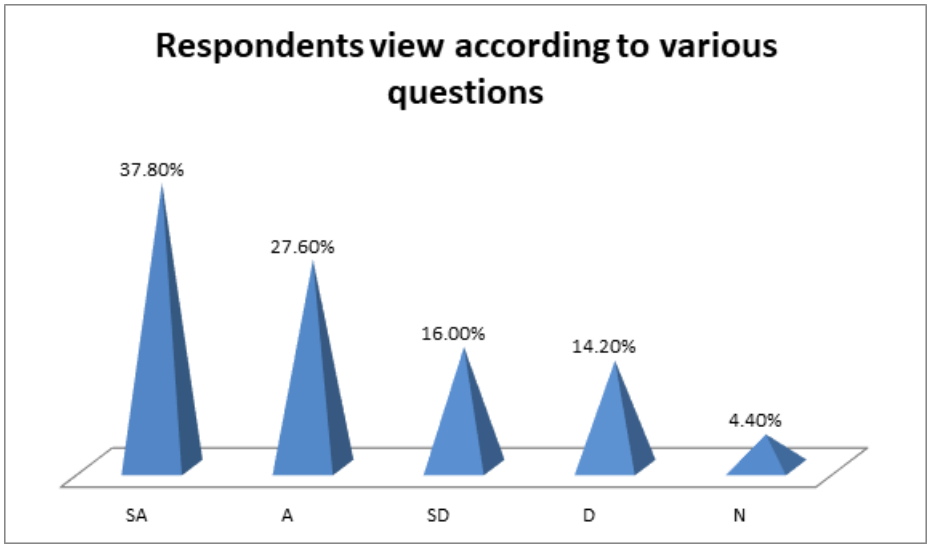

Figure 4.2 pyramids showing total view of respondents according to various Responses.

Source: Field Survey 2025

Data presented on table 4.2 and figure 4.2 above, examines the extent to which the proliferation of internet and volume of digital transactions correlate with the evolution of national cyber security regulations. In general the aggregate agreement on the eleven issues raised around this objective was 65.4% and the aggregate disagreement was 30.2%% In particular, 37.8% of respondents strongly agreed on the eleven issues raised while 27.6%% agreed. Then 14.2% of respondents strongly disagreed while 16%% disagreed and as many as 4.4%% of respondents were neutral on issues raised, giving a total response rate of 100%.

Discussion of Findings

From the questionnaires that were administered, respondents view reveal that the proliferation of internet and volume of digital transactions does not correlate significantly with the evolution of national cyber security regulations. This is backed by a total high general agreement rate of (65.4%) as opposed to the general disagreement rate which stands at (30.2%) and 4.4% undecided of all the questions raised respectively.

The above findings can be confirmed by documentary evidence . for instance, A study by the World Bank examined the relationship between digital development and cybersecurity readiness in developing countries. The study found that while digital development (including internet penetration and digital transactions) is a necessary condition for cybersecurity readiness, it is not a sufficient one. The study highlighted that factors such as political stability, institutional capacity, and international cooperation play a more significant role in shaping cybersecurity regulations and their effectiveness World Bank. (2024:45-47).

Conclusion

The Cameroonian government has recognized the need to address the rapid expansion of internet access and the surge in digital transactions in the Buea municipality mirroring national trends which have created new vulnerabilities and risks.

The National Cyber-security Strategy, updated in 2024, outlines key priorities, including the protection of critical infrastructure, the fight against cybercrime, and the promotion of cybersecurity awareness. However, the implementation of these strategies faces several challenges, including limited resources, a shortage of skilled cyber-security professionals, and the need for greater public-private collaboration. The volume of digital transactions, including mobile money transfers, online banking, and e-commerce, has increased significantly in Buea, making the municipality a prime target for cyber-attacks. The correlation between the growth of digital transactions and the evolution of cybersecurity regulations is evident, with the government responding to the increased risks by enacting and updating relevant laws and policies. Therefore, the paper concludes that there is a clear correlation between the proliferation of the internet, the growth of digital transactions, and the evolution of national cybersecurity regulations in Cameroon, particularly in the Buea Municipality. The government's response, while present, requires further strengthening in terms of implementation, resource allocation, and public awareness campaigns to effectively mitigate cyber threats.

Recommendation

Digitalization of space regulations in Buea Municipality, Cameroon, offers significant opportunities for improved efficiency, transparency, and economic development. The following recommendations are based on a review of best practices in digital governance, relevant Cameroonian legal frameworks, and the respondents questionnaire view

Develop a Comprehensive Digital Strategy: The Buea Municipality should create a detailed digital strategy specifically for space regulation. This strategy should outline clear goals, objectives, and timelines for digitalization. It should also identify key stakeholders, including government agencies, private sector actors, and citizens. The strategy should align with national digital transformation initiatives and international best practices.

Establish a Centralized Digital Platform: Implement a centralized digital platform for all space-related regulatory processes. This platform should serve as a one-stop shop for applications, permits, inspections, and other relevant activities. The platform should be user-friendly, accessible, and secure, ensuring data privacy and integrity. Consider using open-source software to reduce costs and promote flexibility.

Digitize Land Records and Cadastral Data: Digitize all land records and cadastral data within the municipality. This includes creating a digital map of land parcels, ownership information, and zoning regulations. This will improve transparency, reduce land disputes, and facilitate efficient land administration. The digital system should be integrated with the centralized digital platform.

Implement Online Application and Permitting Systems: Introduce online application and permitting systems for all space-related activities, such as building permits, land use permits, and business licenses. This will streamline the application process, reduce processing times, and improve transparency. The system should provide real-time status updates and allow for online payment of fees.

References

1. Rebecca, B. (2001). "What Kind of Space is Cyberspace?" 5 Minerva - An Internet Journal of Philosophy 138-155.
2. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8.
3. Tuija, K. & Rauno, K. (2015). "Cyber World as a Social System" in Lehto & Neittaanmäki (eds.), Cyber Security: Analytics, Technology and Automation, Intelligent Systems, Control and Automation: Science and Engineering 31-43
4. Markovac, V. & Rogulja, N. (2009). Key ICT Competences of Kindergarten Teachers (Faculty of Education, University of Zagreb), 72-77.
5. Kirkorian, W., & Anderson, (2009). "Media and Young Children's Learning" 18 Future of Children, 39-61.
6. Plowman, M.P. & Stephen, (2008). "Just picking it up? Young Children Learning with Technology at Home" 38 Cambridge Journal of Education, 303-319.
7. Jitender, K. M. & Sanjaya, C., (2018). PolicyXZ. International Journal of Recent Scientific Research, 9 (12), 211-214.
8. Kling, R., McKim, G., & King, A, (2003). "A Bit more to it: Scholarly Communication Forums as Socio-technical Interaction Networks 54(1) Journal of the American Society for Information Science and Technology, 47-67.
9. Prasanna, K. (2014) "Information Technology: Roles, Advantages and Disadvantages" 4 (6) International Journal of Advanced Research in Computer Science and Software Engineering 120-124.
10. Jitender, K. M. (2018). cyber crimes- policy in India, International Research Journal of Human Resources and Social Sciences, 5, (4), 54-65.
11. Thakur, M. (2024). Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE), 4(1), 1-20.
12. Tagarev, T., &Stoianov, N. (2019). Digital Transformation, Cyber Security and Resilience. Information & Security: An International Journal, 43(1), 1-398.
13. Stewart, H. (2023). Digital transformation security challenges. Journal of Computer Information Systems, 63(4), 19-36.
14. Taherdoost, H., Madanchian, M., &Ebrahimi, M. (2021). Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges. Handbook of Research on Advancing Cybersecurity for Digital Transformation, 99-117.
15. Damaraju, A. (2024). Cloud Security Challenges and Solutions in the Era of Digital Transformation. International Journal of Advanced Engineering Technologies and Innovations, 1(3), 387-413.
16. Möller, D. P. (2023). Cybersecurity in digital transformation. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 1-70).

17. Spremić, M., &Šimunic, A. (2018, July). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.
18. Cotlier, M. 2001. The Electronic Catalog: The Payoff of Paid Search Listings. Catalog Age 18. Cotriss, D. 2002. Marketers Report High ROI With Paid Listings. BtoB87 (3):19–20.
19. Couclelis, H. 1996. Editorial: The Death of Distance. Environment and Planning B: Planning and Design 23:387–389.
20. Dodge, M., and R. Kitchin. 2004. Flying Through Code/space: The Real Virtuality of Air Travel. Environment and Planning A 36 (2):195–211.
21. Graham, S. 1998. The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology. Progress in Human Geography 22 (2):165–185.
22. Zook, M. 2000. The Economic Geography of Commercial Internet Content Production in the United States. Environment and Planning A 32:411–426
23. Zoto, E., Kowalski, S., Frantz, C., Lopez-Rojas, E. and Katt, B., 2018. A pilot study in cyber security education using cyberAIMs: a simulation-based experiment. IFIP Advances in Information and Communication Technology, pp.40-54.
24. Zhou, Y., Dong, F., Kong, D. and Liu, Y., 2019. Unfolding the convergence process of scientific knowledge for the early identification of emerging technologies. Technological Forecasting and Social Change, pp.205-220.
25. Zeng, J., Yang, L. and Ma, J., 2016. A System-Level Modeling and Design for Cyber Physical-Social Systems. ACM Transactions on Embedded Computing Systems, 15(2), pp.1-26.
26. Zamawe, F., 2015. The Implication of Using NVivo Software in Qualitative Data Analysis: Evidence-Based Reflections. Malawi Medical Journal, 27(1), p.13.
27. Yeh, R.-S., 1983. On Hofstede's treatment of Chinese and Japanese values, Asia Pacific Journal of Management, 6(1), 149–160.
28. Xu, Y. and Dai, L., 2019. Research on the Influence of Situational Teaching Mode on Online Learning Experience. Lecture Notes in Computer Science, pp.514-527.
29. Williams, C., 2007. Research Methods. Journal of Business and Economic Research, 5(3), pp.65-72.
30. Von Solms, R., and Van Niekerk, J., 2013. From Information Security To Cyber Security. Computers and Security, 38, 97–102.
31. Viberg, O. and Grönlund, Å., 2013. Cross-cultural analysis of users' attitudes toward the use of mobile devices in second and foreign language learning in higher education: a case from Sweden and China. Computers and Education, 69, pp.169-180.
32. Van Manen, M. and Adams, C., 2009. The phenomenology of space in writing online. Educational Philosophy and Theory, 41(1), pp.10-21.
33. Valdez, V. and Omerbašić, D., 2015. Multimodal self-authoring across bi/multilingual educator and student learning spaces. Bilingual Research Journal, 38(2), pp.228-247. Välimaa, J., 1998. Higher Education, 36(2), pp.119-138.
34. Tran, Y., Yonatany, M. and Mahnke, V., 2016. Crowdsourced translation for rapid internationalization in cyberspace: a learning perspective. International Business Review, 25(2), pp.484-494.

35. Tømte, C., Fossland, T., Aamodt, P. and Degn, L., 2019. Digitalisation in higher education: mapping institutional approaches for teaching and learning. Quality in Higher Education, 25(1), pp.98-114.
36. Teixeira, M., de Lima Júnior, J., de Farias Júnior, I., de Aquino, C. and Teixeira, M., 2017. Mobility, cyberspace culture, app and digital citizenship: a case study of "universidade conectada". Advances in Intelligent Systems and Computing, pp.503 510.
37. Talebian, S., Mohammadi, H. and Rezvanfar, A., 2014. Information and communication technology (ICT) in higher education: advantages, disadvantages, conveniences and limitations of applying e-learning to agricultural students in Iran. Procedia - Social and Behavioural Sciences, pp.300-305.
38. Sun, P., Ku, C. and Shih, D., 2015. An implementation framework for E-Government 2.0. Telematics and Informatics, 32(3), pp.504-520.
39. Street, B., 2003. What's "new" in New Literacy Studies? Critical approaches to literacy in theory and practice. Current Issues in Comparative Education, 5(2), 77-91.
40. Soreide, G., 2006. Narrative construction of teacher identity: positioning and negotiation. Teachers and Teaching, 12(5), pp.527-547.
41. Skakni, I., Calatrava Moreno, M., Seuba, M. and McAlpine, L., 2019. Hanging tough: post PhD researchers dealing with career uncertainty. Higher Education Research & Development, 38(7), pp.189-103.
42. Silahtaroğlu, G. and Alayoglu, N., 2016. Using or not using business intelligence and big data for strategic management: an empirical study based on interviews with executives in various sectors. Procedia - Social and Behavioural Sciences, 235, pp.208-215.
43. Signorini, P., R. Wiesemes, and R. Murphy., 2009. Developing alternative frameworks for exploring intercultural learning: A critique of Hofstede's cultural difference model. Teaching in Higher Education, 14(3), 253–264
44. Siegel, A.F., 2012. Time Series. Practical Business Statistics, pp.429–464.
45. Schlienger, T., and Teufel, S., 2003. Information security culture: From analysis to change. South African Computer Journal, 31, 46–52.
46. Schein, E. (1984). Culture as an environmental context for careers. Journal of Organisational Behaviour, 5(1), pp.71-81.
47. Savrul, M., Incekara, A. and Sener, S., 2014. The potential of e-commerce for SMEs in a globalizing business environment. Procedia - Social and Behavioural Sciences, 150, pp.35-45.
48. Safa, N., Maple, C., Watson, T. and Von Solms, R., 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications, 40, pp.247-257.
49. Rowland. J., Rice, M. and and Shenoi, S., 2014. The Anatomy of a Cyber Power. International Journal of Critical Infrastructure Protection, Vol. 7, No. 2, pp. 3-11.
50. Reynolds, C., 2002. Changing gender scripts and moral dilemmas for women and men in education, 1940–1970. In C. Reynolds (Ed.), Women and school leadership (pp.29 48).
51. Reamer, F., 2013. Social Work in a Digital Age: Ethical and Risk Management Challenges. Social Work, 58(2), pp.163-172.