Protection of Data of Enterprises under Cameroonian Law: A Critical Appraisal

Quincy Awoh Fon

2nd Year Doctorate Student, University of Yaoundé II, Cameroon

DOI: 10.55662/JLSR.2024.10603

Abstract

Data protection has always been a thorny and controversial issue in the world at large and in all domains of human existence. In the present context of digitalisation and globalisation, the phenomenon for the data protection has been an unfavourable factor for the growth or downfall of an enterprise. In many areas of the world, especially in the industrialised and developed countries, there are strong legal dispositions to protect individual, collective, and enterprise data. However, in the under developed countries, the idea of data protection is a challenging venture because in most cases, the principles that are created with the intention of protecting data of enterprises, lacks well defined checks and balances or a robust mechanism for accountability, potentially resulting in breaches of enterprise data. This has therefore inspired this work to pose a question as to what extent does the legal provisions on data protection provides for the protection of data of enterprises in the country Cameroon? The fundamental objective of this research is to examine the extent to which the legal provisions on data protection effectively enable for the protection of data of enterprises in Cameroon. To meet the objective of this study and address the problem, data was collected through the exploitation secondary sources of information. In treatment of the data, findings revealed that the raison d'etre for the inadequate and insufficient nature of data protection of enterprises in Cameroon is due to the insufficient nature of the data protection legislation in Cameroon, and the non-concerned nature of the owners of enterprises in Cameroon when it concerns the protection of data. In

this light, it is recommended that the Government of Cameroon legislates' laws that satisfactorily guarantee the protection of enterprise data.

Keywords: *Data, Data Protection, Data of Enterprises, Protection, Impact, Confidentiality, Cameroon.*

Background to the study

Data has become a great asset for many organisations promising improved operations and new business opportunities[i]. However, data has increased access to sensitive information that when processed can directly jeopardize the privacy of individuals and violate data protection laws[ii]. Therefore, data controllers and data processors in collaboration with the law may impose tough punitive measures for non-compliance with the general data protection regulation that can result even to bankruptcy.

Data is information, especially facts or numbers collected, examined, considered, and used to help decision-making[iii], or information in an electronic form that can be stored and used by a computer.[iv] In computing, data is information, which is converted into a form that is efficient for movement or processing[v]. In modern computers and communication systems, data is typically represented in binary digital form. However, this work focuses on data of enterprises and not data in its generic term. Thus, data of enterprise is the totality of the digital information flowing through an organisation. This includes structured and unstructured data. Structured data includes recordings in spread sheets and relational data bases. While unstructured data deals with images and video contents.[vi]

However, though this definition has defined data of enterprises as being information that is digital, it must be noted that, an enterprise that is not digital will have in its possession information, and not just any kind of information but sensitive information that is stored in books and the most traditional forms of storing information and will be considered data. Therefore, data of enterprise is information that flows through an organisation.

After having discussed what data of enterprise is, it is of essence that the notion of data protection is understood and its importance. Data protection is the process of safeguarding important information from corruption, compromise, theft or loss[vii]. 'Any organisation that

wants to work effectively needs to ensure the safety of all the information in their organisation by implementing a data protection framework which ensures that sensitive data is only accessible to approved parties' said Mr Oyegoke[viii]. Protecting data is important because it prevents the information of an organisation from fraudulent activities, hacking, and or identity theft.

As the global economy and the information age is rapidly developing, so is cyber criminality rapidly increasing, thus there is an underlying need for a general law on data protection and punitive measures put in place if a breach on these regulations occur. In 2020, it was estimated that people created an average of 2.5 quintillion bytes of data in a day.[ix] This proliferation of data creation, coupled with the technological capacity to store and analyse unprecedented amounts of data, has caused concerns around its misuse[x]. Little amounts of data which concerns an individual may be collected to create an overview which is used for informed decisions, such as the type of material or advertisement to make for an individual. In response, countries have incrementally enacted legislation that aims to regulate how data is processed[xi]. That notwithstanding, presently, 66% of countries globally have active legislation, with another10% having proposed bills under consideration.[xii]

In the united states data privacy is not highly regulated, so by extension there are no strict data protection laws that apply, although that is quickly changing as people become aware of the value of privacy and data protection[xiii]. In the United Kingdom however, the legislative body passed enacted the Data Protection Act of 1998, which updated the foundational 1984 Act, establishing regulations for data users and outlining individuals' rights concerning data that pertains to them personally, and the act became effective on March 1, 2000[xiv] .The act gives guidelines, eight principles, which a data controller must observe when handling personal data in the course of doing business.[xv] These principles emphasis that data should be obtained fairly and lawfully and it should not be transferred abroad unless specific conditions pertaining to protection are met.[xvi] The European Union on her on part has a General Data Protection Regulation that went into effect May 25, 2018 which is set to administer how the personal data of individuals in the European Union may be processed and transferred.

Though data protection and the concerns surrounding it is not a new concept to Africa, as they have been raised decades ago, the adoption of relevant legislation has been slow. Countries in African are behind the world trend, with only 52% having active data protection legislation[xvii]. Such delayed development has been linked to presumptions that African countries favour collective rights over rights that are primarily concerned with the individual, such as the right to privacy[xviii].

Data protection in Africa is encompassed by the convention of the African Union on cyber security and personal data[xix], which has been ratified by only a small number of the 55 African Union members[xx]. To enable realization of the Convention, the African Union Commission asked the internet society to collectively, develop the privacy and personal data protection guidelines for Africa ('the guidelines')[xxi]. The guidelines offer guidance on how to help individuals take a more active part in the protection of their personal data, amongst other things[xxii]. In the last decade, African nations have progressively enacted laws and introduced regulation to safeguard data protections.[xxiii]

Presently, 33 countries have data protection legislations and/or regulations[xxiv]. In 2021, only 3[xxv] countries enacted their first data protection law and one country Cape Verde, amended her existing legislation[xxvi]. Another country, Burkina Faso, replaced her 2004 data protection Act with a new one. These past years, jurisdictions with a data protection legal framework also adopted and issued regulations and guidance[xxvii]. The adoption of data protection legislations throughout Africa is a positive sign for the future.

Cameroon is situated at the boundary of Western and Central Africa. According to the data of the United Nations, Cameroon is positioned 52 in the list of countries by population, estimated at 26,545,863 individuals[xxviii]. This constitutes a lot of individual's information that can potentially be collected, hence needing to be safeguarded. It may not be obvious at first glance, but few data protection principles have been put in place[xxix]. Although there is no comprehensive data protection legislation, the country opted for a sectorial approach. As a specific data protection legislation is yet to be adopted; it is quite challenging for data subjects to control the use of their own data[xxx]. However, Cameroon is preparing a privacy bill ("the bill"), according to the competent services of the ministry of posts and telecommunications[xxxi]. The drafting of the bill is currently in motion; the bill will govern the collection, processing,

transmitting, storage, and use of data[xxxii]. Although the is no specific law in Cameroon regulating data protection at the moment, the applicable provisions that are found in several enactments mostly cover information that relates to electronic communications, meanwhile some other sectors handle personal data daily. In the preamble of the Cameroon Constitution and the duly ratified international relating thereto:[xxxiii] 'Freedom and security are guaranteed to every individual with due respect for the rights of others and the best interest of the state; and Privacy of all correspondence is inviolable- no interference may be allowed except provided in a judicial decision'. Hence, Data protection is a right upheld by the Cameroon Constitution.

Data protection legislations apply to identifiable natural persons, and to facts governed by national laws in Cameroon[xxxiv]. Although, the CEMAC[xxxv] Laws apply to the facts that the specifically cover[xxxvi]. As far as electronic communication is concerned, specific laws govern the collection of personal data by operators and of electronic communication network service providers[xxxvii]. Furthermore, in telecommunication Law No. 2010/012 of 21 December 2010[xxxviii] relating to cyber security and cyber criminality in Cameroon has been enacted[xxxix].

Additionally, several executive orders have been enacted, including the electronic communications[xl] law, E-Commerce[xli] law, consumer protection[xlii] law, and ANTIC[xliii]. In the health and pharmaceutical sectors, different decrees and the Penal Code cover the protection of data. More so, some companies have been subject to sanctions, making case law a great indicator of where the country is regarding data protection. In other for one to see the full picture of data protection in Cameroon, all these regulations must be taken as a whole.

In Cameroon, an authority dedicated for data protection, otherwise known, as the data protection officer has not yet been appointed[xliv]. However, the national information and communication technology agency on behalf of the Government ensures, the supervision, regulation, and oversight of activities related to the protection of information systems and electronic communications networks, and aids in the identification of cybercriminals[xlv]. It is relevant to take note that the government, through the Ministry of Telecommunications, and agencies such as the ANTIC and ART, and organizations like African Wits have done a great job launching sensitization efforts. Consent is described as a primordial requirement in several Legislation governing the processing and collection of personal data in Cameroon. In

addition, the data subject has rights concerning their data, such as, the right to be informed, to access and to object. However, accruing to the fact that there is no specific legislation on the protection of data in Cameroon, Cameroon has not ratified any treaty addressing the protection of data specifically personal data[xlvi]. Because of this void, digitalisation boom exposed citizens to many dangers. The protection of data of enterprises in Cameroon is mostly left at the discretion of the organisation and the processing, storing and use of data collected from individuals known as the data subject is also left in the discretion of the enterprise as there is no special organisation in Cameroon charged with this responsibility[xlvii].

For this reason, the government and her citizens all together should put in measures in Cameroon for the protection of data of enterprises as soon as possible.

Research problem

The development of data protection in the world and in Cameroon specifically is expected to be of great benefits to the society and a source of job creation. Data protection is not only beneficial to the data subject but as well the enterprises and the state. Thus, the protection of data will automatically raise the hopes of the community for better economic opportunities. Thus, the government has put in place several laws that regulates on data protection in Cameroon.

Despite these legal provisions, there is still persistent violation of individual and enterprise data irrespective of the different laws protecting data in Cameroon, some factors are the causes of such persistent violation.

To begin with, the lack of a specific regulation, legal framework or law enacted on the protection of data, as well as the lapses in the current legal framework in Cameroon is a call for concern.

Adding to this is the situation of no specific institution and independent authority in charge with the responsibility of ensuring that the laws relating to processing, storage and usage of data in Cameroon is respected.

Furthermore, ineffective implementation of the existing data protection regulations and laws by the courts and the executive body in charge of implementation is a call for concern.

Data protections in the Cameroonian legal system has put in place certain rights and obligations for the data subjects and data collector and even mention the legal basis for an action. The appropriate framework for the collection, processing, transmission, storage or use of data, let alone the obligations of those responsible for their processing or the rights of persons whose data are collected, and the steps they should take in case of an unlawful processing[xlviii] has not been taken into consideration by the several laws that dealing with data protection

In addition, what are the means set by the enterprises and the law in case of a breach of data protected by enterprises over the cyber space.

The research problem of this study is therefore to find out how the Cameroonian legal system provides for the protection of data of enterprises and why there is persistent violation of data of enterprises in Cameroon despite the existence of legal instruments relating thereto. Coupled with the fact that some enterprises do not care about protecting data of her customers nor do they take reasonable care to secure data

Research question

To what extent do the legal provisions on data protection guarantee the protection of data of enterprises in Cameroon?

Research objective

The objective of this research work is to examine the extent to which the legal provisions on data protection effectively enable for the protection of data of enterprises in Cameroon

Research methodology

The doctrinal/Bench methods

This is a research method that involves using already existing data[xlix]. Existing data is summarised to increase the overall effectiveness of the research work[l]. Secondary data is collected by someone other than the actual user. This simply means that information is already available and someone analyses it. Researchers leverage secondary data analysis in an attempt to answer a new research question, or to examine an alternative perspective on the original question of the previous study[li]. The Secondary research method includes;[lii]

The consultation of documents from online sources and other means, reading of books, articles, journals, dissertations, thesis, and laws to later on analyse them.

There is also the consultation of useful internet websites, watching of news and reading newspapers, and the visitation of libraries and documentations. This study will make use of the secondary research method, and every article, book or journal read and every consultation done is what is relevant to this study.

Literature review

Although much has been written and researched concerning technological methods of securing data of enterprises, very little has been researched about the legal aspect of protecting data of enterprise and the sanctions for people who attack such data. Perhaps, this is due to the relatively young field of information technology and as such not enough consideration has been put in place for the protection of data. However, they have been some researchers who researched about the different areas of data protection.

Data Protection: Governance, Risk Management, and Compliance

David G. Hill [liii] in his book says the failure to appreciate the full dimension of data protection can lead to poor data management, costly resource allocation issues, and exposure to unnecessary[liv] risk. Data protection: Risk Management and Compliance explains how to gain a handle on the vital aspects of data protection. The author begins by building the foundation

of data protection from a risk perspective and then introduces two pillars in the governance, risk management and compliance framework. After exploring data protection and data security, the book focuses on data protection technologies primarily from a risk management point of view. It also discusses the special technology requirements for compliance, governance and data security; the importance of e-Discovery for civil litigation; the impact of third party services in conjunction with data protection and data processing facts, such as the role of server and storage visualization. The final chapter describes a model to help businesses get started in the planning process to improve their data protection. This book offers a solid understanding of how data protection fits into various organisations and allows these organisations to decide what technologies and tactics best meet those requirements[lv]. However, though David G. Hill's book exploits risk management, this work on the other hand will not only talk on the concept of risk management, but the impacts of not protecting data of enterprises in Cameroon.

Data Protection: Ensuring Data Availability

Preston D. Guise[lvi]in his book takes a holistic, business-based approach to data protection. It explains how data protection is a mix of proactive and reactive planning, technology and activities that allow for data continuity[lvii]. Data protection is neither RAID nor is it continuous availability, replications snapshots or backup—it is all of them, combined in a considered and measured approach to suit the criticality of data and meet all the requirements of the business[lviii]. Enterprises and businesses seeking to creatively, leverage their IT investments and to drive through cost optimisation are increasingly looking at data protection as a mechanism to achieve those goals. In addition to being a type of insurance policy, data protection is becoming an enabler for the new processes around data movement and data processing. Furthermore, this book arms readers with information critical for making decisions on how data can be protected against loss in the cloud, on-premises, or in a mix of the two. Even though this book talks about data protection as a means for enterprises and businesses to drive through cost optimisation, this work will not only look at this concept, but at the positive impacts of effective data protection of enterprises in Cameroon.

Big Data in Context: Legal, Social and Technological Insights

Thomas H. and Barbara[lix] in his book shed new light on a selection of big data scenarios from an interdisciplinary perspective. It features legal, sociological and economic approaches to fundamental big data topics such as privacy and data quality on the one hand and practical applications such as smart cars, and web tracking on the other hand. It also provides a comprehensive overview of an introduction to the emerging challenges regarding data. Though this book might have however spoken about the emerging challenges regarding data, and what big data is, this work on the other hand will focus on the challenges of data protection of enterprises in Cameroon.

Challenges of Regulating Financial Service Provision in Cameroon in the Digital Age and a Globalised World

Cosmas C[lx]. In his article, say the pre-digital age rules on the ascription of legal responsibility as well as the basis on which the regulation of financial services was founded have been profoundly redefined by the information, communication and technology revolution and globalisation. Accordingly, there are some challenges of the digital revolution and globalisation to the regulation of financial services in Cameroon that are key concepts on which the regulation of business and enterprise financial service provision is found. These challenges include; the concepts of 'time', 'space', and 'being', which are central to the ascription of legal responsibility. The results are significant in alerting to the dire need for reform of the rules governing the provision of financial services. Even though this article looks at legal responsibility in the pre-digital age, as well as how the basis on which the regulation of financial services was founded have been redefined by the information, communication and technology, this work is out to give a clear understanding of what data protection of enterprise in Cameroon is.

What We Do With Data: A Performative Critique of Data Collection, Creative Commons Attribution 3.0 Germany

Garfield B.[lxi]in his work, says data collection is everywhere. It happens overtly and behind the scenes. It is a specific moment of legal obligation, the point at which the purpose and conditions of data are legitimised. However, what does the term data collection mean? What does it say or not say? Does it really capture the extraction and imposition-taking place? How do terms and practices relate in defining the norms of data in society? This article undertakes a critique of data collection using data feminism and as per formative theory of privacy: as a resource, an objective discovery and an assumption. It also discusses alternative terms and implications of how we describe practices of collecting data. Even though Garfield B's work talks on data collection and critiques of data collection using data feminism, this research work will talk on the concept and principles in data collection of enterprises in Cameroon.

Nature and Methods of Data Protection of Enterprises in Cameroon

Introduction

Data protection within enterprises in Cameroon has gained significant attention, particularly with the advent of the information age. This increase in focus stems from the necessity of safeguarding personal and sensitive data handled by both public and private organisations. In response to growing concerns, Cameroonian legislators have enacted laws for sectorial management of data protection, appointing specific authorities to oversee compliance and obligations[lxii]. This chapter will explore the nature and methods of data protection in Cameroon, covering concepts, importance of data protection and the legal grounds for data protection.

- The concept of data protection

Data protection is fundamental to maintaining trust between individuals and organisations. It involves the ethical handling of personal data collected for purposes beyond personal or household use[lxiii]. This practice not only aligns with the right to privacy but also fosters public confidence in both private and public sector innovations. Essentially, data protection ensures

that critical information is safeguarded against corruption or loss and remains accessible solely to authorised parties, in compliance with legal standards[lxiv].

Data protection laws apply universally to any entity that processes personal data for business purposes. However, they do not extend to personal data usage for household activities, such as private communications or social media interactions.

- The importance of data protection of enterprises

With increased reliance on cloud and online transactions, more and more data is being handled by many enterprises[lxv]. Bad actors, outside and inside an enterprise, constantly look for ways to to compromise an organization's data security for their own ends. Data violators often aim to steal information from a company, selling it to others, or using it to commit acts of fraud[lxvi].

Since enterprises handle a great deal of personal identifiable information (PII) from their customers, employees, and stakeholders, a data breach can do a great deal of harm. Some of the most potentially damaging effects come from data breaches that steal especially sensitive PII, such as social security numbers, business information, driver's licenses, and passports.

Data protection for enterprises is especially important because data breaches and losses can end up costing a significant amount of money, and a reputational hit. Below are some of the reasons why data protection of enterprises is important.

- Enterprise credibility

A breach can erode consumer trust, as customers may hesitate to share personal information if they perceive a risk of theft. Consequently, protecting data is essential for maintaining credibility and fostering consumer confidence[lxvii].

- An increase in enterprise turnover

Safeguarding data is crucial for financial health. Data breaches can incur costs that detract from profitability. A secure environment fosters customer satisfaction, leading to increased revenue[lxviii].

- Decision making facilitation

Effective data protection enables enterprises to make informed decisions based on accurate data analysis, improving operational efficiency and strategic planning[lxix].

- Understanding the risks of not having data protection

Sometimes, small and medium-sized businesses think they don't face much risk from data breaches. They usually believe that bad actors are more likely to target larger organizations. However, this thinking doesn't stand up to reality, as 43% of data breaches[lxx] affect small and medium-sized businesses. While large businesses face the most data breaches, small and medium ones still face a significant number of breaches, making data protection a must-have for all organizations[lxxi]. When organizations don't take their data security risks seriously, they open themselves up to several risks. Below are some of the primary risks of not having data protection framework:

- Credibility issues

Failure to secure data can lead to a loss of customer trust, even if breaches do not directly impact them. Negative publicity can deter potential customers, impacting overall business viability.

- Financial losses

A lack of data protection can result in organizations suffering from financial losses. A report in 2021 found that the average costs of data breaches reached $4.24 million, with this finding representing a 10% increase[lxxii] from the previous year. This same report found that this average cost rises to $4.96 million when an organization relies on remote workers. Given the impact these financial losses could have on an organization, data protection is essential.

i. The high costs of data breaches tend to come from various actions a company might have to take after a data breach, such as:
ii. Paying out compensation to customers affected by the breach
iii. Purchasing new security mechanisms
iv. Covering legal fees
v. Paying for an investigation to discover how the breach occurred

vi. A data breach can also cause regulatory penalties if the organization was not complying with particular security regulations.

- Legislative sanctions

Organisations risk legal repercussions for inadequate data protection. Victims of breaches can seek compensation, leading to costly litigation and reputational damage.

If an organization loses the case, they will end up needing to pay out compensation, which could be in the millions of dollars. Equifax's 2017 data breach ended up causing the company to have to pay as much as $700 million to U.S. customers[lxxiii] in compensation. Besides compensation costs, an organization will also have to spend time and money on its legal defence and suffer from reputational damage. Due to the financial and credibility concerns surrounding legal action, proper data protection is essential.

- Data loss

Organisations risk legal repercussions for inadequate data protection. Victims of breaches can seek compensation, leading to costly litigation and reputational damage

- Unauthorised access to data of enterprises

Data of enterprises will be considered to be accessed unlawfully if the consent of the data subject is not taken into consideration. In Cameroon, data can be accessed without the authorisation of the data subject in the following instance:

- The law

The Constitution of the Republic of Cameroon amended by the law No 96-06 of 18 January 1996 establishes a number of safeguards. The Preamble affirms "affirm our attachments to the fundamental freedoms enshrined in the Universal Declaration of Human Rights, the Charter of the United Nations and the African Charter on Human and people's Rights, and all duly ratified international conventions relating thereto", including "the home is inviolate. No search may be conducted except by virtue of the law".[lxxiv] Data of enterprises will only be given to a third party without the consent of the data subject, where it is for legal purposes or required by the law.

- Legal bases for the protection of data of enterprises in Cameroon

The protection of enterprise data is based on the following:

- Consent of the data subject

The consent of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of data relating to him or her[lxxv].

In Cameroon, consent is described as a prerequisite in several laws governing the collection and processing of data[lxxvi].

Section 3 of the regulating Electronic commerce decree[lxxvii] provides that persons engaged in electronic commerce and established in a third country must specify the applicable law and obtain the consent of the recipient of the proposed service[lxxviii].

Moreover, section 7 of the E-commerce law[lxxix] provides that prior consent is necessary for direct marketing using an automatic calling machine, fax or e-mail using, in any form whatsoever, the contact details of a natural or legal person.

Challenges Affecting the Protection of Data of Enterprises in Cameroon

Introduction

Data protection remains a contentious issue across all sectors, as enterprises increasingly prioritize safeguarding against breaches that threaten valuable information. According to the International Data Corporation (IDC), over 1.5 billion people were projected to be impacted by data breaches by 2020[lxxx]. Effective data protection is essential for any country's development and is crucial for modern enterprises, influencing both their core assets and customer privacy[lxxxi]. Legal actions and penalties related to breaches are rising, prompting governments to impose stricter data privacy regulations, thereby granting consumers enhanced rights.

Security professionals are tasked with categorizing data by risk and employing appropriate security measures for sensitive and personally identifiable information. Despite the significant

technological advancements driven by data over the past decade, enterprises face considerable challenges in protecting this data[lxxxii]. Rapid data growth outpaces many organizations' budgets, hindering their ability to implement the necessary technologies to secure users' information.

This chapter will explore the specific challenges faced by enterprises in Cameroon regarding data protection.

The growth of data is exponential

Data generation is accelerating, with more than 1.7 megabytes created every second. Enterprises must not only safeguard customer personal information but also sensitive data[lxxxiii]. The Breach Level Index[lxxxiv] reports that nearly 9.2 billion data records have been lost or stolen since 2013[lxxxv]. Despite the exponential growth of data, inadequate security practices leave enterprises vulnerable to breaches. The protection of personally identifiable information is particularly concerning, as the sheer volume of data in our technology-driven world makes it overwhelming for organizations to manage millions, if not billions, of records effectively[lxxxvi].

Cost of maintaining data protection

A data breach can result in significant financial losses for enterprises, with the Ponemon Institute reporting an average cost of $3.62 million in 2017 and a 30% likelihood of experiencing a breach. Companies may face severe regulatory penalties, especially in the European Union, where fines can reach 4% of adjusted gross revenue or €20 million for major breaches. In Cameroon, high costs associated with implementing data protection measures often lead enterprises to overlook customer data security. Even when protective measures are in place, ongoing maintenance costs can exceed budgets, resulting in further neglect.

Human error

The sectorial nature of the instruments on data protection of enterprises in Cameroon-

The sectorial nature of the protection of data is a challenge for enterprises in Cameroon. For instance the principle of consent as a pre requisite is found in several laws governing the collection and processing of personal data in Cameroon.[lxxxvii] This is a challenge because of the following reasons:

The case of determining the appropriate law

The Cameroon legal system, like most in Africa, is a relic of the colonial era. However, it is unique in that it consists of two distinct and often conflicting legal systems, the English Common Law and the French Civil Law operating in some sort of tenuous coexistence[lxxxviii]. The Cameroonian legal system can therefore be described as bi-jural, although most of the uniform laws that are now being introduced are essentially based on French legal concepts. This makes Cameroon one of the few examples of such a dual legal system in the world[lxxxix].

Due to the sectorial nature of the instruments on the protection of data, and the Cameroon legal system, enterprises find it challenging when it comes to determining the appropriate law for the protection of data of their enterprise.

The challenge on the identification of offenders

Every crime contains a progression of activities or steps that is always moving from the gathering of evidence, to that of gathering information, developing the evidence acquired so as to form reasonable grounds for everyone in believing that the suspect or accused in question is really responsible for all the allegations made against him or her[xc].

Since the laws on data protection are found in disparate instruments, the identification of offenders is challenging to enterprises in Cameroon because different instruments have different laws on who is an offender in data, and how offenders of data protection are identified.

Challenge of jurisdiction

Jurisdiction is the power to exercise authority over persons and things within a territory[xci]. In a legal sense, it gives a court the power to hear and trail a case or lawsuit[xcii]. Jurisdiction can also relate to a geographical area in which political authority is recognised[xciii]. The three main types of jurisdiction are known as territorial, personal, and subject matter[xciv]. Some courts may also have exclusive or concurrent jurisdiction[xcv]

The fact that the laws on data protection are found in different instruments is a challenge to enterprises that want to protect their data because, they cannot easily identify the jurisdiction in charge of cases in data protection because some instrument may provide punishment which is less, while some instruments may provide punishments that are higher.

The challenge in punishing cybercriminals

Technological developments have affected accelerated, changed and transformed human life as well as communications and interactions between humans throughout history. People can communicate and make trade easily without taking into consideration the borders and distances because of developments in telecommunication and information technologies which has also increase the chances of our rights being violated especially in an attempt to regulate these new developments. However, though there is a rapid increase in technology, the cyber space[xcvi], and growth in cybercriminals[xcvii], the Cameroon legal system seems not to be moving at this rapid pace, and this is quite disturbing.

The cyber law in Cameroon has not successfully deterred cybercriminals from committing crimes because the sanctions are less severe. When the sanctions provided for are looked upon, it is found that the maximum term for imprisonment of cybercriminals is 10 years, making their offence which is a serious offence a misdemeanour rather than a felony[xcviii]. This of course, makes cybercriminals very comfortable in committing the offence. Thus when the data of an enterprise is stolen, the inadequacy of the law makes it difficult for the enterprise to stop suffering from such offences which in turn makes the enterprise to suffer a great loss.

With regards to the anonymity of cybercriminals, the wide nature of the cyber space and the discrete nature of cybercrimes makes it very difficult to locate or identify a culprit, added to this is the lack of expertise among investigating officers, and thus obtaining evidence[xcix]. An enterprise that suffers a loss because of stolen data is more likely to suffer more loss, because the anonymity of the offenders makes it very challenging to prosecute or even recover he lost data.

Insider threats

A small percentage of people trying to protect systems from hacking breach and poor data stewardship practices are either already bad actors or could become bad actors. With insider and outsider mingling, human resource and the legal department must be engaged to better understand the risks from employees and others, such as third-party contractors, with potential access to data[c]. Most enterprises eliminate access privileges upon termination, but it requires near-real-time coordination to be successful. An angry employee going out the door with access capabilities intact can cause a lot of trouble for the enterprise in a brief period.

Thus this becomes problematic for enterprises because there are no clear rules, roles and responsibilities spelled out in an unambiguous language, as well as enforcement mechanisms.

Corporate Culture in ignoring cyber attacks

The first, and perhaps least recognized, challenge to data protection is a corporate culture that undervalues cyber security. Many small to medium businesses (SMBs) are often taken by surprise when they face a security incident, as they don't believe they could be targeted by cybercriminals. This misconception is dangerous; cybercriminals often target smaller businesses precisely because they lack strong cyber security measures, making them easier prey. Adopting a preventative approach to cyber security is far more beneficial than a reactive one. Security incidents, particularly data breaches, can have lasting repercussions on an organization's reputation, along with risks of class-action lawsuits and financial disaster.

Establishing a culture that prioritizes data protection must begin at the top. When senior executives, board members, and decision-makers emphasize the importance of cyber security, it will resonate throughout the organization, influencing employees, third parties, and customers alike.

Challenges specific to the protection of data in the face of digitalisation

- Duplicate resources across dispersed workplaces and dealing with digitalisation

IT staff managing offsite backups have major challenges. Managing redundant hardware and software in multiple remote branch locations adds to the complexity and expenses.

Almost all enterprises in Cameroon are struggling to adapt to the rapid changes introduced by digitalisation. With the presence of the internet and sophisticated software, enterprises find it relatively easy to shift the burden of data protection from using books to using the computer and advanced technology

Technology though a tool in data protection has marred the idea of data protection with a lot of encumbrances. It is now very easy for data criminals to connect and interact with persons across the globe easily thereby making it relatively easy for enterprises in developing countries to be hacked by advance data thieves from developed countries that has had some great mastery in manipulating technology to their advantage.

Digitalisation therefore doesn't only pose the problem of cyber-attacks and theft but also poses the problem of jurisdiction. For example, it will pose a great deal of worry for the Cameroon legislators and law enforcement offers to be able to define and enforce laws that can track and punish a cyber-data criminal nowhere he operates from the globe

- Data Tampering in relation to enterprise digital data

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.

In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the FCFA amount of a banking transaction from 100.000 to 1000.000 FCFA

In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid 10.000 FCFA bank account transfer transaction.[ci]

- Eavesdropping and Data Theft of digital data of enterprises

Data must be stored and transmitted securely, so that information such as credit card numbers cannot be stolen. Over the Internet and in Wide Area Network (WAN) environments, both public carriers and private network owners often route portions of their network through insecure land lines, extremely vulnerable microwave and satellite links, or a number of servers. This situation leaves valuable data open to view by any interested party. In Local Area Network (LAN) environments within a building or campus, insiders with access to the physical wiring can potentially view data not intended for them. Network sniffers can easily be installed to eavesdrop on network traffic. Packet sniffers can be designed to find and steal user names and passwords.[cii]

- Falsifying User Identities in enterprises

You need to know your users. In a distributed environment, it becomes more feasible for a user to falsify an identity to gain access to sensitive and important information of an enterprise. How can one be sure that user Pat connecting to Server A from Client B really is user Pat?

Identity theft is becoming one of the greatest threats to individuals in the Internet environment. Criminals attempt to steal users' credit card numbers, and then make purchases against the accounts. Or they steal other personal data, such as checking account numbers and driver's license numbers, and set up bogus credit accounts in someone else's name.

Nonrepudiation is another identity concern: how can a person's digital signature be protected? If hackers steal someone's digital signature in an enterprise, that person may be held responsible for any actions performed using their private signing key.

Conclusions and Recommendations

Business in Cameroon is expanding rapidly due to a proliferation of investment opportunities in the country[ciii]. To effectively conduct business in Cameroon, enterprises need to understand the personal data protection regulatory landscape. Non-compliance with personal data protection legislation in Cameroon may potentially prevent multinational enterprises from capitalising on their ventures in the country by restricting their ability to transfer personal data to third parties beyond Cameroon's borders, thereby hindering business operations[civ].

Despite its many benefits, the protection of data for enterprises in Cameroon faces numerous challenges. By promoting capacity-building programmes, strengthening the legal framework on data protection regarding its applicability, creating a transparent and accessible multi-stakeholder approach to data protection in the cyberspace, establishing universal jurisdiction for crimes committed in the cyberspace, and transforming corporate culture, the aim of enhancing and fostering the protection of data for enterprises in Cameroon could be achieved.

Additionally, raising awareness about the importance of data protection among businesses and the public is crucial. Implementing training for employees on best practices for data handling and security can further mitigate risks. By fostering a culture of accountability and responsibility towards data protection, enterprises can not only comply with legal requirements but also build trust with their customers, ultimately leading to sustained growth and success in the Cameroonian market.

Endnotes

[i] https://zenodo.org , accessed 17 November 2024
[ii] ibid
[iii] https://www.coursehero.com accessed November 17, 2024
[iv] Colin M., Cambridge Advanced Learner's Dictionary, Fourth Edition, published by Klett Sprachen gmbh, August 5, 2013, P.381.
[v] https://Jineshajain20.wordpress.com , Coursera case study, accessed November 17, 2024
[vi]Https://www.stitchdata.com,accessed September 20, 2024 2022.
[vii] https://lexafrica.com accessed November 17 2024, Overview of Data Privacy and Protection in Lesotho
[viii] https://www.businessdailyafrica,com accessed November 17, 2024
[ix]Https://www.forbes.com , accessed September 20, 2024.
[x]Https://www.opengovpartnership.org accessed November 17, 2024 Data Protection in Africa: A Look at OGP Members Progress
[xi] ibid
[xii]Https://www.opengovpartnership.org , accessed September 20, 2024.
[xiii] https://www.techopedia.com accessed November 17, 2024.
[xiv] ibid
[xv] ibid
[xvi] ibid
[xvii] Https://www.opengovpartnership.org , accessed November 18, 2024.
[xviii] ibid
[xix]2014 Convention
[xx]Https://www.bakermckenzie.com , accessed September 20, 2024.
[xxi] Https://www.internetsociety.org accessed November 18 2024
[xxii] ibid
[xxiii]Https://www.jdspra.com , accessed September 20, 2024.
[xxiv]ibid
[xxv] Rwanda, Zambia, Zimbabwe.
[xxvi]Https://www.jdspra.com , accessed September 20, 2024.
[xxvii] Case of Uganda, Kenya, Senegal and South Africa.
[xxviii] https://iapp.org , accessed November 18, 2024.
[xxix] ibid
[xxx] ibid
[xxxi] Https://www.dataguidance.com , accessed September 20, 2024.
[xxxii]Https://www.lexafrica.com , accessed September 20, 2024.
[xxxiii] law no. 96/6 of 18 January 1996 revising the Constitution of 02 June 1972, as amended and supplemented by law no. 2008/001 of 14 April 2008 it is stated that:
Affirm the people of Cameroon their attachment to the fundamental freedoms enshrined in the Universal Declaration of Human Rights 1945, the Charter of the United Nations 1945, the African Charter on Human and Peoples' Rights 1981
[xxxiv]Https://www.dataguidance.com , accessed September 20, 2024.
[xxxv] Central African Economic and Monetary Community
[xxxvi] Ibid
[xxxvii] ibid
[xxxviii] https://iapp.org accessed November 18, 2024
[xxxix] ibid
[xl] Law No 2010/013 of 21 December 2010 governing Electronic Communications in Cameroon.
[xli] Law No 2010/021 of 21 December 2010 on Electronic Commerce in Cameroon.
[xlii] Law No 2011/012 of 06 may 2011 on Consumer Protection in Cameroon.
[xliii]Decree No. 2012/1637/PM of 2012, National information and Communication Technology Agency Decree
[xliv]Https://www.dataguidance.com , accessed Septemebr 20, 2024.
[xlv]*"Data Protection Overview in Cameroon"*,Https://www.dataguidance.com , accessed September 20, 2024.
[xlvi] https://www.businessincameroon.com accessed November 19 2024.
[xlvii]Https://www.oecd.org , accessed September 20, 2024.

[xlviii] https://www.businessincameroon.com accessed November 19 2024.
[xlix] https://www.alchermer.com , accessed 27/09/2024
[l] ibid
[li] https://www.alchermer.com , accessed 27/09/2024
[lii] https://www.qualtrics.com , accessed 27/09/2024
[liii] David G. Hill. DATA PROTECTION: Governance, Risk Management, and Compliance, 1ST Edition, CRC Press in August 13, 2009.
[liv] ibid
[lv] ibid
[lvi] Preston D. Guise, Data Protection: Ensuring Data Availability, 1st Edition, Auer Bach Publications, February 22, 2017.
[lvii] ibid
[lviii]ibid
[lix] Thomas H. And Barbara, Big Data in Context: legal, social and technological insights (Springe Briefs in Law), 1st ed. 2018 Edition, Springer, October 17, 2017.
[lx] Cosmas C., "*Challenges of regulating financial service provision in Cameroon in the digital age and a globalised world*", CODESRIA 2019.
[lxi] Garfield B., "*What we do with data: a performative critique of data collection*", Creative Commons Attribution 3.0 Germany, 7th of December 2021, Https://doi.org/10.14763/2021.4.1588
[lxii] Https://cipesa.org , accessed September 19, 2024.
[lxiii] Https://ico.org.uk , accessed September 11, 2024.
[lxiv] Https://www.techtarget.com , accessed September 11, 2024
[lxv] https://blog.box.com accessed November 18, 2024
[lxvi] ibid
[lxvii] Https://pecb.com , accessed 14 September, 2024.
[lxviii] Https://www.blue-pencil.ca , accessed 14 September, 2024
[lxix] Https://softjourn.com , accessed 14 September, 2024.
[lxx] Https://cybersecurity.magazine.com/10-small-business-cyber-security-statistics- accessed 17 September 2024
[lxxi]https://blog.box.com accessed November 18, 2024
[lxxii] Https://www.cpomagazine.com, accessed 19th September 2024
[lxxiii] Https://www.theverge.com, accessed 21st September 2024
[lxxiv]Https://www.lexafrica.com , accessed 15 September, 2024, the preamble of the 1996 constitution.
[lxxv]See article 4(11) of the European Union General Data Protection Regulation 2016
[lxxvi] Article 44(1) of the 2010 law relating to cyber security and cyber criminality provides that: "it is prohibited for any natural person or legal entity to listen, intercept, store communications and related traffic data, or subject them to any other means if interception or surveillance, without the consent of the users concerned, except where such person is legally authorised to do so."
[lxxvii] Decree No. 2011/1521/PM of 15 July 2011 laying down the Conditions of Application of Law No.2010/021 of 21 December 2010 Regulating Electronic Commerce in Cameroon.
[lxxviii]"*Cameroon Data Protection Overview*", Danielle MOUKOURI DJENGUE, Https://www.dataguidance.com
[lxxix] Law No. 2010/021 of 21 December 2010 regulating Electronic Commerce in Cameroon.
[lxxx] [lxxx]Https://www.gulfbusiness.com accessed October 07, 2024
[lxxxi] Https://www.researchgate.net accessed October 07, 2024.
[lxxxii] Https://www.vera.com accessed October 07, 2024.
[lxxxiii]Https://www.quora.com accessed October 07, 2024.
[lxxxiv] Https://www.itnews.com.au accessed October 07, 2024.
[lxxxv] Https://www.quora.com accessed October 07, 2024
[lxxxvi] Https://www.quora.com accessed October 07, 2024
[lxxxvii] Article 44(1) of the 2010 law relating to cyber security and cyber criminality provides that: "it is prohibited for any natural person or legal entity to listen, intercept, or store communications and related traffic data, or subject them to any other means of interception or surveillance, without the consent of the users concerned, except where such person is legally authorised to do so."
Article 3 of Decree 2011/1521/PM of 15 July 2011 fixing the modalities of application of Law No. 2010/021 of 21 December 2010 governing electronic commerce in Cameroon provides that: "persons engaged in electronic commerce and established in a third country must specify the applicable law and obtain the consent of the recipient of the proposed service."
[lxxxviii]Https://www.nyulawglobal.org accessed October 8, 2024.

[lxxxix]Ibid.
[xc]Https://www.ajol.info accessed October 8, 2024.
[xci]Https://www.thebalancesmb.com accessed October 8, 2024.
[xcii]Ibid.
[xciii]Ibid.
[xciv]Https://www.mylawquestions.com accessed October 8, 2024, personal jurisdiction is the authority over a person, regardless of their location. Territorial jurisdiction is the authority confined to a bounded space, including all those present therein, and events which occur there. Subject matter jurisdiction is the authority over the subject of the legal questions involved in the case.
[xcv]Https://www.mylawquestions.com accessed October 8, 2024. Where a court has exclusive jurisdiction over a territory or a subject matter, it is the only court that is authorised to address the matter. Where a court has a concurrent jurisdiction, more than one court can adjudicate the matter.
[xcvi] This is a global domain within the information environment consisting of the independent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers, Https://csrc.nist.gov accessed October 8, 2024.
[xcvii] These are individuals or a group of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data and generating profit.
[xcviii] Prof Andre Boraine, Dr Ngaundje Leno Doris, " The Fight against Cybercrime in Cameroon", International Journal of Computer global society of scientific research and researchers, ISSN 2307-4523 (Print & Online), 2019, Https://core.ac.uk accessed October 8, 2024.
[xcix]Ibid.
[c]Https://www.techtarget.com accessed October 9, 2024.
[ci] Common Data Protection Challenges & How to Overcome Them, **Published May 20, 2022 , By Reciprocity available at** Https://reciprocity/.com/blog/ **accessed 18th October 2024**
[cii] ibid
[ciii] https://www.afsic.net accessed 20th October 2024.
[civ] Ibid