NATIONAL UNIVERSITY OF LESOTHO

THE IMPACT OF THE ABSENCE OF ELECTRONIC COMMERCE LEGISLATION ON DATA PRIVACY AND SECURITY IN ELECTRONIC TRANSACTIONS IN LESOTHO

By: Malefetsane Michael Sephoso, 201902585

A mini-dissertation submitted in partial fulfilment of the requirements of the degree of Master of Laws (LL.M.) of the Faculty of Law of the National University of Lesotho

Supervised by: Dr. ‘Matšepo Kulehile

May, 2025

Table of Contents

Declaration iv

Acknowledgements v

List of abbreviations and acronyms vi

1. **Chapter one** 1

Introduction of the study 1

1.1 **Introduction** 1

1.2 **Research question** 4

1.3 **Problem statement** 4

1.4 **Hypothesis** 7

1.5 **Aim of the study** 8

1.6 **Objectives of the study** 8

1.7 **Research methodology** 8

1.8 **Literature review** 9

1.9 **Justification of the study** 13

1.10 **Significance of the study** 14

1.11 **Chapter outline** 15

1.11.1 **Chapter one: Introduction of the study** 15

1.11.2 **Chapter two: Critical discussion of the significance of e-commerce legislation** 15

1.11.3 **Chapter three: Outlining the causes of data breaches: The impact of the absence of legislation into the breaches** 15

1.11.4 **Chapter four: Comparison of Lesotho to European Union on regulation of data privacy and security** 16

1.11.5 **Chapter five: Conclusion and recommendations** 16

2. **Chapter two** 17

The significance of e-commerce legislation 17

2.1 **Introduction** 17

2.2 **The importance of data privacy and security in electronic transactions** 18

2.3 **The history behind the emergence of e-commerce legislation** 20

2.4 **The value of legislation in e-commerce** 25

2.5 **Conclusion** 31

3. **Chapter three** 32

Investigating the causes of data breaches and the role of the e-commerce legal framework in Lesotho 32

3.1 **Introduction** 32

3.2 **Causes of data breaches in Lesotho** 32

3.3 **E-commerce Legal framework of Lesotho** 37

3.4 **Nexus between data breaches and ineffectiveness of data protection laws** 48

3.5 **Conclusion** 50

4. **Chapter four** 51

Comparison of Lesotho to European Union on regulation of data privacy and security 51

4.1 **Introduction** 51

4.2 **GDPR provisions on data privacy and security in e-commerce** 51

4.3 **Comparison of the GDPR and e-commerce data protection laws of Lesotho in data protection and security** 59

4.4 **Conclusion** 62

5. **Chapter five** 64

Conclusion and recommendations 64

5.1 **Introduction** 64

5.2 Key Findings 64

5.3 Recommendations 66

5.3.1 Legislative reform 66

5.3.2 Institutional strengthening 69

5.3.3 Enforcement of existing laws and compliance 70

5.4 Conclusion 72

Bibliography 74

Declaration

I Malefetsane Michael Sephoso, solemnly declare that this mini dissertation has not been submitted for a qualification in any other institution of higher learning, nor published in any journal, textbook or other media. The contents of this dissertation entirely reflect my own original research, save for where the work or contributions of others has been accordingly acknowledged.

Name: Malefetsane Michael Sephoso

Signature. M.M. Sephoso

Date: 10th May 2015

Place: Ha-Abia, Maseru

Acknowledgements

Upon the completion of this dissertation, I wish to express my sincerest appreciation to the following people without whose unrelenting help, support and encouragement I would not have been able to carry this task to completion:

- My mother, ‘Mannana Sephoso and my father Teboho Sephoso, thank you for your unconditional financial and emotional support that you offered me from the beginning of this dissertation up until the very end.
- My sister, Bohlokoa Sephoso, I also wish to express my utmost thanks to you for the support and motivation you always gave me throughout my writing of this dissertation.
- My supervisor, Dr Kulehile, I wish to express my heartfelt appreciation to you for the expertise and guidance that you provided me throughout this dissertation.

List of abbreviations and acronyms

CBL	Central Bank of Lesotho
E-commerce	Electronic commerce
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
LeSwitch	Lesotho Payment Switch
LMPS	Lesotho Mounted Police Service
OECD	Organization for Economic Cooperation and Development
MLEC	Model Law on Electronic Commerce
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
USA	United States of America

1. Chapter one

Introduction of the study

1.1 Introduction

The aim of this chapter is to introduce the research topic. This is conducted by setting out the background of electronic commerce (e-commerce), data privacy and security in e-commerce. The chapter will subsequently indicate the problem statement, research question, hypothesis and the relevance of the study.

Electronic commerce (e-commerce) refers broadly to all forms of commercial and/or economic activity conducted through electronic means.[1] It comprises of not only the buying and selling of goods and services over the internet,[2] but also activities such as advertising, online banking, digital content delivery and many others.[3] The growth of e-commerce has, amongst others, reduced the need for buyers and sellers to meet physically, as many transactional activities can now be carried out online. However, with the increasing use of the internet and the expansion of e-commerce, concerns have arisen regarding the adequate protection of consumer information.[4] Thereby giving rise to significant cybersecurity risks.[5] Cybersecurity in this context is defined as the practice of protecting the integrity and confidentiality of information in the digital realm.[6] It is for this reason that the problem that this study discusses is cybersecurity in Lesotho. Particularly the right to privacy of information in e-commerce, data protection and data security.

---

[1] UNCITRAL, *Model Law on Electronic Commerce (1996),* UN Doc A/RES/51/162, Art 1.
[2] Anjali Gupta, 'E-Commerce: Role of E-Commerce in Today's Business' (2014) 4 *International Journal of Computing and Corporate Research* 1.
[3] Supra note 1.
[4] Richard Ansah *et al,* 'Barrier Free Internet Access: Evaluating the Cyber Security Risks Posed by the Adoption of Bring Your Own Devices to e-Learning Network Infrastructure' (2017) 176 *International Journal of Computer Applications* 61.
[5] Ibid.
[6] Dr. Mats'epo Kulehile, 'Digital Rights in Lesotho: A Situational Analysis' (Transformation Resource Centre, 2023) https://www.trc.org.ls/documents/ Accessed 19 December 2024.

The first recorded incident of e-commerce is regarded to have taken place when Stanford University students bought and sold marijuana through the internet in 1971.[7] However, due to the unlawful nature of the internet transactions by Stanford University students, the first commercial transaction effected through the internet is accredited to Michael Aldrich in 1979.[8] It is for this reason that he is renowned as the father of e-commerce.[9] Fast forward to the 1990s, e-commerce significantly grew concurrently with the internet because effecting transactions through the internet spelled easier and convenient mode of trade for both buyers and sellers.[10] The swift exponential growth of e-commerce is the reason why the general problem of this study is cybersecurity.

From its inception, e-commerce has been preferred by consumers. Some of the reasons for this was because through the use of the internet, the movement of information is free, instantaneous and can travel globally with little to no cost.[11] Due to this reason, e-commerce is regarded to have done away with the aged costly and time consuming hurdles that buyers and sellers had to jump over in order to effect transactions.[12]

As a result of the foregoing, it is easy to come to see that the meteoric rise of e-commerce is as a result of it offering convenience to consumers and sellers.[13] Some of the conveniences brought about by e-commerce (online shopping) include *inter alia* website product recommendations, free delivery of products, easier comparisons as there are more choices and many other benefits.[14] When consumers were asked about the factors they consider to be important in online shopping, 32% stated that quality is

[7] Ben Kazinik, 'The History of e-Commerce- How it All Started' (28 March 2024) https://www.mayple.com/blog/history-of-ecommerce Accessed 17 October 2024.
[8] Ibid.
[9] Ibid.
[10] Peter Swire, 'Trustwarp: The Importance of Legal Rules to Electronic Commerce and Privacy' (2003) 54 *Hastings Law Journal* 847.
[11] Ibid.
[12] Ibid.
[13] Farhang Salehi *et al,* 'The Impact of Website Information Convenience On E-commerce Success of Companies' (2012) 57 *Procedia- Social and Behavioral Sciences* 381.
[14] Ibid.

the most important aspect while 30% favored price.[15] Another 13% of consumers pointed out convenience as the most important aspect of online shopping.[16] However, 97% of consumers ultimately withdraw from their purchase (abandonment of carts) if the process of actually getting the product is not convenient.[17]

Despite the lack of convenience stated above, the right to privacy and security in e-commerce has become an important concern to users.[18] Due to widespread e-commerce usage, data protection in terms of privacy and security ought to evolve with technology because technology is not static.[19] Comprehensive e-commerce laws and regulations that shall protect data of consumers are highly needed.[20] As such, Godwin Udo found that the fear of sensitive information being unlawfully disclosed or intercepted by unauthorized people has resulted in some people lacking full confidence in e-commerce.[21]

The fear of consumers to have their sensitive information unlawfully divulged without their consent is well founded.[22] To cure this problem, Mapeshoane & Pather suggest that the government and public sector ought to collaborate in the endorsement of specific laws and policies. These laws and policies are aimed to address computer crimes and improve protection of privacy in online transactions in Lesotho.[23] Godwin Udo also indicated that consumers worldwide tend to hesitate to make use of

---

[15] Smart Insights, 'Convenience is driving e-commerce growth and influencing consumer decision' (28 January 2020) https://www.smartinsights.com/ecommerce/customer-experience-examples/convenience-is-driving-e-commerce-growth-and-influencing-consumer-decisions/ Accessed 7th November 2024.
[16] Ibid.
[17] Ibid.
[18] Meirong Guo, 'A Comparative Study on Consumer Right to Privacy in E-Commerce' (2012) *Department of Social Engineering, Graduate School of Decision Science and Technology, Tokyo Institute of Technology* 402.
[19] Sugeng & Annisa Fitria, 'Legal Protection of E-Commerce Consumers Through Privacy Data Security' (2020) 549 *Advances in Social Science, Education and Humanities Research* 281.
[20] Ibid, at 283.
[21] Godwin Udo, 'Privacy and security concerns as major barriers for e-commerce: a survey study' (2001) *College of Business Administration, University of Texas* 165.
[22] Ibid.
[23] Tsebetso Mapeshoane & Shaun Pather, 'The Adoption of E-Commerce in the Lesotho Tourism Industry' (2016) *The Electronic Journal of Information Systems in Developing Countries* 9.

instruments such as online shopping due to privacy concerns.[24] As a result, privacy and security concerns over online transactions are regarded to be the main reason why people hesitate to make use of e-commerce.[25]

1.2 **Research question**

How effective are Lesotho's cybersecurity laws in safeguarding data privacy and security within the e-commerce sector?

1.3 **Problem statement**

The growth of e-commerce in Lesotho has not been immense because of the absence of an e-commerce strategy and legislation that would propel e-commerce in Lesotho to greater heights.[26] Nevertheless, Lesotho has taken strides to aid the growth of e-commerce by formulating objectives in the Lesotho National Digital Transformation Strategy to augment e-commerce in the country.[27] On the contrary, the United Nations Conference on Trade and Development (UNCTAD) found that Lesotho has fallen short of its objectives[28] in digitizing the country.[29] Some of these objectives include the building of internet infrastructure, adoption of an e-commerce specific legislation and so on.[30]

It is vivid that due to the exponential growth of e-commerce, it is here to stay. Lesotho is no exception to the vast use of e-commerce especially during and post Covid-19

[24] Ibid 16.
[25] Ibid.
[26] United Nations Conference on Trade and Development, 'Lesotho Rapid e-trade Readiness Assessment' (2019) 6.
[27] Lesotho's National Digital Transformation Strategy: Agenda 2030, 7.
[28] National Digital Policy (2024) Ministry of Communication, Science, Technology and Innovation https://www.gov.ls/download/draft-national-digital-transformation-policy-2024/ Accessed 28th November 2024.
[29] Ibid 13. Some of the objectives apart from the building of telecommunications infrastructure include the adoption of a specific e-commerce legislation, policy and strategy. Lesotho however failed to reach these objectives.
[30] Ibid.

era.[31] However, limited internet access of 37% across the country and low connectivity[32] have resulted in the sluggish growth of e-commerce in Lesotho.[33]

Another reason that may impact the usage of e-commerce in Lesotho is that Basotho do not have full confidence in e-commerce.[34] The above standing shows that even though some Basotho make use of e-commerce, privacy of sensitive and personal information holds an integral part in consumers trusting e-commerce.[35]

Ntlatlapa's thesis further outlines that trust plays a significant role in consumers engaging in electronic transactions and using electronic money.[36] As a result, this components inevitably bring about issues of data privacy and data protection. Although the two terms may be used concurrently, they are however materially different. Data privacy denotes the overall storage, retention and access of information whilst prohibiting unauthorized access to the information.[37]

On the other hand, data protection encompasses a set of norms and policies that adopt a holistic approach to safeguarding consumer data.[38] It focuses on preserving the integrity of data by ensuring that it is not unlawfully altered or

---

[31] Karabo Nkolanyane, 'How e-commerce and digital platforms have changed the game for businesses through the pandemic' *Lesotho Times* (Maseru, 8th September 2021) https://lestimes.com/how-e-commerce-and-digital-platforms-have-changed-the-game-for-businesses-through-the-pandemic/ Accessed 9th November 2024.

[32] United Nations Trade and Development, 'Lesotho ready to channel its growth to go digital' (2019) Available at https://unctad.org/news/lesotho-ready-channel-its-growth-go-digital#:~:text=New%20report%20on%20Lesotho%20shows,performance%20and%20diversifying%20income%20sources. Accessed on 28th November 2024.

[33] Ibid.

[34] International Trade Administration, 'Lesotho- Country Commercial Guide' (2024) *U.S. Department of Commerce's International Trade Administration Website*. https://www.trade.gov/country-commercial-guide/lesotho-market-overview Accessed 28 November 2024.

[35] Mamots'eli Ntlatlapa. 'The Determinants of Mobile Money Adoption and Usage: The Case of Lesotho' (Masters thesis, University of the Free State 2017) 41.

[36] Ibid.

[37] Cameron Hashemi-Pour & Stephen Bigelow, 'What is Data Privacy?' date of publication of the document? https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy Accessed 26th November 2024.

[38] Lee Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) *Stockholm Institute for Scandinavian Law* 168.

manipulated.[39]Essentially, these mechanisms are put in place to prevent unauthorized third parties from distorting the content of this data.[40] Consequently, this study focuses on both these components as two distinct components of e-commerce.

Some people believe e-commerce is prone to both data protection (security) and data privacy invasions, while some continue to show their trust in it by continuing to use it.[41]

Budnitz further says that the fact that privacy and security of e-commerce users is regularly invaded, people who do not fully trust e-commerce have a point in not having full confidence electronic transactions.[42] Data privacy and security invasions may be in the form of hacking, phishing and online fraud and many other forms.[43]

The most recent data privacy invasion incident occurred in 2023 when INC Ransomware hacked the Central Bank of Lesotho and demanded ransom.[44] INC Ransomware as it is called, is a ransomware group that unlawfully gains access to information of corporations with the primary aim extorting money out of their victims.[45] Failure to comply with its demands may lead to exposure of such confidential information.[46]

The sudden hike in cyber invasions threatens both individuals and organizations and needs a robust defensive mechanism to combat this invasion threats.[47] Although

---

[39] Ibid.
[40] Christian Kabongo & Asa Asa, 'Factors Influencing E-Commerce Development: Implications for the Developing Countries' (2015) 1 *International Journal of Innovation and Economic Development* 3.
[41] Mark Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate' (1998) 49 *South Carolina Law Review* 874.
[42] Ibid.
[43] Maria Thuraisingham, 'Cybersecurity in Lesotho, Current Challenges and Future Opportunities' (2023) *Durban University of Technology* 12.
[44] Tokelo Khausela, 'CBL Speaks on Cyber Attack' *Lesotho Times* (Maseru, 13th Accessed 28th November 2024. February 2024) https://lestimes.com/cbl-speaks-on-cyber-attack/
[45] Cybereason Security Research Team, 'THREAT ALERT: INC Ransomware' (Cybereason Blog, 20 November 2023) https://www.cybereason.com/blog/threat-alert-inc-ransomware?hs_amp=true Accessed 20 December 2024.
[46] Ibid.
[47] Ibid.

privacy breaches in e-commerce are not as frequent as they are made out to be, the minimal frequency of invasions are enough to deter people from keeping their trust in electronic commerce.[48]

Due to the rapid technological changes, websites offering the buying and selling of services have turned into catalogs and have failed to prioritize consumer privacy, security and trust.[49] These online platforms include local retail platforms and cross-border platforms that operate in Lesotho that fail to comply with data retention and explicit consent for data use.[50]

Although each electronic platform or "online shops" creates its own regulations pertaining to consumers' data privacy and safety in online transactions, some platforms fail to adhere to these regulations.[51] Consequently, consumers become reluctant to entrust their personal information to such platforms.[52] It is for this very reason that this study focuses on the extent to which e-commerce laws in Lesotho impacts data privacy and security when effecting electronic transactions.

1.4 **Hypothesis**

The cyber security risks in Lesotho may be attributed to the absence of a comprehensive and effective e-commerce legislative framework as this absence aggravates distrust in e-commerce. Legislation formulates essential minimum requirements that have to be complied with for a safe use of e-commerce.

---

[48] Nidhi Singh *et al*, 'An analysis of consumer's trusting beliefs towards the use of e-commerce platforms' (2024) *Humanities & Social Sciences Communication* 2.
[49] Anuradha Reddy, 'A Study On Consumer Perceptions On Security, Privacy & Trust On E-Commerce Portals' (2012) 2 *Excel International Journal of Multidisciplinary Management Studies* 2.
[50] Global Encryption Coalition, 'Encrypt to Protect: Empowering Lesotho with Digital Security' (2024) https://www.globalencryption.org/2024/09/encrypt-to-protect-empowering-lesotho-with-digital-security-2024/ Accessed 28th November 2024.
[51] Ibid.
[52] Ibid.

Without e-commerce legislation, the possibility of daily data breaches as a result of the vast use electronic commerce has a likelihood of increasing. Consequently, this research shall demonstrate the correlation between the lack of a comprehensive and effective e-commerce legislation and the high privacy and security issues linked with electronic transactions in Lesotho.

1.5 **Aim of the study**

The aim of this research is to critically analyze the extent to which the current legislation protects data privacy and security in e-commerce.

1.6 **Objectives of the study**

a) To critically discuss the importance of an e-commerce legislation in relation to cybersecurity.
b) To evaluate the adequacy of current legislation in ensuring the right to privacy.
c) To scrutinize the effectiveness of the existing legislation in safeguarding the security of information.
d) To discuss the potential impact of the current e-commerce legislation on data breaches.

1.7 **Research methodology**

The research employs a qualitative methodology in fact finding. The qualitative methodology will be achieved by the use of desk research. Within the desk research, sources such as legislation, textbooks, journal articles, case law and reliable internet websites are used. The abovementioned sources shall be subjected to a comprehensive and critical analysis with the ultimate aim of determining the extent to which the Lesotho e-commerce legislation contributes to data privacy and security breaches of e-commerce users.

1.8 **Literature review**

A study by Anuradha Reddy explained a role played by the understanding of consumers with regard to privacy and security of their data when engaging in e-commerce.[53] Reddy outlined that consumers are growing increasingly reluctant to engage in electronic transactions due to fear of their sensitive information being disclosed to unauthorized people. This study by Reddy goes hand in hand with that of Atienza *et al*.[54] The subsequent study looked into consumer perspective regarding privacy and security whilst simultaneously explaining the critical role played by privacy and security in the success of e-commerce.[55] However, it is important to note that both these studies did not go into the consumer trust in the ever changing world of technological advancements.

A study by Budnitz has shown that due to the dynamic and ever changing e-commerce, concerns on consumer privacy have been on a steady rise.[56] Budnitz's research greatly discloses that although entities have come up with their own regulations for purposes of consumer privacy, these measures have proven to not be enough since they are not binding.[57] Bunditz went on to say that due to the unbinding nature of the self-regulations founded by e-commerce entities, a comprehensive legislation on privacy in electronic transactions would greatly help protect consumer data since legislation has a binding effect.[58]

In amplifying the importance of keeping consumer data private, Budnitz says that privacy ought to be understood as a constitutional fundamental right that ought to be protected by enacting comprehensive e-commerce legislations.[59] Although Budnitz

---

[53] Anuradha Reddy, 'A Study On Consumer Perceptions On Security, Privacy & Trust On E-Commerce Portals' (2012) 2 *Excel International Journal of Multidisciplinary Management Studies* 2.
[54] Audie Atienza *et al,* 'Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings from a Mixed-methods study' (2015) *Journal of Health Communication* 673.
[55] Ibid.
[56] Mark Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate' (1998) 49 *South Carolina Law Review* 849.
[57] Ibid.
[58] Ibid.
[59] Ibid.

touched on the failures of self-regulation in the electronic commerce world and the importance e-commerce laws, he failed to comprehensively discuss the impact that the absence or presence of incomprehensive e-commerce laws may have on consumer privacy and security.

A research authored by Miyazaki and Fernandez[60] discussed the importance of online service providers disclosing their privacy and security policies to consumers. Their study focused more on how the disclosure of privacy and security policies may inspire trust and confidence of consumers more so in this era where privacy breaches are high.[61] Goldfarb and Tucker agree with this standing by stipulating that in the era of privacy and security breaches, online retailers ought to improve and alter how they disclose their own privacy measures to consumers.[62]

The reason behind this is to allay the consumers' concerns regarding their data privacy when entering into online transactions. Trivedi & Yadav's research paper states that disclosing privacy and security measures to consumers is not merely the fulfilment of regulatory requirements but also acts as a significant ingredient in inspiring consumer trust and confidence.[63] Much emphasis has been put on how online retailers may impart consumer confidence in online transactions. This however led to the formation of a gap as to how the absence of legislation affects consumer privacy and security in online transactions.

An article by Belanger *et al* emphasized the value of trust in e-commerce.[64] The article states that although it is easy to say trust only impacts consumers, that is not the case because the issue of trust is two-fold. Trust does not only affect consumer behavior but

[60] Anthony Miyazaki & Ana Fernandez, 'Internet Privacy and Security: An Examination of Online Retailer Disclosures' (2000) 19 *Journal of Public Policy & Marketing* 54.
[61] Ibid.
[62] Avi Goldfarb & Catherine Tucker, 'Privacy and Innovation' (2011) *National Bureau of Economic Research* 66.
[63] Shrawan Trivedi & Mohit Yadav, 'Repurchase intentions in Y generation: mediation of trust and e-satisfaction' (2020) 38 *Marketing Intelligence & Planning* 403.
[64] Belanger *et al,* 'Trustworthiness in electronic commerce: the role of privacy, security and site attributes' (2002) *Journal of Strategic Information Systems* 245.

it also affects performance of businesses. They say this because if too many consumers do not have confidence in a brand, the chances of success for that internet brand shall continue to decline.[65] This standing is supported by that of Yousefi & Nasiripour. Their article states that privacy and security are essential pillars that may make or break customer trust in electronic services even in big institutions such as banks.[66] They went on to outline that e-services have to be accompanied by privacy and security measures of high quality so as to draw in more consumers.[67]

Privacy offered by electronic service providers is regarded to be so key in e-service quality. This is because privacy concerns have a likelihood of negatively affecting the satisfaction and loyalty of consumers the e-services rendered.[68] Although these journal articles profoundly speak to how consumer trust may be affected by privacy and security factors of their data, they leave a gap as to the extent to which legislation may affect consumer confidence in e-services.

The article by Goga and Paelo focused more on the impact of not regulating e-commerce in South Africa in areas such as competition, taxation, industrial policy and trade.[69] They state that e-commerce platform giants such as Amazon, Alibaba, Takealot and so on possess huge amounts of market power. [70] According to them, network effects and economies of scale allow these brands to overwhelm other smaller e-commerce brands and this ultimately distort competition.[71]

---

[65] France Belanger *et al,* 'Trustworthiness in electronic commerce: the role of privacy, security, and site attributes' (2002) *Journal of Strategic Information systems* 251.
[66] Neda Yousefi & Ashkan Nasiripour, 'A proposed model of e-trust for electronic banking' (2015) *Management Science Letters* 1029.
[67] Ibid.
[68] Rami Al-dweeri *et al,* 'The Impact of E-Service Quality and E-Loyalty on Online Shopping: Moderating Effect of E-Satisfaction and E-Trust' (2017) 9 *International Journal of Marketing Studies* 98.
[69] Sha'ista Goga & Anthea Paelo, 'Issues in the Regulation and Policy Surrounding E-commerce in South Africa' (2019) *Centre for Competition, Regulation and Economic Development* 1.
[70] Ibid.
[71] Ibid.

They go on to say that this issue of dominating other e-commerce brands has been remedied in Europe whereby the European Commission fined the tech giant, Google, for mistreating its dominance in "search advertising" which is regarded as a crucial element of e-commerce.[72] Furthermore, their article states that the lack of e-commerce regulation leads to unfair competition especially in competition and tax matters. This study too left a gap by not going into how the lack of e-commerce regulation impacts consumer privacy and security.

Barkatullah's research was a comparative one whereby the author weighed the United States of America's self-regulation of e-commerce regulation against Europe's regulation of e-commerce by statute.[73] He says that the United States tends to allow businesses that offer e-commerce to formulate their own self-regulation rules as this enables the growth of e-commerce. This is contrasted with the European Union one by saying that Europe advocates for legislation as an e-commerce regulator because laws are enforceable and they help to encourage consumer trust.[74]

The study continues to show that albeit self-regulation may benefit consumer security, it is nonetheless non-effective without suitable oversight. One of his recommendations were that countries may merge the US self-regulation and the European legislative e-commerce oversight so as to tailor-make these regulations for each country.[75] The study to some extent makes reference to how significant legislation is regarding e-commerce. However, it somehow leaves a gap as to the degree to which the absence of legislation regulating e-commerce affects trust of consumers.

The investigation by Kobane managed to shed some needed light into Lesotho's e-commerce landscape as the study centered around elements that contribute to the acceptance of e-commerce in Lesotho. It is stated that Technology Acceptance Model

[72] Ibid.
[73] Djumadi Barkatullah, 'Does self-regulation provide legal protection and security to e-commerce consumers? (2018) *Electronic Commerce Research and Applications* 3.
[74] Ibid.
[75] Ibid.

(TAM) was utilized so as to identify some key pillars that encourage and discourage e-commerce in Lesotho.[76] Through the survey of data collected online from 275 people, it was revealed that factors such as convenience, accessibility and dependability were the factors that encouraged e-commerce growth in Lesotho as per the Confirmatory Factor Analysis (CFA).[77]

However, issues such as poor infrastructure, trust issues and lack of e-commerce laws are what hinder e-commerce adoption.[78] As such, it was revealed that e-commerce laws must be formulated to foster a way for secure, safe and accessible electronic transactions to all. Although the value of e-commerce legislation is echoed in the research, the article however still allows for further exploration into the exact impact of the lack of legislation on consumer trust in e-commerce.

1.9 **Justification of the study**

The swift growth of e-commerce globally and particularly in Lesotho has drastically changed the manner in which businesses are conducted and the manner in which consumers enter into transactions. E-commerce has given rise to a plethora of benefits as stated above. However, as stated previously, e-commerce comes with its own disadvantages such as concerns over data privacy and security when engaging in transactions.

E-commerce is accompanied by personal and sensitive information such as payment details being exchanged, this then means that keeping electronic transactions secure remains a grave concern. As such, the absence of a comprehensive e-commerce legislation creates *lacunae* in keeping electronic transactions secure for its users.

---

[76] Molelekeng Kobane, 'Testing an Adapted Technology Acceptance Model (TAM) for Factors Influencing E-Commerce Adoption: A Lesotho Consumers' Perspective' (2023) *American Journal of Economics and Business Innovation (AJEBI)* 158.
[77] Ibid.
[78] Ibid.

The absence of an e-commerce legislation may negatively affect data privacy and security when consumers get into online transactions. This may therefore leave consumers and businesses alike open to cyberattacks, data breaches and unlawful usage of private information. The absence of e-commerce legislation may give rise to e-commerce platforms operating in substandard security measures that put sensitive data of consumers at risk. Ultimately, the lack of a comprehensive law may mean that e-commerce platforms may not account for data breaches and lapse in security.

The justification of this study is anchored in critically analyzing the relationship between a comprehensive e-commerce legislation and privacy and security of data in electronic transactions. By probing into the impact of the absence of the law, this study shall provide a clear understanding on how a comprehensive e-commerce legislation can promote data protection and security in electronic transactions. The outcomes of this study will help in carving a way for legislative promulgation so as to protect data and ensure security in electronic transactions.

1.10 **Significance of the study**

This research is going to tend to an urgent gap in comprehending how the absence of a comprehensive e-commerce legislation affects data privacy and security when executing electronic transactions. Data privacy and security has grown into a critical issue in the present day due to consumers sharing their private and sensitive information online.

So, this puts data privacy and security at the pinnacle. Without a comprehensive legal intervention, consumers are left prone to cyberattacks and data breaches that may result in identity theft and other crimes caused by the unlawful misuse of personal information of customers. Consequently, this dissertation shall provide invaluable insight into the risks and dangers posed by this current legislative void. Further, this study looks into the necessity of the enacting and promulgating comprehensive e-commerce laws that prioritize data privacy and security in electronic transactions.

Moreover, this study is both relevant and significant to policymakers, policy markets and businesses at large. The facts to be uncovered by this study will provide a conduit for the policymakers of Lesotho to formulate a comprehensive e-commerce law that shall benefit and protect consumers. This study also contributes to existing literature into how best the digital environment of Lesotho may be enhanced so as to prioritize consumer safety when executing electronic transactions. When consumer privacy and security is guaranteed and enforced by an Act of parliament, this may have a result of both growing the economy of Lesotho and growing e-commerce in Lesotho due to the increased faith and trust into e-commerce.

1.11 Chapter outline

1.11.1 Chapter one: Introduction of the study

This chapter contains an overview of the contents of the dissertation being; problem statement, the aims of the dissertation, the methodology to be used for fact finding, significance of the study and its justification. Moreover, this chapter also contains existing literature around the subject of electronic commerce.

1.11.2 Chapter two: Critical discussion of the significance of e-commerce legislation

This chapter comprises of a discussion and critical analysis of the significance of electronic commerce legislation *vis a vis* data privacy and security in Lesotho. First, this chapter defines privacy and security in the electronic commerce environment. Secondly, the chapter critically discusses the significance of data privacy and security when engaging in electronic transactions.

1.11.3 Chapter three: Outlining the causes of data breaches: The impact of the absence of legislation into the breaches

This chapter looks into and explains the causes of data breaches in Lesotho. Also, the chapter reviews whether there are available laws in Lesotho that protect e-commerce. If the answer to the above review is in the affirmative, this chapter has a critical analysis

as to whether there is a nexus between data breaches and the adequacy of such laws. The critical analysis sums up whether the suspected absence of legislation contributes to data breaches.

1.11.4 **Chapter four: Comparison of Lesotho to European Union on regulation of data privacy and security**

This chapter contains a comparative analysis of the Lesotho laws on e-commerce with General Data Protection Regulations (GDPR) 2018 that are applicable in the European Union. This is because the GDPR is a more recent data protection framework that assists in ascertaining whether the Lesotho laws offer adequate data protection in e-commerce.

1.11.5 **Chapter five: Conclusion and recommendations**

This chapter firstly sums up the contents in the previous chapters and then form a conclusion thereof. Lastly, consequent to the comparison in chapter four, this chapter explains the recommendations that may be implemented so as to make e-commerce safer for all users when engaging in electronic transactions in Lesotho.

2. Chapter two

The significance of e-commerce legislation

2.1 Introduction

The previous chapter has outlined the legal and policy issues that necessitate a deeper examination of Lesotho's cybersecurity laws in the context of e-commerce. This is because without comprehensive understanding of the weaknesses of Lesotho's cyberspace, it may be difficult to effectively solve these issues. As such, this chapter critically examines how important it is to safeguard the right to privacy in e-commerce along with data security (data protection). It shows how data protection makes trading over the internet seamless and safe for users.[1] As Chapter one indicates, among other benefits of e-commerce is that it provides a more convenient way of shopping.[2] Thus, people want to capitalize on these benefits provided by e-commerce. Furthermore, this chapter discusses the importance of data privacy in e-commerce. This is because the right to privacy of e-commerce users (consumers) is interrelated with data security that ought to be afforded to consumers when engaging in electronic transactions.

E-commerce businesses gather personal data of consumers for varying reasons such as processing sales transactions and to understand personal preferences of each consumer.[3] This helps businesses to tailor make their marketing strategies specifically for each client.[4] As such, maintaining strict data privacy amid high security concerns

[1] Aleksy Kwilinski *et al,* 'E-Commerce: Concept and Legal Regulation in Modern Economic Conditions' (2019) 22 *Journal of Legal, Ethical and Regulatory Issues* 5.
[2] Peter Swire, 'Trustwarp: The Importance of Legal Rules to Electronic Commerce and Privacy (2003) 54 *Hastings Law Journal* 847.
[3] Mindaugas Degutis *et al,* 'Consumers' Willingness to Disclose Their Personal Data in e-Commerce: A Reciprocity-based Social Exchange Perspective' (2023) *Journal of Retailing and Consumer Services* 2.
[4] Tyler Shanahan *et al,* 'Getting to know you: Social media personalization as a means of enhancing brand loyalty and perceived quality' (2029) *Journal of Retailing and Consumer Services* 57.

is of utmost importance.[5] This is because when data privacy guidelines are not complied with, this may lead to consumers losing trust in e-commerce.[6]

As both e-commerce and the internet continue to grow exponentially, there ought to be a legal framework that will more specifically regulate privacy and security in e-commerce. This is to enhance consumer safety and privacy when engaging in electronic transactions. Data protection in e-commerce ensures that trade over the internet (e-commerce) does not remain unchecked. This study therefore highlights the significance of an e-commerce legislation.

Many e-commerce users share their private information on the internet such as their personal identifiable information. Therefore, it is imperative to ensure and enhance the privacy and security of this sensitive information. For this reason, data protection mechanisms aid in the compliance thereof. A comprehensive legislation ensures a safe and secure digital environment for consumers by clearly setting the minimum threshold of privacy and security that the e-commerce platforms must abide by.[7]

2.2 **The importance of data privacy and security in electronic transactions**

Data privacy is defined as a state of controlling the storage, access and retention of sensitive information of consumers and prohibiting unauthorized access to such information.[8] On the other hand, security in relation to e-commerce is defined as a mechanism of data protection that prevents unauthorized third parties from altering and manipulating consumer data.[9] As such, given that data privacy and security are interrelated though are different terms, Nalla and Reddy opine that it is important for

[5] Muneer A *et al,* 'Data Privacy Issues and Possible Solutions in E-commerce' (2018) *Journal of Accounting and Marketing* 1.
[6] Ibid.
[7] Aleksy Kwilinski *et al,* 'E-Commerce: Concept and Legal Regulation in Modern Economic Conditions' (2019) 22 *Journal of Legal, Ethical and Regulatory Issues* 5.
[8] Cameron Hashemi-Pour & Stephen Bigelow, 'What is Data Privacy?' (TechTarget 18 July 2024) https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy Accessed 26th November 2024.
[9] Christian Kabongo & Asa Asa, 'Factors Influencing E-Commerce Development: Implications for the Developing Countries' (2015) 1 *International Journal of Innovation and Economic Development* 3.

data privacy and security to be upheld in electronic commerce because online businesses collect, process and store sensitive and personal information of their consumers.[10] It is therefore important to utilize both concepts so as to give consumer data the best possible protection. As such, e-commerce platforms ought to make use of modern databases that mitigate threats associated with data breaches and illegal access to personal information of consumers.[11]

Data breach entails any cybersecurity incident that threatens security of information through unauthorized third parties unlawfully gaining access to confidential information and personal data.[12] Data breach is distinct from mere unauthorized access of information in that data breaches result in exposing, stealing or unlawfully using such data whereas the latter merely entails entering a database without consent and without necessarily exposing or using such information.[13]

Examples of data breaches include ransomware, password guessing, phishing and many others.[14] These issues must be adequately dealt with to preserve consumer data whilst simultaneously growing e-commerce through stimulating the confidence of consumers in e-commerce. This signals the influence of data privacy and security because consumers mainly use e-commerce when they have confidence that their personal information is kept private and secure.

---

[10] Lakshmi Nalla & Vijay Reddy, 'Data Privacy and Security in E-commerce: Modern Database Solutions' (2023) 1 *International Journal of Advanced Engineering Technologies and Innovations* 248.
[11] Ibid.
[12] Matthew Kosinski, 'What is data breach?' https://www.ibm.com/think/topics/data-breach Accessed 16 December 2024.
[13] Dr. M Niranjanamurthy & Dr. Dharmendra Chahar, 'The Study of E-Commerce Security Issues and Solutions' (2013) 2 *International Journal of Advanced Research in Computer and Communication Engineering* 1.
[14] Big Commerce Team, 'Protect Your Customers' Data Against Ecommerce Data Breaches: Here's How (Why It's Important)' (2021) https://www.bigcommerce.com/articles/ecommerce/ecommerce-data-breaches/ Accessed 16 December 2024.

The United Nations Conference on Trade and Development (UNCTAD) outlines that the lack of security and trust are one of the impediments to e-commerce.[15] It further illustrates that these factors are some of the critical issues that Lesotho has to address in order to pave way for the overall growth of e-commerce.[16] As such, e-commerce businesses are investigating methods they would implement to lower privacy concerns that consumers have regarding e-commerce.[17] Businesses' ability to implement privacy policies may convince countless would-be consumers to trust and make use of e-commerce.[18] Trust in an e-commerce transactions is mainly anchored on whether consumers think a transaction is risky or not.[19]

Chellappa asserts that the risk factor comes from their concerns of the privacy and security of the transactions they make electronically.[20] As a result, this shows that if consumers believe that their transactions are prone to privacy and security risks, their chances of participating in such transactions shall be low.[21] Thereby negatively affecting trust and the overall growth of e-commerce because less people are going to be drawn to use online transactions.

2.3 **The history behind the emergence of e-commerce legislation**

During its early days, the regulation of e-commerce was mainly anchored on e-commerce platforms creating their own rules so as to govern e-commerce,[22] thereby utilizing self-regulation. Barkatullah's research was a comparative one whereby he

---

[15] United Nations Conference on Trade and Development, *Unlocking the Potential of E-Commerce in Developing Countries* (UNCTAD 2015) 6.
[16] Ibid.
[17] Thomas van Dyke *et al,* 'The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce' (2007) 17 *Electronic Markets* 68.
[18] Bob Tedeschi, 'E-Commerce Report; Some online sellers are hiring prominent auditors to verify their privacy policies and increase trust.' *New York Times* (18 September 2000) 12. https://www.nytimes/2000/09/18/business/e-commerce-report-some-online-sellers-are-hiring-prominent-auditors-verify-their.html Accessed 22 December 2024.
[19] Ramnath Chellappa, 'Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security' *Goizueta Business School, Emory University Atlanta* 3.
[20] Ibid.
[21] Ibid.
[22] Peter Swire, 'Markets, Self-Regulation, and Government Enforcement in the Protection of Personal information' (1997) *US Department of Commerce* 3.

weighed the United States of America's (USA) self-regulation of e-commerce against European Union's (EU) regulation of e-commerce by statute.[23] Accordingly, the USA tends to allow businesses that offer e-commerce to formulate their own self-regulation rules as this enables the growth of innovation within e-commerce.[24] The research contrasted this standing with the EU one by stating that EU advocates for legislation as an e-commerce regulator because laws are enforceable and they help to encourage consumer trust.[25]

The study continues to show that albeit self-regulation may benefit consumer security, it is nonetheless non-effective without governmental oversight through legislation.[26] Legislation is important because without it, consumers may be reluctant to make use of electronic commerce because of fear for the privacy of their data.[27] Statutory oversight therefore grants a two-pronged benefit in that by preserving the privacy of consumer data, more consumers will be confident in e-commerce and utilize it.[28]

Thereby online businesses making large amounts of profit due to an increased number of e-commerce users.[29] One of his recommendations were that countries may merge the USA self-regulation and the EU legislative e-commerce oversight to tailor-make these regulations for each country.[30]

Although e-commerce came into being in 1971,[31] it was only in 1996 to 2001 that it was subjected to regulation and many e-commerce vendors subsequently got skeptical

[23] Djumadi Barkatullah, 'Does self-regulation provide legal protection and security to e-commerce consumers? (2018) *Electronic Commerce Research and Applications* 4.
[24] Ibid.
[25] Ibid.
[26] Mark Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate' (1998) 49 *South Carolina Law Review* 848.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid, 20.
[31] Ben Kazinik, 'The History of e-Commerce- How it All Started' (28 March 2024) https://www.mayple.com/blog/history-of-ecommerce Accessed 17 October 2024

about the adoption of e-commerce legislation.[32] They viewed self-regulation as the best approach to e-commerce regulation as it gave them freedom to establish their own rules for e-commerce.[33] Swire remarks that the e-commerce vendors saw legislation as an innovation inhibitor and disruptor of free market.[34]

This was because legislation would come up with its own foreign mandatory and preconditioned practices.[35] The reason behind the hostility towards the upcoming legislation was as a result that e-commerce was already in existence and being practiced before the coming into effect of the law. Meaning that they would have to abandon their own way of doing business and subsequently adopt new practices that would be within the confines of legislation. Accordingly, the vendors felt that legislation would disrupt their way of doing business and would greatly hamper their innovation in the course of business. They had this hostility towards legislation because legislation has a propensity of inhibiting innovation because technology develops at a swifter rate than legislation.[36]

Scholars like Swire regard the USA as one of the pioneers of e-commerce legislation.[37] This is because it is one of the first jurisdictions to recognize the need for a comprehensive legislation to govern electronic transactions.[38] Notwithstanding the foregoing, although the USA initially advocated for self-regulation, it was the first jurisdiction to enact a law aimed at regulating e-commerce.[39]

---

[32] Peter Swire, 'Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy' (2003) 54 *Hastings Law Journal* 860.
[33] Ibid.
[34] Ibid.
[35] Peter Swire & Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (The Brookings Institution Press 1998) 78.
[36] 'Matsepo Kulehile, 'An analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and the SADC region' (Doctor of Philosophy thesis, University of Cape Town 2017) 72.
[37] Peter Swire, 'The Surprising Virtues of the New Financial Privacy Law' (2002) 86 *Minnesota Law Review* 115
[38] Ibid.
[39] Communications Decency Act (CDA) 1996, section 30.

This is in contrast with the EU as it only passed legislation in 2000.[40] Before the coming into force of legislation for the first time in Utah, USA, e-commerce vendors such as websites were given an ultimatum by the Federal Trade Commission (FTC) to prioritize privacy and security of consumers, failing which, a binding legislation would be adopted.[41] Due to exerted pressure of the impending legislation, the number of websites that incorporated the use of privacy policies rose from 14% to 66% in 1999 and subsequently to 88% in 2000.[42] This therefore threatened self-regulation of the industry hence the website operators had to take action to prevent legislation from coming into force.

In order to continue self-regulation of e-commerce, the e-commerce industry formulated some mechanisms that would be distinguishable to consumers as to which e-commerce websites prioritized privacy policies. They did this by announcing the use of web seal programs.[43] The web seals would be displayed on websites only by the consent of web seal programs if they (web seal programs) were satisfied that such websites satisfied the minimum privacy requirements.[44]

As such, the web seal programs would then act as privacy enforcers in instances where the websites contracted to them breached the agreed privacy requirements. By undergoing all these efforts, the website operators sought to keep the implementation of legislation at bay and hoped to continue with self-regulation. However, the ambition of continuing with self-regulation would not hold on for long as the Gramm-Leach-Bliley Act[45] was formed in 1999 in USA to regulate e-commerce. Its rationale was to improve aspects of privacy and security of personal information of customers.[46]

---

[40] Directive 2000/31/EC on Electronic Commerce [2000] OJ L178/1.
[41] Swire, supra note 37, at 122.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Financial Services Modernization Act 1993.
[46] https://policies.vpfa.fsu.edu/policies-and-procedures/technology/gramm-leach-bliley-act-glb-policy Accessed 22 November 2024.

Although one may assume that the swift growth of e-commerce *ex facie* demands the legislator to enact e-commerce laws, some authors however argue that new legislation is not necessary as existing laws may still be sufficient to resolve problems.[47] Mik illustrates that new laws that focus on e-commerce may only be formulated when there is a novel legal problem and also when it has been confirmed that the existing legal principles such as law of contract, are unable to resolve the current problems.[48] He says that *ex ante* legislation is incapable of addressing technological problems with certainty.[49] Bick supports this view by saying that the internet is evolving at an alarming rate, so it would be a mistake to enact laws on the current state of the internet.[50] The author further argues that in this instances the adaptation of existing laws and precedent would suffice in solving modern day e-commerce problems.[51] However, Mik concedes that at times e-commerce and internet progress may end up risking public safety and privacy, so in those instances, *ex ante* regulation intervention is warranted.[52] Therefore, it is justified for an e-commerce legislation to be formulated as e-commerce is evolving at an alarming rate that risks consumer privacy.

The United Nations Commission on International Trade Law (UNCITRAL) was the first international body established by the United Nations General Assembly to enable and facilitate e-commerce.[53] It drafted a legal framework titled Model Law on Electronic Commerce (MLEC). Its rationale is to provide member states with guiding principles on how to best draft legislation that incorporates legally acceptable rules for e-commerce regulation.[54] The coming into force of the MLEC ensured that contractual

[47] Eliza Mik, 'E-Commerce Regulation: Necessity, Futility, Disconnect' (2013) *First International Conference on Technologies and Law* 7.
[48] Ibid.
[49] Ibid.
[50] Jonathan Bick, 'Why Should the Internet Be Any Different?' (1998) 19 *Pace Law Review* 52.
[51] Ibid.
[52] Ibid 26.
[53] United Nations Commission on International Trade Law, 'UNCITRAL Model Law on Electronic Commerce' (1996) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce Accessed 23 November 2024.
[54] Ibid.

agreements done on paper and electronically are treated equally by e-commerce users as both are on equal footing.[55]

It ensured predictability of treatment in terms of information that is in the form of a data message and that is passed by conventional means like paper.[56] Thereby ensuring that information and agreements are not denied validity and/or enforceability solely for the fact that such information is in the form of a data message.[57] As a result, the MLEC entails that the common law requirements for validity of a contract done by conventional means shall apply to contracts concluded electronically.[58] This means that electronic transactions (contracts) are afforded the same treatment as conventional transactions (contracts) as both are placed on equal footing.

2.4 **The value of legislation in e-commerce**

John Austin is one of the very first jurists of positive law. He defined law as a command of a sovereign backed by a sanction that is enforced by the state.[59] Bingham agrees with this definition by outlining that legislation is essentially municipal law.[60] He defines municipal law as a collection of rules passed by a supreme power so as to govern civil conduct by defining what is right and prohibiting what is wrong.[61] Thus, the legislature is essentially the superior body that lays down a set of rules that define what is wrong and right and provides a punishment if people do what is prescribed as wrong. This is reminiscent of contemporary laws because they define the wrongs and right and also provide a punishment that follows wrong doing.[62]

---

[55] UNCITRAL Model Law on Electronic Commerce 1996, Article 5.
[56] Ibid, Article 5 *bis.*
[57] Jeff Dodd & James Hernandez, 'Contracting in Cyberspace' (1998) *Computer Law Review and Technology Journal* 10.
[58] Roberto Rosas, 'Comparative Study of the Formation of Electronic Contracts in American Law with References to International Law' (2006) 46 *Indian Journal of International Law* 332.
[59] John Murray & Albemarle Street, *Lectures on Jurisprudence* (Spottiswoode and Co 1880) xii.
[60] Joseph Bingham, 'What is the Law?' (1912) 11 *Michigan Law Review* 2.
[61] Ibid.
[62] Mahmood Ansari, 'Exploring the Link of Action to Justice: A Review' (2023) 17 *Asian Journal of Advanced Research and Reports* 147. Mahmood says law is concerned with penalizing and punishing wrongdoing. He further illustrates that as per the retribution theory, law looks back on to particular acts of wrongdoing and metes out a deserved punishment.

In the context of Lesotho, the Constitution as the supreme law of Lesotho,[63] empowers the parliament (National Assembly, Senate and the King)[64] as the body that shall have powers to formulate laws.[65] In taking Austin's theory into consideration, the parliament of Lesotho is the sovereign power that formulates sets of rules that determine what is right and wrong and provides punishment for doing wrong. The role played by the parliament is a critical one as through its obligation of enacting laws, it seeks to create an environment that promotes harmony while discouraging actions that may harm or disrupt other people. As such, it follows that an e-commerce legislation also plays a role of setting out standards that would help society to avoid harming and/or disrupting the lives or rights of other people.

With the rapid growth of e-commerce across all markets, there is a strong call for online businesses to maintain high levels of privacy standards in order to protect personal data of consumers.[66] As a result, it is of utmost importance for businesses to put in all measures of protecting personal data of consumers. That is, if there are rules and regulations put in place for online businesses to abide by in order to safeguard consumer data, they have to strictly comply with such rules. E-commerce compliance is defined as the adherence to rules and regulations that govern e-commerce activities in markets which online businesses operate in.[67]

As such, this entails that legislation sets the minimum standard that online businesses must comply with more so currently when privacy breaches are so high.[68] This therefore underpins the role played by legislation in terms of data privacy protection in e-commerce. By setting the minimum requirements for data privacy protection, it is

[63] Constitution of Lesotho 1993, section 2.
[64] Ibid, section 54.
[65] Ibid, section 70(1).
[66] Zlatan Moric *et al,* 'Protection of Personal Data in the Context of E-Commerce' (2024) *Journal of Cybersecurity and Privacy* 731.
[67] Karolina Lubowicka & Pawel Socha, 'Privacy Compliance in Ecommerce- A Comprehensive Guide' (2023) *Data Privacy & Security – GDPR* 23.
[68] Meirong Guo, 'A Comparative Study on Consumer Right to Privacy in E-Commerce' (Tokyo Institute of Technology 2012) 401.

easier to maintain that standard nationwide. This means that the enactment of legislation plays a critical role in binding e-commerce businesses to maintain the required privacy standards.

Just as Austin's positive theory suggests, non-compliance with the law ought to be followed by a sanction[69] to ensure future compliance and deter potential non-compliance with the law. As a result, legislation plays an essential role in keeping e-commerce businesses accountable for adhering to legislative standards.

Legislation that is specific to protecting consumer data plays a two-fold role; it protects sensitive data of consumers whilst also enabling the overall growth of e-commerce through instilling trust in consumers about how their personal information is to be managed in e-commerce.[70]

Thus when consumers are confident about the storage and protection of their data, e-commerce simultaneously grows as this has a likelihood of attracting more consumers. Although the emergence of e-commerce legislation in USA was met with resistance whereby it was cited that governments were putting regulations unnecessarily, the success of e-commerce legislation has however endured the test of time.[71] It achieved this by enabling e-commerce growth through inspiring consumer confidence on the privacy of personal information of consumers. This goes on to show the importance of legislation in that by guaranteeing privacy of personal information, e-commerce subsequently grows. Thereby satisfying both consumers and online businesses alike.

Africa is regarded to be a continent with one of the least data privacy legal frameworks as per Bygrave.[72] To combat this and maximize consumer privacy, Bygrave urges countries to comply with the Organization for Economic Cooperation and

[69] Ibid 20.
[70] Lillyana Jaller *et al,* 'The regulation of Digital Trade- Key Policies and International Trends' (2020) 1 *World Bank Group* 12.
[71] Peter Swire, 'Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy' (2003) 54 *Hastings Law Journal* 860.
[72] Lee Bygrave, 'Data Privacy Law: An International Perspective' (2014) *Oxford University Press* 197.

Development's (OECD) basic principles for data protection.[73] These principles include *inter alia* the collection limitation principle, use limitation principle, accountability principle and others.[74] The collection limitation principle entails that there should be a limit set for the collection of consumer data and that such data should be lawfully obtained through consent of the consumer.[75]

The use limitation principle outlines that businesses are strictly limited to using consumer data only for purposes that have been agreed upon with the consumer.[76] The accountability principle on the other hand outlines that online businesses shall be held responsible to comply with the set regulatory requirements.[77] This therefore highlights the significance of legislation in terms of guaranteeing privacy of consumers which in turn attracts more consumers and therefore enables e-commerce growth.

The United Nations Conference on Trade and Development (UNCTAD) states that the absence of legislation creates a lack of trust and fear of being scammed when engaging in e-commerce.[78] This therefore means that the regulation of e-commerce by legislation creates a sense of trust for consumers in e-commerce as a whole. Furthermore, the UNCTAD illustrates that there are four main regulatory requirements that create a comprehensive and effective legislation and these are: data protection laws, consumer protection laws, cybercrime legislation and electronic transactions laws.[79]

The inverse of this results in a law that fails to meet its primary objective of protecting consumer data. Kobane supports this assertion by the UNCTAD by stating that weak laws that fail to offer consumers tangible protection in cyberspaces also contribute to

[73] Ibid.
[74] Ibid.
[75] Jon Bing, 'The Council of Europe Convention of the OECD Guidelines on Data Protection' (1984) 5 *Michigan Journal of International Law* 277.
[76] Ibid, at 278.
[77] Ibid, at 282.
[78] United Nations Conference on Trade and Development, 'Lesotho Rapid eTrade Readiness Assessent' (2019) 2.
[79] Bingham supra note 61.

the lack of trust in e-commerce.[80] Therefore, this premise shows that an e-commerce legislation is an essential ingredient in fostering trust of consumers in e-commerce. This is due to the fact that legislation offers them a sense of security and protection against scammers.

Christian and Asa suggest that factors such as fraud and hacking are some of the leading issues of security concern in relation to the safety of e-commerce.[81] Fraud in the sense of e-commerce is defined as malevolently promoting goods and/or services with the sole intent of unlawfully and deceptively acquiring personal information of consumers.[82] Fraud distorts e-commerce by creating an unfair competition in advertising.[83]

This is achieved by providing consumers with bogus, misleading information that may impel them to make bad decisions such as providing their sensitive information to third parties.[84] Furthermore, hacking on the other hand is unauthorized access of consumer data which may include theft of such sensitive data of consumers.[85] Hacking may take forms of identity theft where a hacker unlawfully uses a genuine information of a consumer.[86]

Online businesses are normally to blame for data breaches as their data storages are prone to hacking and open doors to sensitive data theft.[87] These storage systems are susceptible to unauthorized entry due to the lack of awareness on hacking and poor

[80] Molelekeng Kobane, 'Testing an Adapted Technology Acceptance Model (TAM) for Factors Influencing E-Commerce Adoption: A Lesotho Consumers' Perspective' 2023 (2) *American Journal of Economics and Business Innovation (AJEBI)* 160.
[81] Christian Kabango & Asa Asa, 'Factors Influencing E-Commerce Development: Implications for the Developing Countries' (2015) *International Journal of Innovation and Economic Development* 66.
[82] Haiqin Weng *et al,* 'Online E-Commerce Fraud: A Large-scale Detection and Analysis' (2018) *IEEE 34th International Conference on Data Engineering (ICDE)* 1.
[83] Ibid.
[84] Ibid.
[85] Sumit Badotra & Amit Sundas, 'A Systemic Review on Security of E-Commerce Systems' (2021) *International Journal of Applied Science and Engineering* 6.
[86] Ibid.
[87] Omid Bigdeli *et al,* 'Barriers of Online Shopping in Developing Countries: Case Study of Iran' (2009) *IADIS Multi Conference on Computer Science and Information Systems* 5.

security of these storages.[88] As such, Jaller *et al* outline that an e-commerce and cybersecurity legislation(s) are crucial in promoting trust in the digital markets.[89] They continue to explain that data breaches endanger the private information of consumers. This may result in a substantial decline of e-commerce as consumers would be realizing that their personal information is vulnerable to unauthorized access.[90] Legislation is therefore important in providing guidelines as to how to securely process consumer information and prevent it from outside attacks.[91]

After data privacy, an important aspect of legislation governing e-commerce is data security. This aspect of legislation protects the integrity of consumer data from unauthorized alteration and manipulation.[92] Data security is an important pillar of data protection as its failure affects how consumers interact with businesses as data security affects consumers directly.[93]

However, Ackerman and Davis highlight that security is a major concern for consumers and businesses alike.[94] Consumers fear interception of their financial data while businesses fear financial losses from data breaches along with those occasioned by bad publicity.[95] This shows how critical security is in e-commerce. Therefore, businesses ought to invest in access control mechanisms and authentication protocols to protect consumer data. These measures aid in preventing unauthorized access and subsequent modification of confidential information.[96] Thereby ensuring the integrity of such

[88] Eric Cole, *Hackers Beware* (1st edn New Riders Publishing 2001) 11.
[89] Swire, supra note 37, at 28.
[90] Ibid.
[91] Ibid.
[92] Kabongo & Asa, *supra* note 9.
[93] Niranjanamurthy M & Dr. Dharmendra Chahar, 'The Study of E-Commerce Security Issues and Solutions' (2013) 2 *International Journal of Advanced Research in Computer and Communication Engineering* 1.
[94] Mark Ackerman & Donald Davis Jr, 'Privacy and Security Issues in E-Commerce' (2003) *New Economy Handbook* 6.
[95] Ibid.
[96] Lakshmi Nalla & Vijay Reddy, 'Data Privacy and Security in E-commerce: Modern Database Solutions' (2023) 1 *International Journal of Advanced Engineering Technologies and Innovations* 250.

data.[97] As such, employment of organizational policies along with modern technology are apt in mitigating data breaches and enhancing security.[98]

Having a comprehensive legislation that tackles all contemporary e-commerce problems has numerous benefits. The most important reason of having an electronic commerce legislation as stated above is the ability of legislation to create an environment suitable for the growth of e-commerce.[99] Legislation is able to achieve this by putting in place standards that online shops have to comply with. This is enough to instill trust and confidence in the privacy and security of services offered by online retailers.[100]

2.5 **Conclusion**

It can safely be concluded that trust, privacy and security are essential aspects of e-commerce that cannot be ignored, hence the need for legislation to enhance data protection. This therefore shows that an e-commerce legislation is crucial as it is the one that enhances privacy and security in online transactions and e-commerce as a whole. The benefit of data protection regulation through legislation acts in a two-fold manner as previously stated in that legislation helps in protecting personal data of consumers and also increases the trust of consumers in e-commerce.[101]

This increased trust subsequently translates to e-commerce growth due to high consumer retention as a result of being confident in e-commerce.[102] Consequently, it has been proven that legislation is an invaluable tool in e-commerce as it also aids in the overall growth of e-commerce. Having unpacked the origins of the legislative framework on e-commerce, it is therefore warranted to turn to the causes of data breaches in Lesotho along with assessing the efficacy of the legislation.

---

[97] Ibid.
[98] Ackerman and Davis Jr, *supra* note 96, at 11.
[99] Swire, supra note 37.
[100] Ibid.
[101] Supra note 18.
[102] Se-Hak Chun, 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability' (2019) *Sustainability'* 4.

3. Chapter three

Investigating the causes of data breaches and the role of the e-commerce legal framework in Lesotho

3.1 Introduction

There is a rise of privacy and security threats in e-commerce due to the swift upsurge of the internet and e-commerce.[1] This is because as the internet grows concurrently with e-commerce, illegal and unlawful cyber activities also rise. The evolution of e-commerce means that electronic commerce has moved from its primitive state of basic virtual storefronts to the current state where it incorporates various technologies such as mobile applications and artificial intelligence.[2]

As such, the vast use of e-commerce means that it is even used by consumers who are not tech-savvy, and this makes them prone to data breaches. Cybercriminals may therefore take advantage of this state and threaten privacy and security of such consumers' data when they are engaging in electronic transaction.[3] Therefore, the lack of technological insight, along with other factors, contribute to some of the causes of e-commerce data breaches.

3.2 Causes of data breaches in Lesotho

The regulation of the e-commerce sector ought to be robust so as to ensure the privacy of consumers when engaging in electronic transactions.[4] This is important for all countries including Lesotho because a stringent legal framework may mitigate the growing rates of e-commerce data breaches.[5] According to Moric and others, stringent e-commerce regulations enable greater levels of scrutiny of e-commerce businesses so

[1] Ruchi and others, 'Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning' (2024) *IGI Global* 501.
[2] Ibid, 502.
[3] Ibid.
[4] Djumadi Barkatullah, 'Does self-regulation provide legal protection and security to e-commerce consumers?' (2018) *Electronic Commerce Research and Applications* 4.
[5] Zlatan Moric and others, 'Protection of Personal Data in the Context of Ecommerce' (2024) 4 *Journal of Cybersecurity and Privacy* 732.

as to protect consumer data.[6] Also, having strong enforcement mechanisms can assist in making stringent legislation even more effective. As such, in their article on data privacy in Africa, Prinsloo and Kaliisa pointed out Lesotho and other African countries such as Botswana and Angola as having enacted data protection legislations but lack enforcement.[7] Showing that enforcement is a critical ingredient in making legislation effective. Thus, legislation devoid of strong enforcement contributes to data breaches.

The lack of legislation or the insufficiency of legislation is regarded to be one of the biggest causes and threats to consumer data protection.[8] This is because legislation is required to protect consumers when engaging in electronic transactions.[9] It achieves this by providing at least minimal guarantees for data protection.[10] Furthermore, inadequate legislation fails to combat issues such as fraudulent and deceptive acts that mislead consumers when engaging in electronic transactions.[11]

This therefore threatens the safety of consumers when navigating the cyberspace. Some of the contributors that render e-commerce laws inadequate is the lack of legislation to address emerging data protection threats in the current age and/or lack of enforcement of legislation. This is because failure to address these emerging issues render the e-commerce laws obsolete hence they fail to grant consumers with the much needed protection in the cyberspace.[12] Consequently, the ineffectiveness of legislation cause e-commerce breaches by failing to provide consumers with requisite protection. It is for this reason that criminals continue to find ingenious ways to maneuver around the guarantees provided by legislation.

---

[6] Ibid, note 752.
[7] Paul Prinsloo & Rogers Kaliisa, 'Data Privacy on the African Continent: Opportunities, Challenges and Implications for Learning Analytics' (2022) *British Journal of Educational Technology* 903.
[8] Randy Marchany and Joseph Tront, 'E-Commerce Security Issues' (2002) *Proceedings of the 35th Hawaii International Conference on System Sciences – 2000* 6.
[9] Mark Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate' (1998) 49 *South Carolina Law Review* 877.
[10] Ibid.
[11] Dilshad Shaik, 'Consumer Protection in E-Commerce: A Legal and Compliance Framework in the Digital Market' (2020) 549 *Advances in Social Science, Education and Humanities Research* 19.
[12] Ibid, note 22.

Data breaches in the e-commerce realm may take numerous forms in Lesotho as previously stated. The first form is phishing. Greco *et al* defines it as a method that entails using emails, phone calls and fraudulent websites in order to steal personal information of consumers.[13] Phishing involves deception whereby hackers disguise communication modes as legitimate notifications coming from reputable sources so as to trick consumers into providing their private and sensitive data.[14]

Data breaches in Lesotho may also take the form of malware and ransomware. Malware and ransomware are a type of computer virus that impairs a victim's computer system and subsequently denies the original owner access to the information on the computer system.[15] This forms of data breach work by shutting out original owners from accessing data on the computer until they pay a stipulated ransom with no guarantee of regaining access.[16] The Central Bank of Lesotho is the most recent body corporate to fall victim to malware and ransomware in Lesotho.[17]

Data breaches are also caused by insufficient cyber security knowledge and limited cyber skills on the part of consumers.[18] This is because when consumers lacking in e-commerce skills use certain networks, such consumers may be oblivious to some inconspicuous data threats.[19] This may therefore impede them from successfully completing their electronic transactions safely. Thereby falling victims to cyber criminals. The benefit of adequate knowledge and skills of the cyberspace stems from

---

[13] Francesco Greco *et al*, 'Explaining Phishing Attacks: An XAI Approach to Enhance User Awareness and Trust' (2023) *CEUR Workshop Proceedings* 1.
[14] Annie Laukaitis, 'Building Strong Ecommerce WEBSITE security to Combat Online Attacks' (2024) https://www.bigcommerce.co.uk/articles/ecommerce/ecommerce-website-security/ Accessed 9 December 2024.
[15] Jamie Pont and others, 'Why Current Statistical Approaches to Ransomware Detection Fail' (2020) *Kent Academic Repository* 1.
[16] Ibid 14.
[17] Tokelo Khausela, 'CBL Speaks on Cyber Attack' *Lesotho Times* (Maseru, 13th Accessed 28th November 2024. February 2024) https://lestimes.com/cbl-speaks-on-cyber-attack/. This shows that it matters not whether it is a natural person or a juristic person involved, data breaches may affect anyone (any person) at any time.

[18] Xiang Liu and Others, 'Cyber security threats: A never-ending Challenge for E-Commerce' (2022) *Frontiers of Psychology* 5.
[19] Ibid.

the fact that knowledge and skills help to equip consumes with necessary information that that may help them avoid cyber threats.[20] As a result, due to the lack of the minimum knowledge and skills, consumers are unable to protect themselves against cyber criminals who possess high knowledge of the computer networks.[21] Therefore, the lack of knowledge and skills remains one of the root causes of data breaches in e-commerce.[22]

Some of these security threats leading to data breaches that are caused by lack of awareness may take the form of shopping on unsecure websites, providing excessive personal information than necessary, leaving computers prone to viruses and so on.[23] As a result, this inadequate consumer awareness may leave consumers open to easy attacks in the cyberspace as this lack of awareness is one of the leading causes of data breaches. Maliehe outlines that all countries including Lesotho are enjoined to raise awareness so that e-commerce users gain the necessary education and awareness of the cyberspace to ensure safety when engaging in electronic transactions.[24]

However, although this is a crucial recommendation, awareness campaigns in Lesotho regarding cyber threats are virtually nonexistent. This therefore leaves many consumers with lacking important knowledge and awareness when traversing the cyber landscape.[25]

Moreover, data breaches may be attributed to e-commerce businesses failing to invest in infrastructure that would prevent or at least mitigate data breaches.[26] As such, when businesses commit to threat defense systems, this does not only protect consumer data

[20] Moti Zwiling and others, 'Cyber Security Awareness, Knowledge and Behavior: A comparative Study' (2020) *Journal of Computer Information Systems* 1.
[21] Ibid.
[22] Ibid.
[23] Ibid, 12.
[24] 'Mamotumi Maliehe, 'Cybercrime Legislation for Lesotho' (LLM thesis, University of Cape Town 2007) 55.
[25] Maria Thuraisingham, 'Cybersecurity in Lesotho: Current Challenges and Future Opportunities' (2023) *Durban University of Technology* 7.
[26] Se-Hak Chun, 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability' (2019) *Sustainability'* 4.

from breaches but it also enhances consumer retention as this increased protection may strengthen consumer trust in such businesses.[27]

Thus, this may result in improved sales and ultimately, increased profits. When e-commerce businesses install cybersecurity measures such as firewalls, intrusion detection systems and monitoring, security alerts just to name a few, this may result in lowered data breaches.[28] They thereby create a safe space for storage of consumer data and make the cyberspace safer for the execution of electronic transactions. For these safe computing techniques to remain relevant in executing their tasks, e-commerce businesses not only have to invest in the data protection mechanisms but they also have to invest in continuously enhancing them.[29] Consequently, this shows that deep investment in cyber protection techniques helps in protecting sensitive information of consumers. The inverse is thus one of the causes of data breaches.

The ever increasing data breaches in e-commerce are the reason why Dr. Thuraisingham outlines that Lesotho is a victim of ever-increasing cybercrime incidents.[30] With the first half of 2023 alone experiencing surges in ransomware by 57%, an increase in fraud by 323% and spam related incidents that rose by 284%.[31] As such, it is imperative for e-commerce businesses to invest in comprehensive data protection measures. These measures also ought to be updated in order to prevent them from being obsolete and irrelevant in the current age where data breaches are so rife. At this stage, it is crucial to investigate the availability of a legal framework aimed at mitigating these causes of data breaches in e-commerce.

---

[27] Ibid.
[28] Niranjanamurthy M & Dr. Dharmendra Chahar, 'The Study of E-Commerce Security Issues and Solutions' (2013) 2 *International Journal of Advanced Research in Computer and Communication Engineering* 4.
[29] Efrim Boritz and Won No, 'E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery' (2011) 25 *Journal of Information Systems* 26.
[30] Dr. Maria Thuraisingham, 'Addressing Cybercrime Challenges Faced by Lesotho Mounted Police Service' (2024) *Faculty of Accounting and Informatics, Department of Information Technology, Durban University of Creative Technology* 3.
[31] Ibid.

3.3 **E-commerce Legal framework of Lesotho**

Protection of consumer data is important because consumers lodge with online businesses their private and confidential information that require protection by the e-commerce businesses.[32] It is for this reason that the Constitution guarantees that all persons are entitled to the right of privacy in aspects of their lives such as their home and/or personal affairs.[33]

This provision entails that no person's right to privacy may be abridged by anyone without the right owner's consent. This provision therefore extends to e-commerce in that even in a virtual setting such as e-commerce, the right of consumers to privacy shall still remain guaranteed. The peremptory nature of the wording of this provision entails that all persons are obliged to strictly obey privacy of other people even in the e-commerce realm. As a result, this provision sets a standard for protection consumers' right to privacy. When this right is contravened, the aggrieved consumer may approach the High Court for redress.[34] This therefore underscores the role played by legislation in terms of guarding privacy in e-commerce.

Lesotho has an array of laws that are meant deal with data protection and security when engaging in electronic transactions. These legislative frameworks include the Data Protection Act 2011, Payment Systems Act 2014 and the Payment Systems Regulations 2017. There also exists Parliament Bills on e-commerce such as the Electronic Transactions and Electronic Commerce Bill 2022 and the Computer Crime and Cyber Security Bill 2024.

As previously shown, the Constitution guarantees that personal information of consumers ought to be kept private.[35] This means that e-commerce business are bound to at all times guarantee the privacy of personal data of consumers by taking all necessary steps to maintain such privacy. As such, legislations such as the Data

[32] Data Protection Act 2011, section 17(1).
[33] Constitution of Lesotho 1993, section 11(1).
[34] Constitution of Lesotho 1993, section 22(1)
[35]Supra note 33.

Protection Act aid in nuancing this provision of the Constitution in enhancing the privacy of consumer data.

The Data Protection Act 2011 is one of the earliest laws in Lesotho aimed at protecting consumers when engaging in electronic transactions. The preamble of this Act outlines that the Act creates guiding rules and principles for the handling of consumer data whilst also balancing privacy rights with other legal and societal needs.[36] Additionally, the Act makes provision for the creation of a body called the Data Protection Commission that has the aim of overseeing compliance of data protection in the cyberspace.[37]

The Act applies only to data controllers who are domiciled in Lesotho or who have a principal place of business in Lesotho.[38] A data controller is defined by the Act as either a natural or juristic person responsible for setting the purpose and methods of processing data regardless of whether such processing is done by that person or an agent.[39] The Act remains applicable irrespective of whether a data controller uses automated or non-automated means of processing and storing consumer data.[40] As such, the Act aims to regulate how data controllers interact with and store personal data of consumers.

In order to ascertain that the collection of data is fair and lawful, a data controller is bound to collect personal data solely from a data subject.[41] Moreover, the data subject has to explicitly consent to the processing of their data.[42] The Act defines a data subject as a person who is the owner of personal data (customer).[43] As such, when a data controller collects data from a data subject, he is bound to explicitly disclose why such

[36] Data Protection Act 2011.
[37] Data Protection Act 2011, section 6(a).
[38] Data Protection Act 2011, section 3.
[39] Data Protection Act 2011, section 2.
[40] Ibid.
[41] Data Protection Act 2011, section 17(1).
[42] Data Protection Act 2011, section 15(2)(a).
[43] Data Protection Act 2011, section 2.

data is required and that such data shall be used for a legitimate purpose.[44] The rationale of this is to ensure that data subjects are well informed when they provide data controllers with their information. Also, this serves as a transparency requirement regarding the storage and retention of such data.[45]

These provisions ensure that as soon as soon as data controllers acquire personal data from data subjects, data controllers ought to handle such data with utmost care so as to prevent any unauthorized access. Hence data controllers are bound to inform data subjects at all times about their objectives with such personal data. It is for this reason that the Data Protection Commission was founded so as to ensure that data controllers comply with the provisions of the Act.[46]

After the collection of data, the data controller is bound by the Act to ensure the integrity and protection of data in its possession by preventing unlawful access[47] and loss and/or damage of such data.[48] The Act therefore provides that this may be achieved by processing personal information of consumers in an automated manner[49] and subsequently stored either in a filing cabinet[50] or in an electronic form.[51] In this vein, the Act aims to ensure data security by giving data controllers effective peremptory measures as to how to store data and prevent unlawful manipulation thereof.

As alluded to above, the Data Protection Commission aims to oversee compliance with the provisions of the Act.[52] As such, a data subject may lodge a complaint with the Commission on any contravention that he alleges the data controller has done.[53] This

[44] Data Protection Act 2011, section 18(1).
[45] General Data Protection Regulation, 'Right to be Informed' (2 August 2018) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed-1-0.pdf Accessed 17 January 2025.
[46] Data Protection Act, section 8(1)(c).
[47] Data Protection Act 2011, section 20(1)(b).
[48] Data Protection Act 2011, section 20(1)(a).
[49] Data Protection Act 2011, section 15(1).
[50] Data Protection Act 2011, section 15(1)(a).
[51] Data Protection Act 2011, section 15(1)(b).
[52] Data Protection Act 2011, section 6(1).
[53] Data Protection Act 2011, section 39(a).

duty of the Commission ensures that the deeds of data controllers do not go unchecked when dealing with personal data of data subjects. After a grievance has been lodged against a data controller, the Commission is bound to execute its duty of investigating the said grievance.[54]

In order to settle disagreements between the two parties, the Commission has a duty of resolving such disputes through conciliation where it appears that a settlement between the two parties is possible.[55] The adoption of conciliation is rooted on its benefit of assisting the parties to continue their relationship even after a settlement is reached.[56] However, although the Act makes a provision for the founding of the Data Protection Commission, it has still not been established and this raises critical issues as to the protection of personal data by data controllers.

The main weakness of the Data Protection Act is that since it is an Act of Parliament enacted in 2011, it is unable to protect consumers from newer cyber threats that endanger their personal information. This is due to the fact that the Act only generally provides for data controllers to store consumer data where it shall not be illegally accessed or manipulated by unauthorized people.[57] As a result, due to failing to have a provision that instructs data controllers to constantly update their data protection mechanisms, data controllers may proceed using obsolete measures that offer little to no protection in the current age.[58] Due to this, data controllers may maintain outdated systems and argue that they are still in compliance with the Act.[59] As such, these obsolete data protection systems swiftly become a huge threat to data security because they are easy to bypass.[60]

---

[54] Data Protection Act 2011, section 40(1)(a).
[55] Data Protection Act 2011, section 40(1)(c).
[56] Dr. Ujwala Shinde, 'Conciliation as an Effective Mode of Alternative Dispute Resolution System' (2012) 4 *Journal of Humanities and Social Science* 6.
[57] Data Protection Act 2011, section 15(1).
[58] Nedim Maric, 'Data Breaches: Causes, Compliance, and Best Practices' (6th September 2024) https://brightsec.com/blog/data-breaches-causes-impact-and-best-practices/ Accessed 6th March 2025.
[59] Ibid.
[60] Ibid.

This makes the Act only effective on the contraventions of confidentiality rules and no other offences such as theft in the cyberspace.[61] This is because the Act expressly provides that any person convicted of breaching confidentiality rules may be fined a fine not exceeding M50 000.00 or imprisonment period not exceeding five years or both.[62] Due to its main focus being on breach of confidentiality rules, the Act ends up being incomprehensive and unable to effectively deal with other cybercrimes of the modern age. Thereby opening a gap that criminals may utilize in order to breach sensitive data of consumers. Consequently, the inadequacy of legislation contributes to high data breaches as one of the causes thereof.

The second law that was enacted to safeguard data in the cyberspace is the Payment Systems Act 2014. The preamble of the Act entails that the Act regulates payment systems that occur between banks themselves.[63]

The Act also applies to clearing houses and securities settlement systems that include collateral and netting arrangements.[64] Essentially, this Act makes a provision for electronic funds, governance of electronic transactions and payment systems between banks that operate in within Lesotho. The Act describes a payment system as a set of rules and banking procedures that use interbank funds transfer systems to enable the free and unimpeded movement of money.[65]

Furthermore, an interbank payment system is explained as a formal framework that is binding between two banks in order to ensure money transfer between the two participating banks.[66] Therefore, Payment Systems Act 2024 is not applicable to data protection of consumers when engaging in electronic transactions as the Act does not govern e-commerce activities.

[61] Ibid.
[62] Data Protection Act 2011, section 55(b).
[63] Payment Systems Act 2014.
[64] Payment Systems Act 2014, section 3(a).
[65] Payment Systems Act 2014, section 2.
[66] Ibid.

The objective of the Payment Systems Act 2014 is to ensure that there is a reliable inter-bank payment system.[67] However, there are gaps within the Act itself that may result in data breaches. This is due to the fact that the Act lacks specific wording that give explicit requirements to payment service providers in relation to the upkeep of cybersecurity infrastructure. Without the specific and stringent requirements, financial institutions may end up failing to maintain the robust measures that would be aimed at preventing data breaches.

However, to maintain compliance with Act, the Central Bank of Lesotho (CBL) has a duty to establish and operate a settlement system and payment system.[68] As such, in 2024, the CBL launched a new payment system called the Lesotho Payment Switch (LeSwitch) so as to promote financial inclusion.[69] LeSwitch ensures seamless electronic payment processing by connecting various payment channels like automated teller machines, mobile payment and online commerce.[70] LeSwitch was therefore established with challenges such as cyberattacks in mind so as to not be an enhancer of cyberattacks and data breaches in e-commerce.[71] However, the focal point still remains that the Act is ineffective in terms of protecting personal data of consumers in e-commerce. This is because the Act was not enacted with consumer data privacy in mind but was enacted to make the payment system safer and more inclusive.

A third legal framework aimed at governing electronic transactions is the Payment Systems (Issuers of Electronic Payments Instruments) Regulations 2017 hereinafter referred to as "the Regulations". The purpose of the Regulations is to grant both licenses and supervision of issuers of electronic payment instruments along with the dispensation of electronic money as well as regulating e-money issuers.[72] The

[67] Payment Systems Act 2014.
[68] Payment Systems Act 2014, section 5(2)(b).
[69] Leemisa Thuseho, 'CBL Launches National Payment Switch' *Lesotho Times* (20th March 2024) https://lestimes.com/cbl-launches-national-payment-switch/ Accessed 24th March 2025.
[70] Ibid.
[71] Ibid.
[72] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 3.

Regulations define an issuer of electronic payment instruments as a company licensed to issue payment instruments.[73]

For clarity, electronic payment instruments are payment means that enable the transfer of funds in an electronic manner between financial institutions.[74] Essentially, the Central Bank of Lesotho is the body that is empowered by the Regulations to grant licenses to companies to utilize payment instruments in order to effect electronic transactions.[75] This therefore emphasizes the regulatory and supervisory powers of the Central Bank over issuers of electronic payment instruments. This is because the Central Bank of Lesotho ensures that the issuers of electronic payment instruments comply with the requirements of the Regulations.[76]

The supervisory duties of the Central Bank ensure that the issuers of electronic payment instruments maintain privacy of consumer data and may only disregard such privacy in instances of suspected money laundering or suspicious activity.[77] The Central Bank achieves this by monitoring compliance of the issuers of electronic payment instruments with the Regulations and the Payment Systems Act.[78] This means that although e-commerce consumers are entitled to privacy of their data and transactions,[79] their right to privacy of transactions may be lawfully limited if such limitation is to the furtherance of public safety as per an existing law.[80] As a result, when an issuer of electronic payment instruments suspects a transaction of a consumer is a subject of money laundering or funds terrorist activities, an issuer of electronic payment

[73] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 2(b).
[74] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, 4(2).
[75] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 7.
[76] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 20(2).
[77] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 24(2).
[78] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 18(5)(b).
[79] Meirong Guo, 'A Comparative Study on Consumer Right to Privacy in E-Commerce' (2012) *Modern Economy* 402.
[80] Constitution of Lesotho 1993, section 11(2)(a).

instruments may report such a transaction. Thereby showing that the right to privacy when engaging in electronic transactions is not absolute.

Moreover, the Regulations provide that an issuer of electronic payment instruments is bound to put in place consumer protection mechanisms for the furtherance of consumer protection and privacy.[81] These mechanisms are aimed at providing a minimum threshold of ensuring safe operations that include transparency and privacy of customer information.[82]

The Regulations therefore outline that consumer protection is key to the success of electronic transactions and subsequent trust thereof by prioritizing data safety. As a way of preventing and mitigating fraud and criminal activities, issuers of electronic payment instruments are enjoined to utilize "end-to-end" electronic audit trails so as to keep record of all transactions undertaken by the consumer.[83] Non-compliance with the requirements of the Regulations may result in an issuer of electronic payments instruments being fined a fine not exceeding M50 000.00.[84] This fine however applies if an issuer of electronic payments instruments failed to remedy its infringements with the Regulations within the requested time which is to the discretion of the Central Bank.[85]

The Payment Systems Regulations 2017 are adequate in ensuring data privacy and data security because of its specific requirements that it has put in place within its provisions. Furthermore, the imposition of heavy fines for failing to comply with the Regulations serves as a deterrent against any potential privacy infringements.[86] As a result, issuers of electronic payment instruments are impelled to adhere to the

[81] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 33(1).
[82] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 33(1)(a).
[83] Payment Systems (Issuers of Electronic Payment Instruments) Regulations 2017, regulation 38(a)(ii). End-to-end electronic audit trails enable the easy digital tracking of records and provide a detailed step by step process of a transaction from the beginning to the end.
[84] Payment Systems Act 2014, section 18(2).
[85] Payment Systems Act 2014, section 18(1).
[86] Ibid.

provisions of the Regulations so as to avoid being hit with the heavy fine. Consequently, although the Regulations provide hefty punishment for those who breach its provisions, enforcement of these sanctions still remains a focal point because with lack of enforcement, the Regulations are of little effect.

Lastly, Lesotho has a Bill of Parliament called the Computer Crime and Cybersecurity Bill 2024 which was founded for Lesotho to comply with the Budapest Convention on Cybercrime 2001 and the African Convention on Cyber Security and Personal Data Protection 2014. The broad object of the Bill is to make provisions for offences relating to improper and wrongful use of electronic communication devices and electronic networks.[87]

It aims to achieve this by providing a plethora of outlawed activities along with the sanctions that may be attached to perpetrators of such actions. Section 21 (1) of the Bill entails that gaining unauthorized access to a computer system is an offence punishable by M5 000 000.00 or imprisonment term not exceeding ten years or both upon conviction.[88] However, a person who breaches measures put in place to prevent unlawful access may be fined M7 000 000.00 or twelve years imprisonment or both upon conviction.[89]

Moreover, the Bill provides that whoever intercepts a private transmission of a computer dishonestly without lawful cause commits an offence and upon conviction, may be fined M10 000 000.00 or imprisonment term not exceeding fifteen years or both.[90] This therefore entails that the Bill entirely prohibits third parties from intercepting computer networks of e-commerce businesses that hold personal data of

[87] Computer Crime and Cyber Security Bill 2024.
[88] Computer Crime and Cyber Security Bill 2024, section 21(1).
[89] Computer Crime and Cyber Security Bill 2024, section 21(2).
[90] Computer Crime and Cyber Security Bill 2024, section 23(1)

consumers. The idea behind such heavy punishments is in line with the deterrence theory which outlines that severe punishments decrease crime by deterring it.[91]

Guaranteeing to protect personal data of consumers is of utmost importance. As such, any alteration to such personal data without consent of the consumer as an owner of such personal information is prohibited. It is for this reason that the Bill outlines that any person who unlawfully alters or forges computer data with the sole motive of having such data being misconstrued as legal commits an offence of computer forgery.[92]

This is a move to ensure that any acts of third parties that result in unlawful alteration of consumer data shall be punished. This also extends to instances where a third party fraudulently alters personal data with the intent of dishonestly acquiring an economic benefit.[93] This act is punishable on conviction by an imprisonment term not exceeding ten years or an imposition of a fine not exceeding M5 000 000.00 or both.[94] The Bill further seeks to protect personal data of consumers by providing that it is an offence for a third party to use identification of another person for commission of a crime.[95]

If formally enacted, the Bill may serve as a very effective deterrent and preventative measure of data breaches in e-commerce.[96] However, although theoretically the Bill looks to be effective, it does not provide for a body or institution that will be aimed at enforcing the provisions of the Bill and ensure compliance. This means that perpetrators may only be punished if a consumer comes to know about the data breach if they ever would. This is because cybercriminals mainly use inconspicuous means that are not easily detected by laypersons. Further, even if e-commerce consumers report the crime of illegal access or interception to the police, the Lesotho Mounted

[91] Hsin- Wen Lee, 'Taking Deterrence Seriously: The Wide-Scope Deterrence Theory of Punishment' (2017) 46 *Criminal Justice Ethics* 2.
[92] Computer Crime and Cyber Security Bill 2024, section 30(1).
[93] Computer Crime and Cyber Security Bill 2024, section 31(a).
[94] Ibid.
[95] Computer Crime and Cyber Security Bill 2024, section 34.
[96] Supra note 79.

Police Service (LMPS) is not well equipped and educated to investigate the intricate activities in the cyber realm. Furthermore, the Bill falls short in protecting personal data of consumers in e-commerce because it employs a more holistic and general approach to computer crimes. Its provisions apply generally to computer crimes and not specifically on data protection and security in terms of e-commerce. Thereby failing to squarely protect consumer data in e-commerce.

Legislation serves a role of maintaining a balance between aggressively protecting consumer data and also ensuring that transactions are completed seamlessly.[97] Furthermore, legislation ensures the constitutional right to privacy by guarding against data breaches that may lead to issues such as security and privacy threats.[98] It is for this very reason that Lesotho has enacted cyber laws as stated above, that have an aim of protecting consumer data in the cyberspace.

However, although Lesotho has enacted privacy laws that protect consumer data, the UNCTAD states that the Lesotho laws fall short of providing ample data protection to consumers when engaging in e-commerce.[99] This is because although the laws are enacted, they fail to exhaustively address all aspects of data privacy and security in e-commerce. That is, the Lesotho laws are not effective in combatting data breaches in e-commerce.

The weak legal framework ultimately fails to offer consumers invaluable protection against those who may unlawfully attempt to access their information.[100] This is because a comprehensive e-commerce framework is not only aimed at criminalizing

[97] Corey Ciocchetti, 'E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors' (2007) 44 *American Business Law Journal* 57.
[98] Ibid.
[99] United Nations Trade and Development, 'Lesotho ready to channel its growth to go digital' (2019) Available at https://unctad.org/news/lesotho-ready-channel-its-growth-go-digital#:~:text=New%20report%20on%20Lesotho%20shows,performance%20and%20diversifying%20income%20sources Accessed 7th March 2025.
[100] Molelekeng Kobane, 'Testing an Adapted Technology Acceptance Model (TAM) for Factors Influencing E-Commerce Adoption: A Lesotho Consumers' Perspective' 2023 (2) *American Journal of Economics and Business Innovation (AJEBI)* 160.

data breaches but also to deter them.[101] As a result, Robinson reiterates that deterrence and punishment of cybercrimes may only truly be achieved when the e-commerce law(s) support the detection and resultant successful prosecution of offenders.[102] However, although this is the case even in Lesotho, the main drawback is the scant to no enforcement of the law at all.[103] This shows how important it is to have an e-commerce law that is cognizant with conventional offences that happen over the medium of e-commerce along with effective enforcement thereof. Added to this, a robust enforcement system for the legal framework would assist in the laws being even more effective in protecting personal data of consumers. Moreover, if there are very weak cybersecurity measures in place, data breaches shall remain high as the mechanisms would easily get overwhelmed by ingenious ways of breaching data privacy.

3.4 **Nexus between data breaches and ineffectiveness of data protection laws**

Data protection laws may be deemed to be ineffective if they fail to achieve desired outcome(s).[104] In the context of the laws enacted for the protection of consumer data in the digital space, these laws may be regarded as ineffective if data breaches remain rife even after their enactment.

As previously stated, the laws in Lesotho aimed at data protection are rendered ineffective due to being outdated and failing to possess comprehensive and explicit wording. This may therefore result in ambiguity and therefore threaten exact compliance with the law(s). For legislation to be effective, it needs to withstand the test of time by still being able to curb privacy risks even in the current generation, thereby

[101] 'Mamotumi Maliehe, 'Cybercrime Legislation for Lesotho' (LLM dissertation, University of Cape Town 2007) ii.
[102] James Robinson, 'Internet as the Scene of Crime' (International Computer Crime Conference, 29-31 May 2000) http://www.usdoj.gov/criminal/cybercrime/roboslo.htm Accessed 6 January 2025.
[103] Supra note 7.
[104] Sherry Ebrahim, 'Factors Contributing to the Maintenance of Ineffective Policies: Case Study of the Independent Unsupervised Return Policy in the Netherlands' (Master of Science thesis, Erasmus University of Rotterdam2022) 9.

still remaining relevant in this age.[105] Inversely, when e-commerce businesses omit to maintain up to date data breach counter-measures, data breaches in Lesotho shall continue to rise because the laws do not provide for maintenance of updated cyber measures.

Furthermore, the Acts of Parliament enacted to prevent or at least to mitigate data breaches in e-commerce constantly fail to do so. This is due to the fact that the laws only provide general provisions aimed at applying across the whole cyberspace. Not taking into account how wide the cyberspace is. As such, failing to enshrine specific and stringent provisions renders the laws ineffective in terms of dealing with the cyber problems of the current age.

More so when more people are utilizing e-commerce. The Cybercrime and Security Bill allows for the creation of a National Cybersecurity Incident Response Team (the Team) with the objective of providing oversight for cybersecurity.[106] However, the fact that the Team has not yet been established, because the Bill is not yet enacted into law, means that objectives of the Team such as to provide reactive and proactive measures for guarding against cyber threats have not yet been reached.[107]

Consequently, this renders the legal framework ineffective as enforcement will not be achieved. This issue is further exacerbated by the fact that the Lesotho Mounted Police Service (LMPS) is not well equipped and skilled on how to investigate cybercrimes of the modern age. Consequently, although the laws are essentially put in place to prevent data breaches in e-commerce and mitigate cybercrimes in general, the laws still possess gaps that cyber criminals are able to exploit easily.

[105] Bahaudin Mujtaba and Frank Cavico, 'E-Commerce and Social Media Policies in the Digital Age: Legal Analysis and Recommendations for Management' (2023) 3 *Journal of Entrepreneurship and Business Venturing* 123.
[106] Computer Crime and Cyber Security Bill 2024, section 12(1).
[107] Computer Crime and Cyber Security Bill 2024, section 12(2)(a)(iii).

3.5 **Conclusion**

Data breaches in Lesotho are attributed to a number of causes as stated above. Effectively addressing these causes of data breaches may result in the creation of a safer digital space for consumers. This means that when the digital space is safe for consumers, more consumers may have trust in the e-commerce sector. This increased trust results in more consumers willing to use e-commerce and this may benefit the profit margins of the e-commerce businesses.[108] It is therefore imperative for e-commerce businesses to ensure that they prioritize the safety of consumer data and invest in it because they too will eventually benefit from this act.[109]

Although Lesotho has a number of laws that are aimed at ensuring the safety of consumers when engaging in electronic transactions, most of the laws however are unable to provide comprehensive protection to consumers by preventing data breaches. This is mainly due to the fact that the Lesotho laws are both outdated and not effectively enforced. This subsequently makes the laws to fail to offer consumers with the much needed protection against cybercriminals.[110] Thereby making it easy for cybercriminals to easily accesses sensitive data of consumers.

[108] Supra note 23.
[109] Ibid.
[110] Supra note 79.

4. Chapter four

Comparison of Lesotho to European Union on regulation of data privacy and security

4.1 Introduction

The EU has enacted a regulatory framework that is aimed at making the execution of electronic transactions safer for all users in the form of the General Data Protection Regulations 2018 (GDPR). The GDPR may essentially be compared and contrasted with the legal regime on data protection of Lesotho being the Data Protection Act 2011, Payment Systems Act 2014, Computer Crime and Cyber Security Bill 2022. As such, this chapter contains a comparative analysis between the GDPR and the data protection legal framework.

4.2 GDPR provisions on data privacy and security in e-commerce

The object of the GDPR is to protect fundamental rights and freedoms of e-commerce consumers particularly the inalienable right and entitlement to the protection of personal data.[1] That is the right of consumers to have their personal data private even when it is in the hands of e-commerce businesses. This protection extends to the processing of personal data of consumers along with the free movement of such data.[2] Prior to processing of personal data of consumers, the GDPR provides that the data ought to be collected solely for the specified, explicit and legitimate reasons.[3]

After its collection, the data controller is bound by law to process personal data of consumers in a lawful, fair and transparent manner that complies with the law.[4] Processing of personal data is defined as any automated or non-automated undertakings performed on personal data ranging from the collection, storage, transmission and destruction of personal data.[5] Consequently, a data controller is liable to ensuring that[6]

[1] General Data Protection Regulations, Art 1(2).
[2] General Data Protection Regulations, Art 1(1).
[3] General Data Protection Regulations, Art 5(1)(b).
[4] General Data Protection Regulations, Art 5(1)(a).
[5] General Data Protection Regulations, Art 4(2).
[6] General Data Protection Regulations, Art 5(2).

personal data is processed in a way that guarantees holistic security of the personal data of consumers.[7] Moreover, the GDPR provides that data controllers must at all times prior to processing personal data, attain consent from the data subject (consumer) for the processing of their data.[8] This essentially means that if for some reason a data controller collects personal data and goes on to process it without the consent of the data subject, such act shall be ruled to be unlawful.[9] This is to provide the data subject with some level of control over how and why their personal data is to be processed.

Since data subjects are typical day to day persons, the GDPR grants them numerous rights over their personal data in order to enable them to retain some control over their personal data and how it is to be administered. It is for this reason that the GDPR enjoins data controllers to furnish data subjects with sufficient details relating to the purpose, rationale and the legal basis for which their (data subject) personal data is to be processed.[10] This therefore means that without disclosing the purpose for the collection and subsequent processing of data as a result of a data controller getting consent from a data subject, such processing of data shall be deemed unlawful. In the case of *Orange Romania SA v Autoritatea Nationala de Supraveghere a Prelucrarii Detalor cu Caracter Personal,*[11] Orange Romania was a telephone company that operated by concluding mobile contracts with its consumers. The contracts it provided outlined that the customers consented to the collection and storage of copies of their identity cards. This "consent" came as a result of pre-ticked boxes that customers had to uncheck if they disagreed. The issue in this matter was whether "consent" that came as a result of pre-ticked boxes constituted actual consent? The court therefore held that this act did not amount to consent because consent demands unambiguous indication of the wishes of data subjects. Therefore, data controllers ought to provide data subjects

[7] General Data Protection Regulations, Art 5(1)(f).
[8] General Data Protection Regulations, Art 6(1)(a).
[9] General Data Protection Regulations, Art 6(1).
[10] General Data Protection Regulations, Art 13(1)(c).
[11] (Case C-61/19, Judgement of 11 November 2020) EU: C: 2020: 901.

with all information pertaining to reasons of collection of their data and allow data subjects to either grant or withhold their consent.

Also, to ensure justness and openness, the data subject has a right of being informed of how long their personal data is to be stored by the data controller.[12] Also, if there arises the need for a data controller to process personal data for any reason besides one for that the personal information was collected, the data controller ought to keep the data subject abreast with such changes.[13] This is to ensure that the data controller seeks consent for the new purpose of processing.[14] Moreover, since disputes arise time and again in agreements, data controllers are obliged to notify data subjects of their right to lodge complaints with a supervisory authority.[15] This entails that the supervisory authority would act as a mediator and aid with resolving any and all disputes that may arise.[16]

Supervisory authorities in each member states are bound to act in complete independence[17] when monitoring adherence to the conditions and requirements of the GDPR in ensuring high levels of personal data protection.[18] This is to ensure the integrity of how personal data is treated as the supervisory authorities retain complete impartiality when handling issues pertaining to data privacy. This therefore means that all forms of direct or indirect influence on the supervisory authority are completely ousted in order to ensure this independence. In the case of *European Commission v Hungary,*[19] Hungary terminated prematurely the mandate of the Hungarian Data Protection Commissioner by enacting a law that created a new authority. This therefore meant that the Commissioner who held office at the commencement of this new Hungarian law did not complete his term as a result of this new law. The European

[12] General Data Protection Regulations, Art 13(2)(a).
[13] General Data Protection Regulations, Art 13(3).
[14] Ibid.
[15] General Data Protection Regulations, Art 13(2)(d).
[16] Ibid.
[17] General Data Protection Regulations, Art 52(1).
[18] General Data Protection Regulations, Art 51(1).
[19] Case C-288/12 [2014] ECLI: EU: C: 2014: 237.

Commission sought to have this act by Hungary annulled due to it undermining the complete independence of the supervisory authority. The issue for determination was whether this new law (external from the GDPR) undermined independence of the supervisory authority guaranteed by the GDPR? The court held that independence of the supervisory authority was crucial in order to prevent any external factors from interrupting the seamless operations of the supervisory authority. As such, this new law that affected the independence of the supervisory authority was set aside.

When a data subject has granted his personal information to a data controller, he still retains some form of control over such information because data subjects get to have access over their personal data even when it is in the databases of the data controller.[20] Furthermore, data subjects still reserve their right to access information such as being told reasons for the processing of their personal data[21] and persons whom the personal data will be transmitted to.[22]

The data subject may even go as far as requesting the data controller to provide him with a copy of his personal data that is undergoing processing.[23] Where the personal data of a data subject is incomplete or incorrectly stated, the data subject has a right to inform the data controller to make such demanded changes without undue delay.[24] Added to this, the data subject has a right to demand the data controller to erase all his personal data promptly if the personal data is no longer needed for the function which it was collected for.[25] This right was enforced in the case of *Google Spain v AEPD and Mario Gonzalez*[26] whereby Gonzalez lodged a complaint against Google Spain and Google Inc.requesting the delition of his search results from the browser. Gonzalez argued that the search results were outdated and infringed on his right to privacy under the EU data protection law since they dated back to the year 1998. The issue for

[20] General Data Protection Regulations, Art 15(1).
[21] General Data Protection Regulations, Art 15(1)(a).
[22] General Data Protection Regulations, Art 15(1)(c).
[23] General Data Protection Regulations, Art 15(3).
[24] General Data Protection Regulations, Art 16(1).
[25] General Data Protection Regulations, Art 17(1)(a).
[26] Case C-131/12 [2014] ECLI:EU:C:2014: 317.

determination was whether an individual has a power to request his personal information be removed from a search engine? The court held that an individual may request for their personal information to be "forgotten" if such information is irrelevant or excessive.

Moreover, a data subject has a right to demand for his personal data to be erased if the data subject withdraws his consent for any further processing of his personal data.[27] Furthermore, when a data subject has requested for the erasure of his personal data and the data controller(s) have already made such personal information public, the data controller(s) are obliged to take reasonable steps to erase any trace of such personal data.[28] This right to erasure is also called the right to be forgotten because when all traces of the personal data of a data subject is deleted, the memory of such a data subject shall also be unremembered.[29] As such, after any erasure or rectification of personal information, a data subject has a right of being informed of this action by the data controller.[30]

The reason why data subjects have so many rights regarding their personal data is that data subjects have a fundamental right to have their personal data to be protected.[31] This stringent regulation also aids in eliminating a possibility of any grey areas in the rights of data subjects and to also ensure that data subjects get "efficient and timely protection."[32] Added to the rights that data subjects have, there are some other responsibilities that data controllers owe data subjects through an extension of their personal data. These responsibilities include, *inter alia*, the obligation to adopt and implement technical and organizational measures that prove that the processing of personal information has followed the required protocol.[33] Added to this, data controllers are enjoined to implement appropriate data protection policies that will

[27] General Data Protection Regulations, Art 17(1)(b).
[28] General Data Protection Regulations, Art 17(2).
[29] General Data Protection Regulations, Art 17.
[30] General Data Protection Regulations, Art 19(1).
[31] Jef Ausloos and others, 'Getting Data Subject Rights Right' (2019) *Jipitec* 283.
[32] Ibid.
[33] General Data Protection Regulations, Art 24(1).

ensure to mitigate and prevent unlawful data access.[34] Moreover, data controllers are obliged to track and maintain record of all processing activities that are undertaken on each data subject's personal data.[35] The rationale behind the keeping of processing records is on the basis that it is easier for data controllers to oversee the data processing procedure.[36] Due to the fact that this keeping of records is made pursuant to compliance with the GDPR, the data controllers ought to ensure that they are able to produce the records upon demand by the supervisory authority.[37]

Data controllers also have rights and obligations towards personal information of data subjects. This is mainly through ensuring high levels of security towards personal information. This may be achieved through data controllers adopting technical and organizational techniques to ensure security.[38] These data security measures may be in the form of the cyphering of personal data,[39] the ability of deletion to ensure privacy and accuracy of the data processing systems[40] and the ability to timeously retrieve personal data in the event of any incident.[41]

Furthermore, the GDPR concedes that security risks are non-exhaustive, as such, security measures to be undertaken ought to be able to suit risks associated with the processing of personal data.[42] If there are data breaches during the data processing phase, the data controller is obliged to inform the supervisory authority within seventy-two hours.[43] In the same manner, data controllers ought to notify data subjects of any pertinent threats to their personal information.[44] This is due to the fact that data

[34] General Data Protection Regulations, Art 24(2).
[35] General Data Protection Regulations, Art 30(1).
[36] Marija Batarelo, 'What is a Record of Processing Activities (ROPA)?' (Parser Compliance, 15th December 2022) https://dataprivacymanager.net/records-of-processing-activities/#:~:text=Record%20of20processing%20activities%20should,remove%20information%20asc ircumstances%20change. Accessed 21st March 2025.
[37] General Data Protection Regulations, Art 30(4).
[38] General Data Protection Regulations, Art 32(1).
[39] General Data Protection Regulations, Art 32(1)(a).
[40] General Data Protection Regulations, Art 32(1)(b).
[41] General Data Protection Regulations, Art 32(1)(c).
[42] General Data Protection Regulations, Art 32(2).
[43] General Data Protection Regulations, Art 33(1).
[44] General Data Protection Regulations, Art 34(1).

controllers have a delicate role of processing information that is constitutionally protected.[45] Data controllers are therefore obliged to maintain records of any data breaches, the ramifications of the breaches and the mitigation procedures taken and relay same to the supervisory authority to guarantee conformity with the legislation.[46] This therefore echoes the fact that data controllers are operating with sensitive information of data subjects that requires significantly high levels of protection.

The safekeeping of processed personal data is not only limited to the EU but extends globally. This is because the GDPR outlines that the transfer of personal data to third countries (countries not in the EU) or international organizations must only be made when the strict provisions of the GDPR are complied with.[47] The benefit of this is such that personal data of data subjects shall not get substandard protection solely because it is to be transferred to other international countries.

Furthermore, this transfer of personal information shall only be made when the European Commission has ensured that such non-EU or international organizations have stringent levels of safeguards.[48] The rationale of this stipulation is to guarantee that high levels of data protection are maintained even when personal data is transmitted to destinations outside the EU. The adequacy of the data protection mechanisms is achieved through the Commission investigating whether such third countries have strict data protection legal frameworks.[49] Also, the Commission may assess whether non-EU countries and international organizations have established efficient supervisory authorities for purposes of ensuring the safekeeping of data transferred to them.[50] This provision was enforced in the case of *Data Protection*

[45] Supra note 37.
[46] General Data Protection Regulations, Art 33(5).
[47] General Data Protection Regulations, Art 44(1).
[48] General Data Protection Regulations, Art 45(1). The duty of the European Commission is to allow personal data of data subjects to flow freely to non-European countries and international organization provided that the destination offers similar protection that the GDPR offers.
[49] General Data Protection Regulations, Art 45(2)(a).
[50] General Data Protection Regulations, Art 45(2)(b).

Commissioner v Facebook Ireland Ltd and Maximiliano Schrems[51] whereby after Schrems challenged the act of Facebook Ireland Ltd's act of transferring personal data to Facebook Inc. in the US. Schrems challenged this act by outlining that US laws do not offer personal information similar protections that the GDPR offers. Thereby failing to comply with Art 45. The issue in this matter was whether the US offers substantially similar level of protection required by Art 45 of the GDPR? The court therefore held that the transfer of personal information should be suspended because US laws did not offer adequate protections to personal data nor provide EU citizens with effective remedies that the GDPR offers.

The Commission goes a step further in ensuring high levels of data protection for personal data that is conveyed to non-EU countries. This is because the Commission is tasked with collaborating with such third countries to enhance international cooperation that will lead to effective enforcement of legislation so as to guarantee personal data protection.[52]

Compliance with the requirements of the GDPR on the side of data controllers is not always guaranteed. It is for this reason that an aggrieved data subject who is of the opinion that his data protection rights have been infringed may lodge with a supervisory authority his complaint regarding careless processing of personal data.[53] Consequently, should a data controller be deemed liable for failing to comply with the prescribes of the GDPR, the data subject thus has a right to a prompt and effective remedy against such a data controller.[54]

Effective sanctions therefore play a two-fold role in that firstly, they act as compensation towards a data subject and secondly, they impel data controllers to comply with the rules.[55] Consequently, the supervisory authority may then issue a

[51] *(Schrems II)* Case C-311/18 [2020] ECLI: EU: C: 2020: 559.
[52] General Data Protection Regulations, Art 50(1)(a).
[53] General Data Protection Regulations, Art 77(1).
[54] General Data Protection Regulations, Art 79(1).
[55] Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2021) 37 *Santa Clara High Technology Law Journal* 15.

ruling that empowers an aggrieved data subject to claim damages in the form of compensation from the data controller.[56]

It is therefore vivid that the GDPR places a very high standard on data controllers in terms of personal information belonging to data subjects that is in their (data controllers) possession. Thus, it is imperative for data controllers to abide by the prescribes of the GDPR in order to avoid being plunged into unnecessary costs of having to compensate aggrieved data subjects.

4.3 **Comparison of the GDPR and e-commerce data protection laws of Lesotho in data protection and security**

As mentioned earlier, the protection of personal data of consumers is a critical pillar in e-commerce because this is very sensitive information that the data subjects share with data controllers.[57] As such, statutory regulation of the security of personal data ensures that the security of personal data of consumers is guaranteed at all times.[58] This is the broad benefit of legislation in e-commerce: to guarantee that e-commerce businesses maintain a high standard of personal data protection. Although different jurisdictions enact laws that seek to regulate data protection, such laws are more often than not, never on par in terms of their effectiveness in the regulation of data privacy and security. This is the case also in the case of the GDPR and data protection laws of Lesotho.

In terms of scope, the GDPR has a very large reach and general applicability regarding the protection of personal data of consumers. This is because the GDPR expressly provides that the entitlement of data subjects to have their personal data protected constitutes a fundamental right that data controllers ought to uphold.[59] The GDPR further specifies that after the collection of data from a data subject, a data controller is

[56] General Data Protection Regulations, Art 82(1).
[57] Itok Kurniawan & Vincentius Setyawan, 'The Importance of Protecting E-Commerce Consumer Personal Data' (2024) 2 *Indonesian Journal of Law Research* 54.
[58] Ibid.
[59] Supra note 1.

bound to comply with the law to process such data in a just and transparent manner that guarantees privacy at all times.[60] Should a data controller process personal data in a negligent way that opens up such data to unlawful access of such data, such a data controller shall be considered to have breached the law. Furthermore, as shown in the *Schrems*[61] above, the reach of the GDPR is global. It was shown that transfers of personal data to foreign countries are strictly precluded if the destination country fails to guarantee similar data protection mechanisms.

On the same issue, in the previous chapter, the Data Protection Act has, as its primary principle, to provide for rules and principles for the handling of personal data of data subject.[62] This protection only applies to data controllers within Lesotho.[63] This is because although the Act allows for personal data to be transferred beyond Lesotho,[64] there is no supervisory body to guarantee its protection when it is transferred.[65] This is a complete opposite of the application of the GDPR which applies both within the EU and to any foreign country at which personal data may be transferred to.[66] This provision ensures that treatment of personal data in terms of its protection remains consistent irrespective of whether such data is in the EU or is transferred to a non EU member. On the other hand, the scope of the Payment Systems Act is only limited to regulating payment systems across banks situated in Lesotho.[67]

Other legal instruments in Lesotho meant for the protection of personal data are the Payment Systems Regulations and the Computer Crime and Cyber Security Bill. The object of the former is to provide regulation and supervision to issuers of electronic payment instruments. Also, as highlighted in the preceding Chapter, the Regulations provide for the issuers of electronic payment instruments to put in place measures that

[60] Supra note 7.
[61] Supraa note 51.
[62] Data Protection Act 2011.
[63] Data Protection Act 2011, section 3.
[64] Data Protection Act 2011, section 52.
[65] Ibid.
[66] Supra note 43.
[67] Payment Systems Act 2014.

will promote consumer protection and privacy. The Bill on the other hand provides for offences relating to the misuse of electronic communication devices and electronic networks.[68]

Although these two frameworks deal with the protection of consumer data in their own way, they do so in a very general manner that lacks specificity. Although this is the *status quo,* the Data Protection Act as an Act that deals squarely with protection of data in e-commerce, compensates for this lack of definiteness. This is therefore in sharp contrast with the GDPR that expressly provides that personal data ought to be protected invariably across the world as this constitutes protection of a fundamental right to privacy.

As stated above, the GDPR grants data subjects numerous rights from the moment they give data controllers their personal information. These rights range from being told by data controllers reasons for the processing of their personal data,[69] retaining the right to enter databases of data controllers so as to access their data,[70] being informed of their right to take their grievances with data controllers to a supervisory authority,[71] the right to ask data controllers to erase their personal information without any undue delay[72] and many others. The main reason behind these many rights is to enable data subjects to maintain a sense of authority over their personal data and how it is being handled.

This is why if a data subject is not content with how a data subject processes his personal data, he may submit a grievance with the supervisory authority or simply demand the data controller to erase his personal information. On the other hand, the Data Protection Act grants data subjects the similar rights as those that the GDPR grants. However, the Act makes no mention of the right for data subjects to demand for their personal data to be erased by data subjects.

[68] Computer Crime and Cyber Security Bill 2024.
[69] Supra note 10.
[70] Supra note 17.
[71] Supra note 13.
[72] Supra note 22.

This may be a huge problem when a data subject desires for his personal information to be erased. Also, although the Act provides for a body to oversee compliance and resolve disputes between data subjects and data controllers, the main problem is with the fact that this body has not yet been established. This poses a challenge for when disputes arise or when data controllers fail to comply with the Act. There is no body to hold them accountable.

The Regulations provide that the Central Bank of Lesotho shall be the one to enforce the Regulations and maintain compliance with the law.[73] Although the protection is not stringent, financial institutions are obliged to implement measures aimed at addressing consumer protection and privacy.[74] Lastly, the Bill on this point grants consumers protection by illegalizing acts such as unlawfully accessing a computer system without an excuse for doing so.[75] The Bill further forbids illegally interfering with computer data so as to make such information lose its integrity[76] and intercepting a private transmission of data without lawful cause.[77]

On the issue of compliance with the provisions of the Bill, the Bill establishes a National Cyber Security Incident Response Team which functions to provide reactive and proactive measures against cyber security threats.[78] However, it does not provide for the establishment of a body that data subjects may report to in instances where data controllers breach the provisions of the Bill. This therefore makes it impossible for data subjects to report data controllers. That is, the Team may fail to address some matters that need critical attention.

4.4 **Conclusion**

Taking into account the applicability of the abovementioned regulatory frameworks, it may be concluded that the GDPR is more effective and comprehensive in terms of

[73] Payment Systems (Issuers of Electronic Payments Instruments) Regulations 2017, regulation 20(2).
[74] Payment Systems (Issuers of Electronic Payments Instruments) Regulations 2017, regulation 33(1).
[75] Computer Crime and Cyber Security Bill 2024, section 21(1).
[76] Computer Crime and Cyber Security Bill 2024, section 24(1)(a).
[77] Computer Crime and Cyber Security Bill 2024, section 23.
[78] Computer Crime and Cyber Security Bill 2024, section 12(2)(a)(iii).

protecting personal data when comparing it with Lesotho's legal framework. Also, the very fact that the GDPR protects data even when it is transferred to other countries outlines its commitment in ensuring all-round data privacy.[79]

This, along with other effective enforcement mechanisms stated above ensure that the soul of the GDPR is always maintained. That is: to safeguard the confidentiality of personal data by maintaining its protection from third parties at all times.[80] It has been shown in this chapter the effectiveness and benefits provided by the GDPR hence Lesotho may adopt its style of data protection so as to make the Lesotho laws more robust.

However, it is not feasible for Lesotho to adopt the GDPR style protections. This is due to the fact that, unlike the GDPR that has established bodies aimed at overseeing compliance with the GDPR,[81] Lesotho, on the other hand, has not established this body. This therefore creates a challenge for Lesotho to guarantee a similar data protection style as the GDPR. Furthermore, one of the obligations of the yet to be formed Data Protection Commission is to promote education and public awareness.[82] As such, since it has not been established, many individuals and businesses alike may not be aware of data privacy risks and this subsequently curbs public demand for the GDPR-like reforms. In light of the foregoing, this chapter revealed some critical gaps in Lesotho's legal framework, the following chapter therefore outlines practical recommendations that may be incorporated so as to strengthen the legal framework.

[79] Supra note 43.
[80] Supra note 1.
[81] General Data Protection Regulation, Art 70(1).
[82] Data Protection Act 2011, section 8(1)(a).

5. Chapter five

Conclusion and recommendations

5.1 Introduction

This study set out to critically examine the effectiveness of Lesotho's cybersecurity laws in safeguarding data privacy and security within the e-commerce sector. The aim of this chapter is thus, to indicate the findings of the study, to make recommendations for reform in Lesotho, and to conclude the study.

5.2 Key Findings

The analysis across the preceding chapters has highlighted several key challenges. First, Lesotho's legislative framework for data protection and cybersecurity is outdated and does not fully address modern cyber threats, particularly those arising in the fast-evolving e-commerce environment. Second, there is a notable lack of enforcement of existing laws, with weak institutional capacity to detect, prevent, and respond effectively to data breaches. Third, Lesotho's legal instruments provide incomplete coverage of contemporary cybersecurity risks, leaving significant gaps that expose consumers and businesses to harm. Fourth, Lesotho's e-commerce sector remains underdeveloped, in part due to these legal and regulatory shortcomings. By contrast, the European Union's General Data Protection Regulation (GDPR) offers a more robust and comprehensive approach that could serve as a useful benchmark for reform.

Against this background, and in light of the research question; how effective are Lesotho's cybersecurity laws in safeguarding data privacy and security within the e-commerce sector? This final chapter proposes recommendations aimed at closing the identified gaps. Each recommendation directly addresses the core issues revealed in the study and takes into account the practical challenges of implementation within the Lesotho context.

It has been discussed and proven in the earlier chapters that what makes the data protection laws in Lesotho peculiar is the fact that they are found in many different and numerous Acts or legislations. This may therefore prove to be a difficult task in

attempting to reconcile some provisions of these legislations due to their fragmentation. This ultimately makes the GDPR more comprehendible and more structured than the data protection laws of Lesotho. Consequently, scouring through all these many and different legislations may prove difficult and result in inhibiting comprehension of the laws and ultimately, compliance thereof.

In an attempt to pit the GDPR against the Lesotho laws on data protection in the above chapters, some weaknesses of the Lesotho laws *vis-a-vis* the GDPR became visible. For instance, the Lesotho laws do not allow data subjects to reserve the power to request data controllers to move their personal data at their will (portability). As such, due to portability of personal information not being provided for in the Lesotho laws, it is therefore evident that it is not a right that data subjects retain. Furthermore, this detailed exploration of the Lesotho laws proved that while at first glance the Lesotho laws also provide for deletion of information, it is not as effective. This is because data controllers may delete information but still retain some of this information in their systems. This is therefore in stark contrast with the right to be forgotten provided by the GDPR which seeks to have the personal data deleted from all databases as if it never existed.

Furthermore, the deep analysis into the Lesotho laws in the previous chapters has revealed some critical cracks that warrant paying attention to. For instance, although the Data Protection Act allows for the transfer of personal data to foreign countries, these transfers are however not regulated. This therefore means that a data controller may willfully transfer personal data to countries that do not offer stringent levels of data protection. Thereby putting the privacy and security of personal information of consumers at risk. As such, due to not having established a body aimed at enforcing compliance with the laws, noncompliance by data controllers may negatively affect personal data of consumers. The nonexistence of this body therefore creates a rather fragile enforcement mechanism because the law is essentially existing in a vacuum. This therefore means that although the Data Protection Act binds data controllers to

notify the Data Protection Commission of any breaches suffered, this shall not happen because the Commission has not been established yet. As a result, all the duties of the Commission that have been discussed previously are inoperative because the Commission has not come into being to date.

5.3 Recommendations

5.3.1 Legislative reform

The United Nations General Assembly created the UNCITRAL and the UNCTAD to govern data privacy and the flow of commerce, they however left some freedom to countries to formulate their own data protection laws.[1] It is therefore up to each signatory state to legislate its own laws for the monitoring of e-commerce. The upkeep of each person's right to respect of his privacy[2] ensures that all consumers have replete protection of their person and their property (personal information).[3] This means that comprehensive e-commerce protection laws and data privacy policies ensure the protection of personal data of consumers whilst engaging in electronic transactions. In essence, it is imperative for Lesotho data protection laws to be comprehensive so as to effectively protect consumer data. This may be achieved by incorporating some provisions from legal frameworks such as the GDPR.

A *prima facie* difference between the GDPR and the Lesotho laws on e-commerce data protection is that the principles of the former are codified into one document whereas those of the latter are placed in different legal instruments. As such, the GDPR has a benefit of making the law more easily accessible and understandable to those who are bound by it and this makes it seamless for people to solve legal questions.[4] In putting this issue into context, the accessibility and comprehension of the provisions of

[1] Lee Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) *Stockholm Institute for Scandinavian Law* 187.
[2] Constitution of Lesotho 1993, section 11(1).
[3] Ida Azmi, 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill' (2002) *International Review of International Computers & Technology* 1.
[4] Gunther Weiss, 'The Enchantment of Codification in the Common-Law World' (1999) 25 *The Yale Journal of International Law* 496.

the GDPR is also as a result of the Articles relating to e-commerce being put into one document. As such, this makes it easier for one to retrieve the GDPR and check his compliance with its provisions. Conversely, the data protection provisions in Lesotho are encapsulated into many different legislations. This therefore makes the access and comprehension of the law more laborious as compared to when there was only one law dealing with data protection in e-commerce. The jumbled nature of these provisions may therefore make it difficult for consumers and e-commerce businesses to access and comprehend the law as a result of incoherence. Making it difficult for them to adhere to the prescribes of the law. Consequently, incorporating all data protection provisions into one law may aid in making the law more comprehensive and accessible to all. Eradicating the need for perusing different laws that contain a similar topic (data protection in e-commerce). However, an implementation barrier of this recommendation is a slow legislative process. This is due to the fact that codification needs a significant amount of time in order for laws to fully be codified into one law.

In order to maintain disclosure regarding the personal information in the custody of a data controller, the GDPR outlines that a data subject has a right to obtain his personal data in a commonly used and machine readable format.[5] Furthermore, it also provides for the "portability" of this personal information.[6] Portability ensures that a data subject has a right to request a data controller to transfer his personal information to himself or to another data controller without any impediment.[7] This ensures that the data subject retains utmost control over his personal information and also with regard to whom he may desire for the personal information to be transferred. This provision further shows how seamless the GDPR has made the transfer of personal information at the request of a data subject.

[5] General Data Protection Regulations, Art 20(1).
[6] General Data Protection Regulations, Art 20(2).
[7] Ibid.

Contrary to this, in Lesotho, the closest provision to this one only provides for the data subject to request access to his own information.[8] Since the Act fails to make mention of the portability of personal information, it may be difficult for data subjects to request data controllers to transfer their personal information to other data controllers. More so in a machine readable manner. As such, the incorporation of the provision of the GDPR would make it effortless for data subjects to easily request for the transfer of their personal data. Notwithstanding that, even if this provision is made in the Act, it would still prove to be a formidable challenge to implement this due to the absence of a body that ensures that data controllers comply with the law.

Moreover, the GDPR emphasizes the entitlement of data subjects to be "forgotten."[9] Data subject may exercise their right to demand data controllers to erase their personal information when they withdraw their consent[10] or when the aim for the gathering of personal data has been achieved.[11] This right to be forgotten is further amplified by a provision that outlines that the right to erasure extends to erasure of any links, copies or replications of such personal data.[12] This right of erasure extends to all other data controllers who may be processing the personal information at any particular time.[13]

However, the Act provides for deletion of personal information in similar circumstances as in the GDPR,[14] it does not expressly provide for the right to be forgotten by data controllers. The right to be forgotten is defined as an entitlement for a data subject to compel a data controller to delete his personal information in all perpetuity from all online databases.[15] Failing to ensure permanent deletion poses significant dangers to data subjects because information put on the internet is "never"

[8] Data Protection Act 2011, section 26(1)(b).
[9] General Data Protection Regulations, Art 17(1).
[10] General Data Protection Regulations, Art 17(1)(b).
[11] General Data Protection Regulations, Art 17(1)(a).
[12] General Data Protection Regulations, Art 65(1).
[13] Ibid.
[14] Data Protection Act 2011, section 19(5).
[15] Robert Walker, 'Note- The Right to be Forgotten' (2012) 64 *Hastings Law Journal* 261.

truly forgotten and may be used wrongly.[16] It follows therefore that this provision be incorporated in the Act so as to assure data subjects of their entitlement to being forgotten when they revoke their consent for further processing of their personal information. This is because this ensures perpetual deletion of personal information with no ability of recovery. However, with the inexistence of a body aimed to hold data controllers accountable, implementation of this recommendation would still prove to be cumbersome.

5.3.2 Institutional strengthening

The GDPR seeks to ferociously protect personal information of data subjects even when such information has been transferred to other countries that are outside the European Union.[17] The main reason why the GDPR does not make it easy for data controllers to transfer personal information to third countries is to ensure that the personal information shall still get similar protection that the GDPR offers.[18] Moreover, this helps the EU to retain a sense of authority over the protection of personal and sensitive information of data subjects. This provision also helps to ensure that strict protection of personal information remains maintained even when personal information is transferred to countries outside the EU.

Although Lesotho provides for data controllers to transmit personal information to persons in foreign countries,[19] there is no body that is empowered to authorize these transfers. This may therefore result in data controllers choosing to unilaterally transfer personal information without any scrutiny of such transfers. The incorporation of the GDPR-like provision on this subject in the Act would ensure that data controllers do not blindly transfer personal information to third countries. This incorporation would ensure that the transfer of such information follows strict regulatory requirements so as to ensure stern protection of data even when it is transferred to other countries. This

[16] Ibid at 259.
[17] General Data Protection Regulations, Art 44(1).
[18] General Data Protection Regulations, Art 45(1).
[19] Data Protection Act 2011, section 52.

matter is easily implementable if there is established an overseeing body that ensures that data controllers only transfer personal information of consumers to destinations that still offer high levels of protection.

5.3.3 Enforcement of existing laws and compliance

The GDPR acknowledges that although it is enacted to protect personal information of data subjects, data breaches may still occur. In such instances, a data controller ought to inform the supervisory authority promptly or within seventy-two hours of a data breach.[20] The seventy-two hours specification ensures that there is clarity on the reporting and this ensures compliance with this timeline. Added to this, data controllers are bound to track and document all data breach incidents, the effects thereof and any remedial action taken.[21] All this is meant to ensure efficiency in instances of data breaches and to ensure that any incidents are dealt with timeously.

On the contrary, the Act provides for data controllers to notify the Data Protection Commission of any breach[22] as soon as possible after being aware of the breach.[23] The "as soon as possible" is a term may be open to different interpretations and may fail to aid in ensuring strict compliance with reporting. Expressly stating the time limits ensures that there is adequate clarity that will not be interpreted otherwise. This therefore means that expressly incorporating the time limits in the section may eradicate any ambiguity and make it easier for data controllers to comply with the provision. Notwithstanding the lack of specificity in terms of time limits regarding reporting, it is impossible to report breaches in Lesotho due to the inexistence of the Data Protection Commission that is yet to be established.

Further, the GDPR provides for the imposition of severe fines when data controllers infringe its provisions. For instance, if a data controller commits the same or similar offence that he was once cautioned of and results in the infringement of any of the

[20] General Data Protection Regulations, Art 33(1).
[21] General Data Protection Regulations, Art 33(5).
[22] Data Protection Act 2011, section 23(1)(a).
[23] Data Protection Act 2011, section 23(2).

provisions of the GDPR, punishment shall be equal to the one imposed on the gravest infringement.[24] Moreover, the GDPR outlines that if a data controller infringes a data subject's rights[25] and also infringes the basic principles of data processing,[26] such data controller may be fined heavily by the National Supervisory Authority.[27] These fines may reach up to €20 000 000 as a way of punishing the data controller for such a grave breach of data protection guarantees.[28] Likewise, should a data controller fail to comply with any decision of the National Supervisory Authority, such controller may be fined a similar fine as stated above.[29] The reasoning behind these heavy fines is that the financial sanctions shall aid in general deterrence and rehabilitation.[30] Thereby preventing any future infractions with the law.

Conversely, the Act adorns the Commission with powers to investigate contraventions of the Act[31] but does not provide it with powers to impose fines on data controllers. This is because in its enforcement notice after investigating a matter and finding that a data controller contravened the Act, it may only order a data controller to refrain from taking action[32] or to stop any further processing of personal information.[33] The only way for a data controller to be subjected economic sanctions is if a data subject applies to court for relief.[34] An avenue that is in most cases expensive that indigent people may not be able to exploit. As a result, the Act may incorporate a provision that grants the Commission power to mete out pecuniary punishment as this may aid in fostering compliance with the Act and deter any future infringements. However, the

[24] General Data Protection Regulations, Art 83(3).
[25] General Data Protection Regulations, Art 83(5)(b).
[26] General Data Protection Regulations, Art 83(5)(a).
[27] General Data Protection Regulations, Art 83(5).
[28] Ibid.
[29] General Data Protection Regulations, Art 83(6).
[30] Torie Atkinson, 'A Fine Scheme: How Municipal Fines Become Crushing Debt in the Shadow of the New Debtor's Prisons' (2016) 51 *Hard Civil Rights-Civil Liberties Law Review* 192.
[31] Data Protection Act 2011, section 40(1).
[32] Data Protection Act 2011, section 46(1)(a).
[33] Data Protection Act 2011, section 46(1)(b).
[34] Data Protection Act 2011, section 49.

implementation of this recommendation is insurmountable because the Commission is yet to be established.

5.4 Conclusion

The hypothesis of this study stated that there is a direct connection between e-commerce data breaches and the lack of a comprehensive legislation. As such, this research has illustrated the benefit that comes along with effective legislative framework aimed at ensuring data privacy. This is because as previously outlined in the research, the lack of a comprehensive and effective legislation makes it easy for cybercriminals to exploit weak protection mechanisms of consumer data. This therefore has a huge bearing on e-commerce as a whole because due to heightened data breaches as a result of incomprehensive legislation, consumers may begin to dread e-commerce. Thereby stifling its growth. In contextualizing this matter, the root cause of the sluggish growth of e-commerce is attributed to high data breaches as a result of the absence of comprehensive legislation.

This research has as its aim the priority of analyzing the extent to which the legislation in Lesotho ensures data privacy and security when engaging in electronic transactions. As such, it outlined that Lesotho has an array of different legislations that protect personal information of different kinds. However, the Data Protection Act is the one that deals squarely with the protection of consumer data when engaging in e-commerce. Although the Act at face value seems to be somewhat effective, the lack of sufficient particularity and lack of enforcement render it ineffective. As shown in the previous chapters, this lack of enforcement is attributed to the LMPS lacking adequate and sufficient resources to investigate intricate cybercrimes. Moreover, the prevalent lack of consumer awareness on the deceptive tactics that cybercriminals employ adds fuel to the fire of the widespread data breaches.[35] This status *quo* continues to prevail

[35] Maria Thuraisingham, 'Cybersecurity in Lesotho: Current Challenges and Future Opportunities' (2023) *Durban University of Technology* 7.

notwithstanding the creation of a Commission tasked with promoting education and awareness.[36] This is therefore attributed to the ineffectiveness of the Act in this regard.

It has been shown in the previous chapters that the privilege for one to have his personal data private is a constitutional right.[37] It is therefore up to the Act to safeguard this right by being comprehensive enough to protect personal information of consumers when engaging in electronic transactions. However, due to technicalities such as incomprehensiveness and lack of strict enforcement, cybercriminals still easily navigate their away around the guarantees of the legislation. This is because when the Act is not comprehensive enough, data controllers as the caretakers of consumer data, may end up not investing as much as they should in newer protective technologies of consumer data. Consequently, this results in the law failing to safeguard consumer data and being of little effect in the protection of personal information of consumers. Thereby proving that there is a correlation between the lack of comprehensive legislation and data breaches.

[36] Data Protection Act 2011, section 8(1)(a).
[37] Constitution of Lesotho 1993, section 11(1).

Bibliography

Primary sources

Case law

Data Protection Commissioner v Facebook Ireland Ltd and Maximiliano Schrems (Schrems II) Case C-311/18 [2020] ECLI: EU: C: 2020: 559

European Commission v Hungary Case C-288/12 [2014] ECLI: EU: C: 2014: 237.

Google Spain SL and Google Inc. v Agencia Espanol de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez Case C-131/12 [2014] ECLI: EU: C: 2014: 317

Orange Romania SA v Autoritatea Nationala de Supraveghere a Prelucrarii Detalor cu Caracter Personal (Case C-61/19, Judgement of 11 November 2020) EU: C: 2020: 901.

Legislation

Communications Decency Act (CDA) 1996. (United States of America)

Computer Crime and Cyber Security Bill 2024. (Lesotho)

Constitution of Lesotho 1993.

Data protection Act No. 5 of 2011. (Lesotho)

Directive 2000/31/EC on Electronic Commerce [2000]. (European Union)

Financial Services Modernization Act 1999. (United States of America)

General Data Protection Regulations 2018. (European Union)

Payment Systems Act No. 11 of 2014. (Lesotho)

Payment Systems (Issuers of Electronic Payment Instruments) Regulations No. 30 of 2017. (Lesotho)

Treaties and conventions

International Trade Administration, ‘Lesotho- Country Commercial Guide’ (2024).

United Nations Commission on International Trade Law Model Law on Electronic Commerce 1996.

United Nations Conference on Trade and Development, ‘Lesotho Rapid e-trade Readiness Assessment’ (2019).

United Nations Conference on Trade and Development, ‘Lesotho ready to channel its growth to go digital’ (2019).

United Nations Conference on Trade and Development, *Unlocking the Potential of E-Commerce in Developing Countries* (UNCTAD 2015).

Secondary sources

Books

Colin Bennet & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Routledge Revivals 2003).

Eric Cole, *Hackers Beware* (1st edn New Riders Publishing 2001).

Samuel Cinini *et al, Cybercrime and Challenges in South Africa* (Palgrave Macmillan 2023).

Journal articles

Aishwarya Pandey, ‘Consumer Protection in the Era of E-Commerce: Issues and Challenges’ (2022) 4 *International Journal of Legal Science and Innovation*.

Aleksy Kwilinski *et al,* ‘E-Commerce: Concept and Legal Regulation in Modern Economic Conditions’ (2019) 22 *Journal of Legal, Ethical and Regulatory Issues.*

Alemayehu Molla & Richard Heeks, ‘Exploring E-Commerce Benefits for Businesses in a Developing Country’ (2007) *The Information Society.*

Anjali Gupta, ‘E-Commerce: Role of E-Commerce in Today’s Business’ (2014) 4 *International Journal of Computing and Corporate Research.*

Anthony Miyazaki & Ana Fernandez, ‘Internet Privacy and Security: An Examination of Online Retailer Disclosures’ (2000) 19 *Journal of Public Policy & Marketing.*

Anuradha Reddy, ‘A Study On Consumer Perceptions On Security, Privacy & Trust On E-Commerce Portals’ (2012) 2 *Excel International Journal of Multidisciplinary Management Studies.*

Audie Atienza *et al,* ‘Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings from a Mixed-methods study’ (2015) *Journal of Health Communication.*

Avi Goldfarb & Catherine Tucker, ‘Privacy and Innovation’ (2011) *National Bureau of Economic Research.*

Bahaudin Mujtaba and Frank Cavico, ‘E-Commerce and Social Media Policies in the Digital Age: Legal Analysis and Recommendations for Management’ (2023) 3 *Journal of Entrepreneurship and Business Venturing*.

Belanger *et al,* ‘Trustworthiness in electronic commerce: the role of privacy, security and site attributes’ (2002) *Journal of Strategic Information Systems.*

Bilqis Sa’adah *et al,* ‘Establishing a Personal Data Protection Agency for E-Commerce in Indonesia: Legal Framework and Implementation Challenges’ (2024) 4 *Journal of Sharia and Economic Law*.

Christian Kabongo & Asa Asa, ‘Factors Influencing E-Commerce Development: Implications for the Developing Countries’ (2015) 1 *International Journal of Innovation and Economic Development*.

Corey Ciocchetti, ‘E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors’ (2007) 44 *American Business Law Journal*.

Dr. Dharmendra Chahar & Niranjanamurthy M, 'The Study of E-Commerce Security Issues and Solutions' (2013) 2 *International Journal of Advanced Research in Computer and Communication Engineering*.

Dhruv Arora, 'Data Privacy Issues with E-Commerce' (2023) 8 *International Journal of Social Science and Economic Research*.

Dilshad Shaik, 'Consumer Protection in E-Commerce: A Legal and Compliance Framework in the Digital Market' (2020) 549 *Advances in Social Science, Education and Humanities Research*.

Djumadi Barkatullah, 'Does self-regulation provide legal protection and security to e-commerce consumers? (2018) *Electronic Commerce Research and Applications.*

Efrim Boritz and Won No, 'E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery' (2011) 25 *Journal of Information Systems.*

Eliza Mik, 'E-Commerce Regulation: Necessity, Futility, Disconnect' (2013) *First International Conference on Technologies and Law*.

Farhang Salehi *et al,* 'The Impact of Website Information Convenience On E-commerce Success of Companies' (2012) 57 *Procedia- Social and Behavioral Sciences*.

France Belanger *et al,* 'Trustworthiness in electronic commerce: the role of privacy, security, and site attributes' (2002) *Journal of Strategic Information systems.*

Francesco Greco *et al,* 'Explaining Phishing Attacks: An XAI Approach to Enhance User Awareness and Trust' (2023) *CEUR Workshop Proceedings*.

Godwin Udo, 'Privacy and security concerns as major barriers for e-commerce: a survey study' (2001) *College of Business Administration, University of Texas*.

Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2021) 37 *Santa Clara High Technology Law Journal*.

Gunther Weiss, 'The Enchantment of Codification in the Common-Law World' (1999) 25 *The Yale Journal of International Law.*

Haiqin Weng *et al,* 'Online E-Commerce Fraud: A Large-scale Detection and Analysis' (2018) *IEEE 34th International Conference on Data Engineering (ICDE).*

Ida Azmi, 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill' (2002) *International Review of International Computers & Technology*.

Issa Najafi, 'The Role of e-Commerce Awareness on Increasing Eelectronic Trusts' (2012) *Life Science Journal*.

Itok Kurniawan & Vincentius Setyawan, 'The Importance of Protecting E-Commerce Consumer Personal Data' (2024) 2 *Indonesian Journal of Law Research*.

Jamie Pont *et al,* 'Why Current Statistical Approaches to Ransomware Detection Fail' (2020) *Kent Academic Repository*.

Jef Ausloos and others, 'Getting Data Subject Rights Right' (2019) *Jipitec.*

Jeff Dodd & James Hernandez, 'Contracting in Cyberspace' (1998) *Computer Law Review and Technology Journal*.

John Murray & Albemarle Street, *Lectures on Jurisprudence* (Spottiswoode and Co 1880).

Jonathan Bick, 'Why Should the Internet Be Any Different?' (1998) 19 *Pace Law Review*.

Jon Bing, 'The Council of Europe Convention of the OECD Guidelines on Data Protection' (1984) 5 *Michigan Journal of International Law*.

Joseph Bingham, 'What is the Law?' (1912) 11 *Michigan Law Review*.

Karolina Lubowicka & Pawel Socha, 'Privacy Compliance in Ecommerce- A Comprehensive Guide' (2023) *Data Privacy & Security – GDPR*.

Lakshmi Nalla & Vijay Reddy, 'Data Privacy and Security in E-commerce: Modern Database Solutions' (2023) 1 *International Journal of Advanced Engineering Technologies and Innovation*.

Lee Bygrave, 'Data Privacy Law: An International Perspective' (2014) *Oxford University Press*.

Lee Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) *Stockholm Institute for Scandinavian Law*.

Lillyana Jaller *et al,* 'The regulation of Digital Trade- Key Policies and International Trends' (2020) 1 *World Bank Group*.

Mahmood Ansari, 'Exploring the Link of Action to Justice: A Review' (2023) 17 *Asian Journal of Advanced Research and Reports*.

Dr. Mamta Kumari *et al,* 'The Impact of Data Breaches on Consumer Trust in E-Commerce' (2014) 4 *International Journal of Current Science.*

Mark Ackerman & Donald Davis Jr, 'Privacy and Security Issues in E-Commerce' (2003) *New Economy Handbook*.

Dr. Maria Thuraisingham, 'Addressing Cybercrime Challenges Faced by Lesotho Mounted Police Service' (2024) *Faculty of Accounting and Informatics, Department of Information Technology, Durban University of Creative Technology*.

Maria Thuraisingham, 'Cybersecurity in Lesotho, Current Challenges and Future Opportunities' (2023) *Durban University of Technology*.

Mark Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate' (1998) 49 *South Carolina Law Review*.

Mary Culnan & Cynthia Williams, 'How Ethics can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches' (2009) 33 *Mis Quarterly*.

Meirong Guo, ‘A Comparative Study on Consumer Right to Privacy in E-Commerce’ (2012) *Department of Social Engineering, Graduate School of Decision Science and Technology, Tokyo Institute of Technology*.

Mindaugas Degutis *et al,* ‘Consumers’ Willingness to Disclose Their Personal Data in e-Commerce: A Reciprocity-based Social Exchange Perspective’ (2023) *Journal of Retailing and Consumer Services*.

Molelekeng Kobane, ‘Testing an Adapted Technology Acceptance Model (TAM) for Factors Influencing E-Commerce Adoption: A Lesotho Consumers’ Perspective’ (2023) *American Journal of Economics and Business Innovation (AJEBI).*

Moti Zwiling and others, ‘Cyber Security Awareness, Knowledge and Behavior: A comparative Study’ (2020) *Journal of Computer Information Systems*.

Muneer A *et al,* ‘Data Privacy Issues and Possible Solutions in E-commerce’ (2018) *Journal of Accounting and Marketing.*

Neda Yousefi & Ashkan Nasiripour, ‘A proposed model of e-trust for electronic banking’ (2015) *Management Science Letters.*

Neelam Chawla & Basanta Kumar, ‘E-Commerce and Consumer Protection in India: The Emerging Trend’ (2022) *Journal of Business Ethics*.

Nidhi Singh *et al,* ‘An analysis of consumer’s trusting beliefs towards the use of e-commerce platforms’ (2024) *Humanities & Social Sciences Communication*.

Omid Bigdeli *et al,* ‘Barriers of Online Shopping in Developing Countries: Case Study of Iran’ (2009) *IADIS Multi Conference on Computer Science and Information Systems*.

Peter Swire, ‘Markets, Self-Regulation, and Government Enforcement in the Protection of Personal information’ (1997) *US Department of Commerce*.

Peter Swire & Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (The Brookings Institution Press 1998).

Peter Swire, 'The Surprising Virtues of the New Financial Privacy Law' (2002) 86 *Minnesota Law Review.*

Peter Swire, 'Trustwarp: The Importance of Legal Rules to Electronic Commerce and Privacy (2003) 54 *Hastings Law Journal*.

Rami Al-dweeri *et al,* 'The Impact of E-Service Quality and E-Loyalty on Online Shopping: Moderating Effect of E-Satisfaction and E-Trust' (2017) 9 *International Journal of Marketing Studies.*

Ramnath Chellappa, 'Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security' *Goizueta Business School, Emory University Atlanta*.

Randy Merchany & Joseph Tront, 'E-Commerce Security Issues' (2002) *Proceedings of the 35th Hawaii International Conference on System Sciences*.

Robert Walker, 'Note- The Right to be Forgotten' (2012) 64 *Hastings Law Journal*.

Roberto Rosas, 'Comparative Study of the Formation of Electronic Contracts in American Law with References to International Law' (2006) 46 *Indian Journal of International Law*.

Ruchi *et al,* 'Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning' (2024) *IGI Global*.

Se-Hak Chun, 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability' (2019) *Sustainability'*.

Sha'ista Goga & Anthea Paelo, 'Issues in the Regulation and Policy Surrounding E-commerce in South Africa' (2019) *Centre for Competition, Regulation and Economic Development.*

Sherry Ebrahim, 'Factors Contributing to the Maintenance of Ineffective Policies: Case Study of the Independent Unsupervised Return Policy in the Netherlands' (Master of Science thesis, Erasmus University of Rotterdam2022).

Shrawan Trivedi & Mohit Yadav, 'Repurchase intentions in Y generation: mediation of trust and e-satisfaction' (2020) 38 *Marketing Intelligence & Planning.*

Sobia Bashir *et al,* 'Impact of Online Consumer Protection Laws on E-Commerce in Global Market' (2023) 9 *Pakistan Journal of Social Research.*

Subba Rao & Glenn Metts, 'Electronic Commerce Development in Small and Medium Sized Enterprises: A Stage Model and its Implications' (2003) *Business Process Management Journal*.

Sugeng & Annisa Fitria, 'Legal Protection of E-Commerce Consumers Through Privacy Data Security' (2020) 549 *Advances in Social Science, Education and Humanities Research.*

Sumit Badotra & Amit Sundas, 'A Systemic Review on Security of E-Commerce Systems' (2021) *International Journal of Applied Science and Engineering*.

Thomas van Dyke *et al,* 'The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce' (2007) 17 *Electronic Markets*.

Torie Atkinson, 'A Fine Scheme: How Municipal Fines Become Crushing Debt in the Shadow of the New Debtor's Prisons' (2016) 51 *Hard Civil Rights-Civil Liberties Law Review*.

Tsebetso Mapeshoane & Shaun Pather, 'The Adoption of E-Commerce in the Lesotho Tourism Industry' (2016) *The Electronic Journal of Information Systems in Developing Countries.*

Tyler Shanahan *et al,* 'Getting to know you: Social media personalization as a means of enhancing brand loyalty and perceived quality' (2029) *Journal of Retailing and Consumer Services*.

Dr. Ujwala Shinde, 'Conciliation as an Effective Mode of Alternative Dispute Resolution System' (2012) 4 *Journal of Humanities and Social Science*.

Xiang Liu and Others, 'Cyber security threats: A never-ending Challenge for E-Commerce' (2022) *Frontiers of Psychology*.

Zlatan Moric *et al,* 'Protection of Personal Data in the Context of E-Commerce' (2024) *Journal of Cybersecurity and Privacy*.

Theses and dissertations

'Mamofana Lichaba, 'The Lesotho Electronic Transactions and Electronic Commerce Bill 2013: An Appraisal' (LLM thesis, University of Pretoria 2015).

'Mamots'eli Ntlatlapa. 'The Determinants of Mobile Money Adoption and Usage: The Case of Lesotho' (Master's thesis, University of the Free State 2017).

'Mamotumi Maliehe, 'Cybercrime Legislation for Lesotho' (LLM dissertation, University of Cape Town 2007).

'Matsepo Kulehile, 'An analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and the SADC region' (Doctor of Philosophy thesis, University of Cape Town 2017).

Online websites

Annie Laukaitis, 'Building Strong Ecommerce WEBSITE security to Combat Online Attacks' (2024) https://www.bigcommerce.co.uk/articles/ecommerce/ecommerce-website-security/ Accessed 9 December 2024.

Ben Kazinik, 'The History of e-Commerce- How it All Started' (28 March 2024) https://www.mayple.com/blog/history-of-ecommerce Accessed 17th October 2024.

Bob Tedeschi, 'E-Commerce Report; Some online sellers are hiring prominent auditors to verify their privacy policies and increase trust.' *New York Times* (18 September 2000) 12. https://www.nytimes/2000/09/18/business/e-commerce-report-some-online-sellers-are-hiring-prominent-auditors-verify-their.html Accessed 22 December 2024.

Cameron Hashemi-Pour & Stephen Bigelow, 'What is Data Privacy?' (TechTarget 18 July 2024) https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy Accessed 26th November 2024. Accessed 17th November 2024.

Dr. Mats'epo Kulehile, 'Digital Rights in Lesotho: A Situational Analysis' (Transformation Resource Centre, 2023) https://www.trc.org.ls/documents/ Accessed 19 December 2024.

Erwan Mahoundo, 'The Growing Threat of Third-Party Cyber Risks' (Senscy, 2023) https://senscy.com/the-growing-threat-of-third-partycyber-risks/ Accessed 8 January 2025.

General Data Protection Regulation, 'Right to be Informed' (2 August 2018) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed-1-0.pdf Accessed 17 January 2025.

Global Encryption Coalition, 'Encrypt to Protect: Empowering Lesotho with Digital Security' (2024) https://www.globalencryption.org/2024/09/encrypt-to-protect-empowering-lesotho-with-digital-security-2024/ Accessed 28th November 2024.

James Robinson, 'Internet as the Scene of Crime' (International Computer Crime Conference, 29-31 May 2000) http://www.usdoj.gov/criminal/cybercrime/roboslo.htm Accessed 6 January 2025 Accessed 6th January 2025.

Karabo Nkolanyane, 'How e-commerce and digital platforms have changed the game for businesses through the pandemic' *Lesotho Times* (Maseru, 8th September 2021) https://lestimes.com/how-e-commerce-and-digital-platforms-have-changed-the-game-for-businesses-through-the-pandemic/ Accessed 9th November 2024.

Kyle Chin, 'The Role of Cybersecurity in Protecting E-Commerce Companies' (UpGuard, 18 November 2024) https://www.upguard.com/blog/how-cybersecurity-protects-ecommerce-companies Accessed 6 January 2025.

Marija Batarelo, 'What is a Record of Processing Activities (ROPA)?' (Parser Compliance, 15th December 2022) https://dataprivacymanager.net/records-of-processing-activities/#:~:text=Record%20of20processing%20activities%20should,remove%20information%20ascircumstances%20change. Accessed 21st March 2025.

Matthew Kosinski, 'What is data breach?' https://www.ibm.com/think/topics/data-breach Accessed 16 December 2024.

Mayet & Associates, 'The Data Protection Act in Lesotho' (22 February 2022) https://zmayetlaw.co.ls/data-protection-in-Lesotho/ Accessed 6 March 2025.

National Digital Policy (2024) Ministry of Communication, Science, Technology and Innovation https://www.gov.ls/download/draft-national-digital-transformation-policy-2024/ Accessed 28th November 2024.

Nedim Maric, 'Data Breaches: Causes, Compliance, and Best Practices' (6th September 2024) https://brightsec.com/blog/data-breaches-causes-impact-and-best-practices/ Accessed 6th March 2025.

Smart Insights, 'Convenience is driving e-commerce growth and influencing consumer decision' (28 January 2020) https://www.smartinsights.com/ecommerce/customer-experience-examples/convenience-is-driving-e-commerce-growth-and-influencing-consumer-decisions/ Accessed 7th November 2024.

Tokelo Khausela, 'CBL Speaks on Cyber Attack' *Lesotho Times* (Maseru, 13th February 2024) https://lestimes.com/cbl-speaks-on-cyber-attack/ Accessed 28th November 2024.

Tony Ademi, 'Impact of Data Breach in E-commerce' (The Cyber Research Databank, 16 July 2024) https://www.cyberdb.co/impact-of-data-breach-in-e-commerce/ Accessed 23 January 2025.

United Nations Commission on International Trade Law, 'UNCITRAL Model Law on Electronic Commerce' (1996) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce Accessed 23 November 2024.