Data Protection Laws and Business Privacy in Cameroon: The Politics and Rhetorics of Implementation

TANYI George ORANG

L.L.M in Business Law, University of Yaounde II, Cameroon.

M.A in Governance and Regional Integration, Pan African University (PAUGHSS), Cameroon.

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90300212

Received: 28 February 2025; Accepted: 07 March 2025; Published: 08 April 2025

ABSTRACT

In the world at large and in every aspect of human activity, data protection and business privacy have long been a difficult and contentious issue. In the present context of globalization, advanced information technology, and e-commerce, the phenomenon of business data protection following the principle of confidentiality has been a very determinant factor for success or failure in the business world. In many countries, especially in the industrialized world, there are strong legal dispositions coupled with technical mechanisms to safeguard an enterprise information system; protect individual, collective, and institutional data. However, in Cameroon, in the absence of a specific text, legal provisions relating to business data protection and corporate privacy can be gleaned from the constitution and other disparate pieces of legislation. This article therefore aims at analyzing the extent to which business data protection and confidentiality are guaranteed in the Cameroonian positive law and the legal intricacies involved in this process. In other words, the study explores the challenges underpinning the effective implementation of laws pertaining to business data protection and privacy in Cameroon. This research is based on the premise that data protection in Cameroon, especially in business institutions, is facing a serious challenge in spite of the existing legal instruments relating to data confidentiality. The act of releasing sensitive information without permission and cybercrimes directed towards the data of these institutions has put business institutions in Cameroon in very embarrassing situations with their customers. During this research which entailed data from primary and secondary sources, it was discovered that, the primary *raison d'etre* for the inadequate or insufficient protection of business data in Cameroon, is due to the lack of suitable business data protection laws in the state. In this respect, it is imperative for the state of Cameroon to legislate laws that satisfactorily guarantee or safeguard the protection of private and institutional business transaction data.

Keywords: Law; Data, Data protection, Business privacy, Information Technology, e-commerce, Cybercrime, Globalization, Cameroon.

INTRODUCTION

The wide use of computer systems and digital networks in Cameroon for both social and economic activities and the ubiquitous nature of the Internet now present new challenges to business organizations, most especially in the sphere of business data protection and corporate privacy. The use of these technologies requires the collection, processing and storage of a wide range of customers' data. Thus Some websites, commercial companies, public entities, health care establishments, banks, and their affiliates, often hold valuable information or price sensitive information in digital forms, on their customers. Protecting such data has grown to be a top regulatory and legislative priority in Cameroon.

Data, is such an expansive, intricate and buzzword that is being used under all conceivable circumstances. Because of its vastness, there are diverse takes on what data is. Semantically speaking, "data is money"[3],

which can be processed and stored electronically. In the most basic sense, data denotes *'Information' i.e.* any information whether on paper or in electronic form, including electronic files no matter the format, database data, text, images, audios, videos etc. Legally speaking, data, on the strength of the Cameroonian cyber security legislation denotes the representation of facts, information, or concepts in a form appropriate for processing by terminal equipment, including a program that allows it to execute a function[4]. In a more technical sense, data denotes raw facts, figures, numbers, such as orders and payments, which are transformed into information. For the purpose of this study, business data shall mean commercially sensitive information that is related to a company, its operations and customers. Such information is sensitive in that if misused or disclosed may cause irreparable damage to the business and its clients and includes inter alia; intellectual property data (trade secrets, trademarks etc.); customers records; banking details (financial information); healthcare information; price sensitive information (inside information in financial markets that must be protected to maintain fair trading practices) etc.

Data Protection denotes the various procedures that ensure that information is secure and available only to authorized users. This includes laws designed to protect data from abuse, compromise or loss. In modern societies, these laws are critical in that they restrict, control and shape the activity of businesses; secure rights and fundamental freedoms of data subjects particularly the right to privacy[5]. On the other hand, business privacy, although often used interchangeably with data protection, are different but intrinsically linked. For the purpose of this research, business privacy means confidentiality i.e. the practice of keeping customers' data in a safe and secured way, in compliant with regulations and preventing it from unauthorized intrusion or interference by third parties. This is crucial to build confidence and maximize profit for an organization pursuing strategic opportunities such as cultivating partnerships or other commercial relations, identifying new markets for products or services in order to drive growth and profitability. Business privacy frameworks therefore ensures that a data subject determine which information is to be shared with whom and for what purpose.

Data protection and business privacy phenomena have always been a thorny and controversial issue in the world at large and in all the domains of human existence. In the present context of globalization, advanced information technology, and e-commerce, the phenomenon of business data protection following the principle of confidentiality has been a very determinant factor for success or failure in the business world[6]. Data protection has become increasingly relevant as the internet has revolutionized the traditional ways of doing business in the contemporary world. Prior to the advent of computer systems and digital networks, both public and private enterprises, businesses, corporate entities kept much of their confidential information in physical forms such as in documents filed in cabinets. It was during this period that business organizations and government institutions had to concern themselves primarily with physical security and internal classification schemes to guarantee data confidentiality. However, today, data security has grown critical as business organizations, government institutions, and people continue to rely primarily on digital platforms for the processing, storing, and transmission of sensitive data. Thus, applying strong legal dispositions and safeguards that satisfactorily guarantee data security and confidentiality in economic activities becomes imperative.

In a world marked by the globalization of risks, cybercrime and threats to cyber security, legal protection to shield business institutions from privacy infringements and harm associated with data breach cannot be overemphasized. While in advanced countries and industrialized nations like in Europe there exist strong legal dispositions to protect individual, collective, and institutional data, in underdeveloped societies and some emerging nations like Cameroon; the idea of data protection and business privacy remains a challenging venture since these societies in most cases do not have convincing legal texts to protect the data of business institutions and their affiliates. The effects are; the loss of customers' confidence and the discrediting of the business institutions which comes along with financial backlashes.

Irrespective of this legal gap, data protection and business privacy remains a major concern in Cameroon especially as the country is in the nascent stage of its digital transformation drive. Moreover, the widespread use of internet technology in Cameroon has resulted in a rise in security risks and computer crimes including hacking, scamming, phishing, pharming, DOS attacks which among others, target the information systems or

data base of business institutions. In fact, according to ANTIC (the National Agency for Information and Communication Technologies), a body which fronts Cameroon's ICT development initiatives and information systems security audits, there are several vulnerabilities in the systems of many institutions in the country which make it easier for online fraudsters to either steal or tamper with their data. This security gap caused a financial loss of approximately 4 billion FCFA to companies in Cameroon due to malicious intrusions in their systems (ANTIC, 2020). Armed with the above such challenges, the government promulgated the cyber security legislation[7] to guarantee an inclusive, sound and safe digital ecosystem in Cameroon. In the same light, in an effort to guarantee the protection of personal data, ensure the ethical use of computer systems and digital networks, the government has recently promulgated the law on personal data protection[8].

Despite these legal instruments for routine governance within the framework of cyber security and personal data protection, institutions in Cameroon are still grappling or better still tussling with serious security gaps most especially as the country is struggling to adapt to innovative information technologies and the rapid evolution of cybercrime in the network space. Consequently, privacy; customers and business transaction data are still persistently violated. In the last few years for instance, several businesses and government institutions have faced challenges related to data breaches and privacy violations even though specific instances involving such breaches are not extensively documented. In September 2024 for example, the National Social Insurance Fund (NSIF/CNPS) faced a data breach incident that was attributed to the hacking group *SpaceBears*. Despite evidence confirming the attack, CNPS initially denied the breach, leading to public criticism regarding their transparency and data protection measures[9]. This breach exposed sensitive employee information, underscoring the vulnerabilities within the public institution, particularly regarding outdated systems and insufficient cybersecurity measures.

Similarly, consumers of electronic services (like the mobile money, orange money services etc.) in Cameroon constantly face serious data breach and privacy violations most especially as cybercrime and security threats like scamming, hacking, phishing etc. have become rampant in the country. In 2016, MTN Cameroon, which is one of the chief electronic service providers in the country, faced allegations of privacy violations when customers received unsolicited messages related to internet usage. The company however refuted these claims, stating that there was no infringement on customer privacy or rights.[10] MTN Cameroon further defended itself after a report suggested that messages it sent to subscribers "violate customer privacy" and were intended to "curtail customer rights". MTN's statement confirmed that messages intended for the "general public" were distributed by the company, alongside other providers in the country, on the request of the country's Ministry of Posts and Telecommunications, that further released a statement confirming it had used the country's mobile operators to distribute messages on the responsible use of social media and warn against spreading "false news". These forgoing incidents therefore highlight the need for robust data protection strategies and comprehensive cybersecurity policies among Cameroonian businesses and institutions.

It may be worthy to also highlight that Courts in Cameroon have been remarkably coy/shy in adjudicating on matters pertaining to data breach and privacy violation as fewer litigations in this area exist. Despite the relative dearth of judicial decisions however, infringement of image rights has led to *Yomba Madeleine v. Les Brasseries du Cameroun*[11] and *Mrs. Mfopa Mama, born Ntouo Sabiatou, vs. Société NESTLE Cameroun S.A. and Société Océan Central Africa SA.* Both cases involved the unlawful use of an individual's photo (PII) for advertising purposes without their consent, resulting in a violation of their image rights. In the same manner, in *Mrs. Mbock Frankline Junior v. Les Films Terre Africaine and Les Brasseries du Cameroun,*[12] a contract for the use of an individual's image within a two-year period was violated when the commercial spot broadcasted beyond the stipulated term. That was a breach of the individual's image rights (personal data). The final judgment of the high court ruled that mere evidence of an invasion of one's privacy is sufficient to warrant compensation, and that there is no need to establish that the claimant suffered damage.[13]

Increase data breach and privacy violation in business sectors in Cameroon indicate several pitfalls among which is the lack of unified strategies amongst institutions to address cyber threats. This gap potentially exposes them, leaving them susceptible to data breaches and privacy violations. In the context of globalization and advanced information technology, this article explores some regulatory and technological loopholes that

undermine or hinder the enforcement of laws relating to business data protection and company privacy in Cameroon. Mindful of these challenges, it can be said that the country is in dire need of innovative criminal policy strategies that embody societal and technical responses to create a credible legal climate for cyber security and data protection. This is very important because computer systems and digital networks have now become potential targets of cyber-attacks, compromising the capacity to process, safeguard, and communicate informational capital, virtual resources, intangible values and symbols across the web. Therefore, the stakes and challenges inherent in the effective control of technological risks are extremely high[14], and have to be addressed while respecting the fundamental rights and freedoms of persons. These challenges may be loosely classified as follows:

The Absence of a Settled Normative Standard on Privacy and Business Data Protection in Cameroon

A successful data protection and business privacy regime is predicted first on a well-articulated legal foundation and structure for any form of data governance. Yet, it will be an open secret to state that despite the country's legislative efforts to protect the cyber space and personal data, Cameroon still lacks a comprehensive text that satisfactorily guarantee the protection of private/institutional business transaction data. Undoubtedly, the digital age has come with invaluable benefits for both businesses and individuals and with the increase collection, processing and storage of a wide range of customers' sensitive data, data protection and business privacy concerns have now become a priority[15]. In addition, much like the natural environment is facing a climate change, the online environment is now facing a climate change as well and the resulting fragile environment needs to be actively regulated[16]. Thus, the importance of a well-articulated legal regime for business data protection cannot be overemphasized. However, Cameroon still appears reluctant in formulating a comprehensive normative standard dedicated to business data protection and corporate privacy[17]. The absence of such a norm is arguably the chief reason for the low level compliance with privacy and data protection obligations by data administrators[18].

Aside just posing serious challenges to the understanding of the basic rights and responsibilities of data owners and administrators operating within the nation's economic space, the forgoing legal deficiency arguably spells doom in balancing the gains and threats of data processing and the shielding of data subjects from negative effects resulting from a data breach, which in all, are the basic tasks of a comprehensive data protection law[19].

In advanced economies, data protection and business privacy laws define and safeguard data subjects' rights[20], by defining penalties in the event of breach which is crucial to promote trust in digital interactions, and upholding of the basic rights and freedoms of persons in an increasingly data-driven world. Furthermore, data protection and business privacy legislations prohibit data breaches, and hold businesses accountable for data misuse, destruction or compromise by articulating on data processing, sharing, storing and confidentiality. Such texts also regulate promises advertised in Privacy Policies which consumers usually agree before conducting online transactions. To reach these benchmarks, data protection laws are in place all over the world and prohibit companies and individuals from disclosing or granting access to sensitive data by outlawing specific forms of data collection; penalize offenders in an effort to bring justice to victims of data misuse; and deter other parties from engaging in data theft; restrict companies' ability to share information collected legally from consumers for transactional or informational purposes.

In the USA for instance, consumer financial service providers such as banks, investment brokers, lenders etc. are required by the Gramm-Leach-Bliley Act (GLBA) of 1999, which was designed to protect consumer financial privacy, to disclose the use and sharing of personal identifiable information (PII) they obtain from individuals and to provide consumers with the opportunity to opt-out of data collection. The GLBA reduces the risk of data breaches by granting consumers greater control over the data they provide to financial institutions. Additionally, the 1914 Federal Trade Commission Act gives the federal trade commission the authority to take legal actions against businesses that violate privacy policies in order to protect consumer data privacy. This is far from what obtains in Cameroon. The relative absence of such robust texts in Cameroon

represents a potential danger to the keeping of customers' (financial/business) information, talk-less of the difficulties tied to implementing ambiguous legal regimes on business privacy.

Low Adherence to Suitable Mechanisms that Ensure Compliance with Data Protection and Business Privacy Regulations

Because Cameroon's government, corporations, businesses, and their affiliates lack appropriate safeguards, procedures, and yardsticks that aims to ensure adherence to business privacy requirements, inadequate enforcement of data protection and corporate privacy laws continues to be a growing concern. Legal instruments pertaining to business privacy and data protection in Cameroon are not sufficiently backed or supported with suitable enforcement strategies and implementation processes in order to remain pertinent.

It must be recall that business data is now a commodity. Thus, safeguarding an enterprise database and the privacy of customers is a pressing concern most especially as the digital age has brought unprecedented connectivity and convenience and has also heightened the risks associated with unauthorized access and misuse of sensitive information[21]. As the linkage of information across databases intensifies, privacy and data protection concerns, legal frameworks, coupled with technological measures can mitigate risks associated with data breach by stipulating the purpose of data retention. Mindful of the risks posed by cyber criminals, the Government and corporate entities must proactively adopt and implement best practices and safeguards to protect data from unauthorized access. This entails crafting strong policies, putting safeguards in place, and making sure that compliance is maintained in order to promote trust with both customers and regulatory bodies.

Business Privacy and data protection have become pivotal issues in the business world and both relates to the right to prevent the dissemination of sensitive or confidential information. Thus, aside protective regulations that set the legal principles and requirements that must be met by data-driven entities[22]; technical mechanisms such as privacy-enhancing technologies (PETs) like encryption have become widely used. These PETs are key in every data governance strategy and must be rooted to form the basis or the foundation of any data governance plan to be applied in Cameroon[23].

On the other hand, the measure of accountability has recently gained popularity and has become fashionable in relation to business privacy. It is a fundamental tenet of data privacy laws and is mentioned, if not explicitly, in all initiatives to hold businesses more accountable for the way they handle data. It is a distinct policy approach to the vexing problem of 'data export' or 'transborder data flow'[24], requiring that some authority account for one's actions. It implies a process of transparent interaction, in which that body seeks answers and possible rectifications. The involvement of an external body is therefore indispensable.

Cameroon's complex legal environment for corporate privacy and data protection necessitates the coupling of even more advanced technological tools to safeguard an enterprise information system from malicious intrusion. This measure which must be implemented through well-defined administrative and technical procedures may include inter alia: *Strong access controls* (to limit access to data using the least privilege principle); *frequent audits* (to find vulnerabilities and make sure data protection measures are consistently applied); *data encryption* (a technique that guarantees that, in the event of unauthorized access, the data remains unintelligible without the proper decryption key); *secure data transmission* (which entails using secure channels for data transmission, especially when communicating sensitive information externally). Also, regular security updates which involves maintaining software, systems, and security measures up to date with the most recent patches and updates helps to prevent interception and unauthorized access during data transfer. Data backup, Data masking, Anonymization, and other measures also lower the risk of exploitation by guaranteeing that vulnerabilities are quickly fixed.

Also, data protection impact assessment (DPIA) will ensure conformity with regulations in force and operationalizes established requirements ensuring appropriate attention to fundamental rights such as the right to privacy[25]. Another potential remedy for privacy and data security issues may be privacy impact assessment, or PIA. This measure is designed to aid organizations enforce privacy by incorporating privacy considerations into their activities and projects from the early stages, thus reducing the risk of privacy

violations and any associated regulatory action or reputational damage. The whole PIA strategy involves assessing the possible privacy implications of new use of data[26].

In addition to the above precautionary measures, adherence to data privacy legislation also requires: understanding the law (i.e. knowing the specific regulation that apply to a particular business is essential); creating a data inventory (to help identify the type of data collected, processed, and stored); developing policies and procedures on regulatory compliance; training employees on data governance; implementing technical and organizational measures such as designating a DPO (Data Protection Officer) to oversee compliance with data privacy regulations; appointing an organizational ombudsman/Data Protection Ombudsman to relay/mediate/channel customers complaints to data Administrator. All these measures are crucial to help navigate the complex landscape of data security in Cameroon, identify potential vulnerabilities, and develop a customized approach to ensure adherence to privacy policies. Because creating a data privacy program that is both safe and effective necessitates a thorough and planned approach, governments and business organizations must therefore deploy appropriate technical and operational security measures to protect data from unauthorized access, disclosure, or alteration. Establishing procedures to handle data subject rights, such as access, rectification, and deletion, is crucial. A well articulated data breach response plan to detect, investigate, and notify individuals and authorities during a breach is also necessary.

The Challenge Posed by the Evolving Foundation upon Which the Economy Operates

The process of economic evolution from agriculture to manufacturing to services is nearing its end and another major evolution along a different dimension is now underway[27]. A fundamental change in the business and technological environment is taking place[28], driven by developments such as the increased globalization of the world economy; the growing economic importance of data processing; the prevalence of data transfers via the internet; the increased direct participation of people in cross-border data flows, the evolving significance of geography, and the escalating threats to privacy.

With the advent of leading edge technologies and IT-induced business processes, data is now a new critical resource[29] and much concern has been expressed in recent times to ensure that information technology considerations are firmly aligned with business imperatives and regulations[30]. With the rapid technology developments and the advent of internet based commerce (e-commerce), nations across the world are forced to enact legislations to protect the information privacy of individuals and corporations[31]. In terms of international data transfer, transborder data flow is now recognized to have a major influence on multinational and transnational corporations because data collection and processing are at the core of these corporations and rapidly growing business models, underpinning the activities of technology companies and acting as a source of market power[32].

Emerging technologies and IT-induced businesses are constantly reshaping the business world. This transformation has significant implications for data privacy laws in Cameroon as regulators strive to keep pace with the changing basis of the operation of the economy; advancements in artificial intelligence, blockchain technology, Internet of Things (IoT), and big data analytics. Understanding the intersection between technology and privacy is therefore crucial in safeguarding data in an increasingly interconnected world. The intersection is however a critical and complex issue that has become increasingly relevant in today's digital age. As emerging technologies develop and become more ingrained or integrated into social and economic activities, the amount of data being collected and processed has also increased. All these poses challenges in relation to data privacy, security, and ethical considerations. Thus, in order to remain relevant, regulations must be flexible to match the new digital environment enabled by the rapid advancement in technology. Otherwise, the market would become chaotic. Maintaining this speed poses a number of difficulties, particularly where new business models in particular seem to indicate where the law should go.

The Lack of Desire to Alter the Status Quo

Although the government of Cameroon has professed its intention to protect the cyber space; protect personal data; and support IT-induced businesses through policy frameworks and have promulgated some regulations

in relation to the above areas, the country is still lagging in some specific regulations that satisfactorily protect both private and institutional business transaction data. Even with the available pieces of legislations for routine governance in the aforementioned fields, their implementation is not sufficiently backed with a commensurate political will and commitment. Government departments and business organizations are constantly struggling to withstand the challenge of recurrent data breaches. All these new challenges may be linked to over reliance on outdated internet technologies to conduct economic activities.

So far, business data protection and corporate privacy in Cameroon has received limited regulatory attention. While in advanced economies and industrialized nations like in Europe, there exist strong legal dispositions and robust institutions with strengthened capacities to safeguard an enterprise information system, in Cameroon; the idea remains a challenging venture since the country lack convincing legal instruments and capacity institutions to protect the data of business institutions. In addition, collaboration and concerted efforts among stakeholders to combat cybercrimes is achieving no results. Also, the absence of Mutual Legal Assistance Treaties (MLAT) to enhance some form of judicial cooperation in the fight against cybercrime is gradually spelling doom to cybercrime investigations. This technic which involves an agreement between two or more nations to collect and share information in an effort to enforce criminal or public laws when a suspect in a criminal case lives abroad can be a potential remedy to the vexing problem of online crimes investigation. MLA request is frequently used to conduct a formal interrogation in criminal proceedings. Moreover, a highly centralized system of government is in charge of enforcing laws that aim to control cybercrimes, while the law enforcement community is less familiar with methods for detecting cybercrimes and obtaining digital evidence.[33] These are no small challenges that must be addressed in order to give meaning to any data governance strategy to be adopted.

The Challenge Posed by Globalization on the Law Making and Enforcement

In its highly complex, intricate and evolving nature, globalization which has now become an overarching international phenomenon denotes in the most basic sense: political; economic; financial; communication; and trade integration most especially, the development of an increasingly linked global economy typified mainly by free trade, free flow of capital, and the exploitation of cheaper foreign labor markets. Through intensification of links; the stretching of economies and the interdependency of global and local landscapes all driven by IT-tools, globalization has led to interconnected world economies, politics, people, products, services, capital, technologies, and socio-cultural practices.

Globalization generally presents a number of stumbling blocks to law making and enforcement. Aside altering traditional modes of life to impose a universal system now coined by experts as *Americanization or Europeanization of culture*, the phenomenon has greatly affected the regulation of services and law enforcement most especially through the disappearance of geographical boundaries. In fact, to Cheka, C. (2018)[34], globalization has brought serious challenges to the implementation of laws generally speaking. In relation to financial service regulation, the author demonstrates that globalization has significantly impacted law enforcement and financial regulators and because of its seemingly legal aspect of commerce, globalization has transformed the global financial system into a refuge for money launderers. It offers a network through which billions of dollars are extracted annually from economies across the globe, expanding the scope of organized crime and strengthening terrorism.

Today, crime, technology development, income distribution, identity etc. are described as phenomena affected by globalization[35]. Thus, criminal law, trade law, and international law making have all grown to be universal phenomena[36]. In fact, everything is now affected by globalization, including the criminal justice system, trial procedures, standard for proving claims, criminal policy, and the process of committing a crime[37]. Cybercrimes today are a result of globalization. Hacking, Identity fraud, and piracy are among the classic crimes that may be committed in new ways by means of computers and the Internet. Additionally, it is now feasible for thieves to anonymously carry out brand-new, destructive crimes like online scamming, hacking from anywhere around the world[38]. Furthermore, borders have been removed and the world is now a global village which has given criminals more opportunities in lucrative sectors like organized crime and

economic crimes. The development of communication networks has also simplified the process of transferring large sums of money at once. With globalization, perpetrators of cybercrimes will no longer be the subject of legal or police inquiries as a result[39].

Additionally, with regards to the determination of jurisdiction, globalization has completely altered the fundamental principle of territoriality (or territorial sovereignty) which is one among other cardinal principles that guide the scope of application of the law. It must be recall that, in statehood, sovereignty is sacrosanct, cardinal and crucial and the key idea behind the notion of territorial jurisdiction is that laws apply only on acts that occurred within a nation's borders and are therefore enforceable against all violators. However, with the disappearance of borders and the creation of virtual space (computer simulated environments) this principle is far from being a guest in any law enforcement debates. Nevertheless, nations across the world are actively attempting to protect their sovereignty and continuously claim that their legal system is the most suitable and efficient. Thus, no nation desires to lose its sovereignty because of globalization. This jurisdictional challenge coupled with the ever growing difficulty to capture cyber criminals and sometimes impossible to detect crimes in the cyberspace makes the enactment of laws a nightmare to regulators, talk-less of enforcement.

The Challenge of States Huge Grip on the Traditional View of Sovereignty

Traditionally speaking, sovereignty denotes hierarchy within a state as well as external autonomy for states. Hierarchy within the state entails supreme and absolute authority or power to make laws and govern without interference while external autonomy on the flipside denotes the power of a state to act independently of other states in their relation with one another. In contrast to these views, the notion of 'new sovereignty' states differently. The concept of new sovereignty centers on a state's reliance on cooperation and collaboration within the international community. To Richard Haass (2013), States should cede some sovereignty to international organizations in the era of globalization in order to safeguard their own interests. This position of ceding sovereignty whether in part or in whole to a supranational institution is still far from being a reality despite growing assertions that globalization and its challenges on law enforcement have become overarching international phenomena requiring some pragmatic international cooperation especially in combating cybercrimes and security threats in the global network space.

The ever-increasing data breaches and privacy violations worldwide due to evolving technology and new lifestyles linked to an intensified online presence requires novel trans-boundary measures such as inter-state cooperation as such violations have now become a global concern. Historically, states have been remarkably coy and unwilling to genuinely cede or surrender part of their legal autonomy to a supranational organ and continuously demonstrate a firm unwillingness to allow investigations or other forms of judicial interference in their domestic legal system by other states. In Africa for instance, despite the African union's effort to protect the cyber space through its cyber security legislation, some states still take their sovereign rights very seriously while others do not. While the latter are focused on a novel definition of sovereignty, the former adhere to the conventional understanding of sovereignty. The conventional perception of sovereignty requires that a state alone is responsible for formulating and enforcing international law. It is the state's highest degree of authority, and no other state is permitted to meddle with how the state administers its citizens[40]. States are deterred from engaging in international cooperation by this notion. The state believes that another state is endangering its sovereignty in this situation.

As already mentioned above, sovereignty in statehood remains sacrosanct and its traditional view today is a potential pitfall to the international enforcement of criminal law[41]. To quote Spies, A. (2011) in this regard, "*the efficacy of interstate cooperation can be impacted by a state's conception of sovereignty"*[42]. Nation states' attitudes towards interstate cooperation can be influenced by their interpretations of sovereignty. In contrast, nation states actively engaged in international cooperation in law enforcement problems are those who are concerned about the new sovereignty. The state is thought to play a part in a network of nations that work in synergy to address regional and global issues[43]. In fact, pursuing international collaboration is a sign of contemporary states viewing sovereignty as a mechanism of assisting one another.

The Problem Posed by the Ongoing Emergence of New Business Models

The rise of new business models is not just an economic shift but a revolution that is radically altering the legal landscape. To Vives, L. (2023), the rapid expansion of transformative business models opens the door for entrepreneurship and social advancement while drastically changing the structure of industries and sectors. [44] Some of these new IT-induced business models represent a more comprehensive shift, changing industries, causing organizational change, and having a significant impact on society. They also continuously influence the direction of the law and in effect, pre-existing legal frameworks become outdated.

Traditional commerce has changed as a result of the growth of e-commerce, exposing customers to higher risks and providing them with little leverage in negotiations for their rights[45]. The internet itself has facilitated a new wave of economic growth and development in which Businesses across the world - both big and small - have taken advantage of the scale, scope, and access that the Internet provides to reach new markets and consumers[46]. These businesses now carry out data-driven transactions which were not possible before the advent of electronic commerce (e-commerce). Moreover, a trade regime that was established to allow only the biggest multinational corporations to actually participate in international trade needs to be reevaluated in light of this kind of transaction. There have been many new laws and regulations across countries as a result of the massive growth of e-commerce, particularly the use of the internet as a transnational and instantaneous medium for business transactions. There has also unavoidably been a minefield of associated uncertainties and potential hazards.[47] For laws to remain relevant therefore, they must be revised frequently to reflect the swift changes in new business models and ICT-driven business environments.

In clarifying the impact of new business models on the regulation of financial services, Cheka, C. (2018) postulates that banks have historically been in the business of managing money because, as credit establishments, banks have historically kept money on servers and registered cards and have generally had restrictions on their ability to oversee and control the issuing of electronic money by a third party whose primary activity is electronic mobile communication[48]. However, in their business of mobile transmission of oral and printed data, mobile telephone operators (MTOs) promote the flow of data (and, in semantics, money is data). Banking practices have changed, making them unusual for the latter. In Cameroon, numerous money transfer conflicts are currently raging between Orange and Mobile Telephone Network (MTN) and microfinance companies like Express Union and Express Exchange over electronic money transfer operations. This is a result of the fact that mobile phone operators (MTOs) originally remained out of the money transfer or mobile money industry, and microfinance institutions relied on MTO bandwidth to conduct these activities. This recent entry of MTOs in to the business of managing money requires new and comprehensive legal frameworks to protect e-commerce consumers.

Law Enforcement/Security/Intelligence Agencies Gap

“Information security is about crime”[49]. Hence, the importance of robust security agencies cannot be overstated. However, Cameroon continues to struggle with empowering law enforcement agencies that are responsible for business privacy and data protection. Agencies like ANTIC (NAICT), a body which fronts the Cameroon ICT development and information system security audit, are finding it difficult to investigate cybercrimes due to the nation's reliance on outdated technologies and inadequate network infrastructure. To combat the swift rise in cybercrimes and network security threats, law enforcement agencies' ICT infrastructure needs to be significantly improved.

Because information security requires not just ICT tools but ICT intelligence, it becomes imperative for the Government to invest/allocate resources in the training of online/forensic investigators with sound knowledge in cybercrime investigation; equip them with high-speed digital tools and sophisticated technologies to enable them perform effectively.

In addition, safeguarding an enterprise information system requires the identification of possible security threats, obstacles to business continuity and suitable measures that would contribute to the effective

enforcement of the rules. These maybe achieved through robust monitoring and evaluation systems in place. As such, investing in the construction and rehabilitation of capacity institutions to monitor the implementation of privacy regulations becomes crucial. This metric will aid in offering a comprehensive evaluation of the advancements made in the direction of a secure and welcoming cyber environment.

Additionally, the newly established role of the corporate data protection officer (DPO), which is empowered to guarantee that the organization complies with all aspects of the new data protection regime under the EU-GDPR, is not yet operational in Cameroon as most data-driven organizations have not yet taken the DPO position into consideration. In this era where data protection and business privacy constitute an emergency and an essential prerequisite for success in the business world, the appointment of an impartial third party (Data Protection Officer/Ombudsman) becomes imperative. The DPO ensures the organization complies with data protection laws; advise senior managers on data processing decision-making and report directly to the top management level; ensures that the organization is aware of, and trained on, all relevant data protection obligations; makes sure that appropriate measures/procedures are followed for subject access requests, privacy impact assessment, and educating staff members about data protection. Also, the DPO performs audits, proactively addresses potential issues, and acts as the public's point of contact for all matters pertaining to data privacy.

Cameroon’s Government Policies Lack Direction

The business data management ecosystem is extensive and spans all economic sectors. In this respect, laws must therefore be designed or tailored to encompass the specific industries concern, including: financial markets *(stock exchange markets, insurance markets, money markets, Forex markets, cryptocurrency markets, commodity markets etc.);* banks; healthcare/pharmaceutical industries etc. This is necessary to comprehend the text's finality and scope as well as how it is being implemented. Although the Cameroonian Government has developed some security and ICT policies for effective data management, implementation remains a major challenge, raising important questions: Paper policies? clearer policy direction is require. And how realistic are such policies? How much has been invested in terms of time, education, personnel, etc.? All these questions raise concerning issues that must be considered in staging effective security against data protection and business privacy menace.

Neighboring Countries Lack Cyber Legislation

One of the transnational legal challenges that should be taken into consideration given the global nature of cybercrime is the fact that countries like Chad, the Central African Republic, and Equatorial Guinea lack comprehensive cyber laws. These countries may be acting (either intentionally or unintentionally) as safe havens for cybercriminals who feel secure enough to commit cybernetic crimes in the cocoon of online anonymity. Additionally, nation-states' increasing hesitance to enact comprehensive cyber laws hinders the signing of judicial cooperation agreements, making it challenging or impossible to work together effectively at the regional, continental, or international level to combat cybercrime and network security threats. It must be recall that the stakes involved in effectively controlling technological risks are extremely high and must be addressed globally while respecting the basic rights of persons.[50] With the globalization of cybercrime, mutual legal or judicial assistance through the harmonization of legal regimes of various states becomes an imperative tool to combat these crimes.

CONCLUSION

This article explores some legal and technical challenges around the effective implementation of laws pertaining to the protection of an enterprise information system in Cameroon. As information technology becomes more ingrained in both social and economic activities, business privacy frameworks and regulatory agencies that enforce them are essential mechanisms for governing data flows. Nonetheless, the implementation of data privacy regulations in Cameroon is facing several obstacles. The ICT revolution has altered and is reshaping the foundation of business operations, which is driving the creation of new businesses

and determining the boundaries of legal frameworks. Also, the lack of resources for monitoring and inspections by regulatory authorities; law enforcement and security gaps; low levels of security awareness through low demand for security education, represent major challenges to effective data protection and business privacy in Cameroon. All of these difficulties, along with the lack of a thorough normative standard on safeguarding commercially sensitive data, underscore the urgent need for improved resource distribution, user education, and more precise laws pertaining to business data security and corporate privacy in Cameroon.

CITED WORKS:

1. **Adebisi, L. (2021).** "Giving 'teeth' to the African union towards advancing compliance with data privacy norms." Information and communication technology, Law 30 (2),87-107
2. **Ahmadi, S. (2018).** "The effect of globalization on the national criminal law systems." University of Nebraska-Lincoln, Library Philosophy and Practice (e-journal) https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5960&context=libphilprac
3. **Akuta, E. et al (2011).** "Combating cybercrime in sub-Sahara Africa: A discourse on law, policy and practice." Journal of Peace, Gender and Development Studies, 1(4), pp. 129-137, Available at; interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al
4. **Asongwe, P. (2010).** "A model regulatory and legislative framework for Cameroon." Presentation to the 1st CTO Cybersecurity Conference, 16-18 June 2010, London.
5. **Asongwe, P. (2011):** "Cameroon's public administration since 1998: Tracking the opportunities and challenges of digital governance." Paper presented at the Fifth eGov Africa Forum, 26-28 April 2011, Yaounde.
6. **Asongwe, P. (2012).** "e-Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges." The African Journal of Information and Communication (AJIC), South Africa, (12). Doi: 10.23962/10539/19714.
7. **Barkatullah, H. (2018).** "Does self-regulation provide legal protection and security to e-commerce consumers?" Electronic commerce research and applications 30, 94-101
8. **Bennett, J. (2012).** "The Accountability approach to privacy and data protection: assumptions and caveats." Managing privacy through accountability, 33-48
9. **Bieker, F.; Friedewald, M. (2016).** "A process for data protection impact assessment under the European general data protection regulation". Privacy technology and policy: 4th annual privacy forum, APF.
10. **Bieron, B.; Ahmed, U. (2012).** "Regulating e-commerce through international policy: understanding the international trade law issues of e-commerce." Journal of world trade 46(3)
11. **Binns, R. (2017).** "Data protection Impact Assessment: a meta-regulatory approach." International data privacy law 7 (1), 22-35
12. **Chayes, A. et al (1995).** "The New Sovereignty: Compliance with International Regulatory Agreement." Cambridge, MA: Harvard University Press.
13. **Cheka, C. (2018).** "Challenges of Regulating Financial Service Provision in Cameroon in the Digital Age and a Globalised World." Africa Development, Volume XLIII, No. 2, 2018, pp. 85-106
14. **Cuijpers, C. and Purtova, N. (2014).** "Data protection reform and the internet: the draft data protection regulation." Research Handbook on EU internet law, 543-568
15. **Danezis, G. et al (2015).** "Privacy and data protection by design-from policy to engineering." Arxiv preprint 1501.03726
16. **Galliers, R. (1994).** "Information systems, operational research and business reengineering." International transactions in operational research 1(2), 159-167
17. **George, H. (2016).** "Criminological Theory." Wolters Kluwer.
18. **Guarda, P. and Zannone, N.(2009).** "Towards the development of privacy aware systems." Information and software technology 51 (2), 337-350
19. **Hert, D. and Papakonstantinou, V. (2016).** "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" Computer law & security review 32 (2), 179-194.
20. **Hondius, F. (1983).** "A decade of international data protection." Netherlands International Law Review, 30 (2), 103-128.

21. **Ikenwe, J.; Magnus, O. (2016).** "Information Security in the Digital Age: the case of developing countries." Chinese Librarianship: an international electronic journal, 42, available at: https://www.researchgate.net/publication/321767925_ Information_Security_in_the_Digital _Age_The_Case_of_ Developing_Countries , accessed, 23 July 2024
22. **Karmarkar, S.; Apte, M. (2007).** "Operations management in the information economy: information products, processes and chains." Journal of operations management 25(2), 438-453
23. **Keenan, J. (2006).** "The New Deterrence: Crime and Policy in the Age of Globalization." Iowa Law Review, Vol. 91, p. 505, Available at: http://hdl.handle.net/11212/1116
24. **Kerber, W. (2016).** "Digital markets, data, and privacy: competition law, consumer law and data protection." Journal of intellectual property law and practice, jpw150
25. **Kira, B. et al (2021).** "Regulating digital ecosystems: bridging the gap between competition policy and data protection." Industrial and corporate change 30 (5), 1337-1360
26. **Kuner, C. (2010).** "Data protection and international jurisdiction on the internet." International Journal of law and information technology, 18 (2), 176-193
27. **Kuner, C. (2010).** "Regulation of transborder data flows under data protection and privacy law: past, present and future." TILT Law and technology working paper
28. **Nadelmann, E. (1990).** "The role of the United States in the international enforcement of criminal law." Harvard International Law Journal 31.
29. **Romansky, R. (2022).** *Digital Age and Personal Data Protection*. Lap Lambert Academic Publishing, (124 p.). Monographic book, International Journal on Information Technologies & Security, № 3 (vol. 14), ISBN: 978-620-4-73564-1
30. **Rudraswamy, V.; Vance, D (2001**). "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment." Logistics information management 14 (1/2), 127-137
31. **Simonovic, I. (2000).** "State sovereignty and globalization: are some states more equal?" Georgia Journal of International and Comparative Law 28 (3): 384
32. **Spies, A. (2011).** "Global data protection: whose rules govern.", Sedona Conf. J. 12, 105
33. **Svantesson, B. (2021).** *Private international law and the internet*. Walters Kluve
34. **Vives, L. (2023):** "The emergence of new business models." Management research: the journal of the iberoamerican Academy of management, Vol. 9 N°3
35. **Walden, I.; Hornle, J. (2001).“**E-commerce law and practice in Europe." Elsevier, 2001

Notes:

36. **Mireille, D. (2003).** "Comparative Legal Studies and the Internationalization of Law." Liz Libbrecht, Available at: https://books.openedition.org/cdf/3878?lang=en
37. **Moukouri, D. (2022).** "Cameroon Data Protection Overview." Dataguidance, https://www.dataguidance.com/notes/cameroon-data-protection-overview
38. **Norton, N. (2023).** "Building a Safe and Effective Data Privacy Programme: A Comprehensive Guide." Available at at https://www.korumlegal.com/ blog/building-a-safe-and-effective-data-privacy-program-a-comprehensive-guide (Lastly visited on the 19th of February, 2025)
39. **Section 4 (41)** of Law N° 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality in Cameroon.
40. https://www.datagrail.io/blog/data-privacy/importance-of-data-privacy-laws-explained/ (Lastly visited on the 19th of February, 2025)
41. https://www.cameroon-concord.com/cameroon/cnps-data-breach-spacebears-hack-confirmed-government-in-denial?utm_source=chatgpt.com(lastly consulted on the 10th of March, 2025)
42. https://www.mobileworldlive.com/mtn/mtn-hits-back-at-cameroon-privacy-accusations/ (lastly consulted on the 10th of March, 2025)

FOOTNOTES

[1] L.L.M in Business Law, University of Yaounde II, Cameroon .

[2] M.A in Governance and Regional Integration, Pan African University (PAUGHSS), Cameroon.

[3] Cheka, C. (2018). "Challenges of Regulating Financial Service Provision in Cameroon in the Digital Age and a Globalised World." Africa Development, Volume XLIII, No. 2, 2018, pp. 85-106

[4] Section 4 (41) of Law N° 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality in Cameroon.

[5] Hondius, F. (1983). "A decade of international data protection." Netherlands International Law Review 30 (2), 103-128.

[6] Romansky, R. (2022). *Digital Age and Personal Data Protection*. Lap Lambert Academic Publishing, (124 p.). Monographic book, International Journal on Information Technologies & Security, № 3 (vol. 14), ISBN: 978-620-4-73564-1

[7] Law N° 2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality in Cameroon.

[8] Law N° 2024/017 of 23Dec 2024 relating to personal data protection in Cameroon.

[9] Available at https://www.cameroon-concord.com/cameroon/cnps-data-breach-spacebears-hack-confirmed-government-in-denial?utm_source=chatgpt.com (lastly consulted on the 10th of March, 2025)

[10] Available at https://www.mobileworldlive.com/mtn/mtn-hits-back-at-cameroon-privacy-accusations/ (lastly consulted on the 10th of March, 2025)

[11] YOMBA Madeleine v. Les Brasseries du Cameroun, YHC (1976) Jugement N° 61 du Mai 1976

[12]Mrs. MBOCK Frankline Junior v. Les Films TERRE AFRICAINE and Les Brasseries du Cameroun (unpublished)

[13] Ibid.

[14] Asongwe, P. (2012). "e-Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges." The African Journal of Information and Communication (AJIC), South Africa, (12). Doi: 10.23962/10539/19714.

[15] Hert, D. and Papakonstantinou, V. (2016). "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" Computer law & security review 32 (2), 179-194.

[16] Svantesson, B. (2021). Private international law and the internet. Walters Kluve

[17] Moukouri, D. (2022). "Cameroon Data Protection Overview." Dataguidance, https://www.dataguidance.com/notes/cameroon-data-protection-overview (Lastly consulted on the 18th of February, 2025)

[18] Adebisi, L. (2021). "Giving 'teeth' to the African union towards advancing compliance with data privacy norms." Information and Communication Technology Law 30 (2),87-107

[19] Cuijpers, C. and Purtova, N. (2014). "Data protection reform and the internet: the draft data protection regulation." Research Handbook on EU internet law, 543-568

[20] Kuner, C. (2010). "Data protection and international jurisdiction on the internet." International Journal of law and information technology, 18 (2), 176-193

[21] Norton, N. (2023). "Building a Safe and Effective Data Privacy Programme: A Comprehensive Guide." Available at at https://www.korumlegal.com/blog/ building-a-safe-and-effective-data-privacy-program-a-comprehensive-guide (Lastly consulted on the 18th of February, 2025)

[22] Guarda, P. and Zannone, N.(2009). "Towards the development of privacy aware systems." Information and Software Technology 51 (2), 337-350

[23] Danezis, G. et al (2015). "Privacy and data protection by design-from policy to engineering." Arxiv preprint arxiv 1501.03726

[24] Bennett, J. (2012). "The Accountability approach to privacy and data protection: assumptions and caveats." Managing privacy through accountability, 33-48

[25] Bieker, F.; Friedewald, M. (2016). "A process for data protection impact assessment under the European general data protection regulation". Privacy technology and policy: 4th annual privacy forum, APF.

[26] Binns, R. (2017). "Data protection Impact Assessment: a meta-regulatory approach." International data privacy law 7 (1), 22-35

[27] Karmarkar, S.; Apte, M. (2007). "Operations management in the information economy: information products, processes and chains." Journal of operations management 25(2), 438-453

[28] Kuner, C. (2010). "Regulation of transborder data flows under data protection and privacy law: past, present and future." TILT Law and technology working paper

[29] Kerber, W. (2016). "Digital markets, data, and privacy: competition law, consumer law and data protection." Journal of intellectual property law and practice, jpw150

[30] Galliers, R. (1994). "Information systems, operational research and business reengineering." International transactions in operational research 1(2), 159-167

[31] Rudraswamy, V.; Vance, D (2001). "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment." Logistics information management 14 (1/2), 127-137

[32] Kira, B. et al (2021). "Regulating digital ecosystems: bridging the gap between competition policy and data protection." Industrial and corporate change 30 (5), 1337-1360

[33] Asongwe, P. (2011): "Cameroon's public administration since 1998: Tracking the opportunities and challenges of digital governance." Paper presented at the Fifth eGov Africa Forum, 26-28 April 2011, Yaounde.

[34] Cheka, C., ibid

[35] Keenan, J. (2006). "The New Deterrence: Crime and Policy in the Age of Globalization." Iowa Law Review, Vol. 91, p. 505, Available at: http://hdl.handle.net/11212/1116

[36] Mireille, D. (2003). "Comparative Legal Studies and the Internationalization of Law." Liz Libbrecht, Available at: https://books.openedition.org/cdf/3878?lang=en (Lastly consulted on the 19th of February, 2025)

[37] Ahmadi, S. (2018). "The effect of globalization on the national criminal law systems." University of Nebraska-Lincoln, Library Philosophy and Practice (e-journal) https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5960&context=libphilprac

[38] Akuta, E. et al (2011). "Combating cybercrime in sub-Sahara Africa: A discourse on law, policy and practice." Journal of Peace, Gender and Development Studies, 1(4), pp. 129-137, Available at; www.interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al (Lastly consulted on the 19th of February, 2025)

[39] George, H. (2016). *Criminological Theory.* Wolters Kluwer.

[40] Simonovic, I. (2000). "State sovereignty and globalization: are some states more equal?" Georgia Journal of International and Comparative Law 28 (3): 384

[41] Nadelmann, E. (1990). "The role of the United States in the international enforcement of criminal law." Harvard International Law Journal 31.

[42] Spies, A. (2011). "Global data protection: whose rules govern.", Sedona Conf. J. 12, 105

Svantesson, B. (2021). Private international law and the internet. Walters Kluwer

[43] Chayes, A. et al (1995). "The New Sovereignty: Compliance with International Regulatory Agreement." Cambridge, MA: Harvard University Press.

[44] Vives, L. (2023): "The emergence of new business models." Management research: the journal of the iberoamerican Academy of management, Vol. 9 N°3

[45] Barkatullah, H. (2018). "Does self-regulation provide legal protection and security to e-commerce consumers?" Electronic commerce research and applications 30, 94-101

[46] Bieron, B.; Ahmed, U. (2012). "Regulating e-commerce through international policy: understanding the international trade law issues of e-commerce." Journal of world trade 46(3)

[47] Walden, I.; Hornle, J. (2001)."E-commerce law and practice in Europe." Elsevier, 2001

[48] Ibid

[49] Ikenwe, J.; Magnus, O. (2016). "Information Security in the Digital Age: the case of developing countries." Chinese Librarianship: an international electronic journal, 42, available at: https://www.researchgate.net/publication/321767925_Information_Security_in_the_Digital_Age_The_Case_of_Developing_Countries , accessed, 19th February, 2025.

[50] Asongwe, P., (2012); ibid.