

https://dspace.org/

Investigating the impact of the cybercrime legislation on online purchasing behaviour in South Africa

Phofu, Maletsema

2025

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/49266

Phofu, Maletsema . (2025). Investigating the impact of the cybercrime legislation on online purchasing behaviour in South Africa [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/49266

Downloaded from a DSpace repository. https://dspace.org/

Investigating the impact of the cybercrime legislation on online purchasing behaviour in South Africa

Maletsema Phofu

Student number - 1840247

Student email: 1840247@students.wits.ac.za

Supervisor: Dr Kiru Pillay

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2025

ABSTRACT

This research investigates the impact of South African cybercrime legislation on online purchasing behaviour. The study aims to understand the adequacy and effectiveness of the legislative framework in reducing perceptions of online risk and increasing consumer trust in e-commerce platforms.

The research employs a qualitative approach, analysing data from legal experts, cybersecurity specialists, and academics. Key findings indicate that while South Africa has a robust legislative framework, its implementation is hindered by complexity, lack of awareness, and insufficient enforcement.

The study concludes that enhancing legislative clarity, increasing public awareness, and improving enforcement mechanisms are crucial for fostering consumer trust and promoting the growth of e-commerce in South Africa.

KEYWORDS

e-commerce, consumer intention, trust, risk management, cybersecurity, cybercrime, regulation, self-regulation

TABLE OF CONTENTS

LIST OF TABLES vi

LIST OF FIGURES vii

LIST OF ACRONYMS viii

CHAPTER 1. INTRODUCTION 1

1.1 STATEMENT OF PURPOSE 1
1.2 BACKGROUND OF THE STUDY 1
1.3 RESEARCH PROBLEM 4
1.4 RESEARCH QUESTIONS 5
1.5 DELIMITATIONS OF THE STUDY 6
1.6 DEFINITION OF TERMS 6
1.7 ASSUMPTIONS 6
1.8 CHAPTER OUTLINE 7

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 8

2.1 INTRODUCTION 8
2.2 BACKGROUND DISCUSSION 8
2.3 TO WHAT EXTENT DOES THE SOUTH AFRICAN REGULATORY FRAMEWORK ADDRESS E-COMMERCE SECURITY RISKS? 12
2.3.1 GENERAL SOUTH AFRICAN E-COMMERCE CONSUMER EXPERIENCE AND TRENDS 12
2.3.2 E-COMMERCE SECURITY RISKS IN SOUTH AFRICA 14
2.3.3 PREVALENCE OF E-COMMERCE CYBERCRIMES IN SOUTH AFRICA 15
2.3.4 THE REGULATORY FRAMEWORK FOR THE SECURITY OF E-COMMERCE IN SOUTH AFRICA 17
2.3.5 ECT ACT AND E-COMMERCE SECURITY 19
2.3.6 POPIA AND E-COMMERCE SECURITY 20
2.3.7 CIPA AND E-COMMERCE SECURITY 22
2.3.8 RICA AND E-COMMERCE SECURITY 22
2.3.9 PAIA AND E-COMMERCE SECURITY 23
2.3.10 CPA AND E-COMMERCE SECURITY 23
2.3.11 CYBERCRIMES ACT IN THE CONTEXT OF E-COMMERCE SECURITY 24
2.3.12 LEGISLATIVE FRAMEWORKS AROUND THE WORLD 25
2.3.13 E-COMMERCE AND THE CONCEPT OF SELF-REGULATION 30
2.3.14 PROPOSITION 1 31
2.4 TO WHAT EXTENT DOES THE SOUTH AFRICAN REGULATORY FRAMEWORK ADDRESS E-COMMERCE PROSECUTION OF CYBERCRIMES? 33
2.4.1 POLICING OF CYBERCRIMES IN SOUTH AFRICA 33

2.4.2 PROSECUTION OF CYBERCRIMES IN SOUTH AFRICA 34
2.4.3 PROPOSITION 2 35
2.5 HOW DOES THE CYBERCRIME LEGISLATION BUILD SOUTH AFRICAN CONSUMERS' TRUST IN E-COMMERCE? 35
2.5.1 ELEMENTS OF TRUST 36
2.5.2 LEGISLATION AS A MEANS TO CREATE TRUST 37
2.5.3 PROPOSITION 3 37
2.6 ANALYTICAL FRAMEWORK 38
2.6.1 THEORETICAL FRAMEWORK 38
2.6.2 CONCEPTUAL FRAMEWORK 40
2.7 CONCLUSION OF LITERATURE REVIEW 41
2.7.1 PROPOSITION 1.1 42
2.7.2 PROPOSITION 1.2 42
2.7.3 PROPOSITION 1.3 42
2.7.4 PROPOSITION 2.1 42
2.7.5 PROPOSITION 3.1 43
2.7.6 PROPOSITION 3.2 43
2.7.7 PROPOSITION 3.3 43
2.7.8 PROPOSITION 3.4 43

CHAPTER 3. RESEARCH METHODOLOGY 44

3.1 RESEARCH APPROACH 44
3.2 RESEARCH DESIGN 44
3.3 DATA COLLECTION METHODS 45
3.4 POPULATION AND SAMPLE 45
3.4.1 POPULATION 45
3.4.2 SAMPLE AND SAMPLING METHOD 46
3.5 THE RESEARCH INSTRUMENT 47
3.6 PROCEDURE FOR DATA COLLECTION 47
3.7 DATA ANALYSIS STRATEGIES AND INTERPRETATION 48
3.8 POSSIBLE LIMITATIONS AND CHALLENGES OF THE STUDY 49
3.9 QUALITY ASSURANCE 49
3.9.1 TRANSFERABILITY 49
3.9.2 CREDIBILITY 49
3.9.3 DEPENDABILITY 49
3.9.4 OBJECTIVITY AND CONFIRMABILITY 50
3.10 ETHICAL CONSIDERATIONS 50

CHAPTER 4. PRESENTATION OF FINDINGS 51

4.1 INTRODUCTION 51
4.2 DEMOGRAPHIC PROFILE OF RESPONDENTS 51
4.3 RESULTS PERTAINING TO PROPOSITION 1 52
4.4 RESULTS PERTAINING TO PROPOSITION 2 61

4.5 Results Pertaining to Proposition 3 65
4.6 Summary of the results 72

CHAPTER 5. DISCUSSION OF THE FINDINGS 74

5.1 Introduction 74
5.2 Discussion pertaining to Proposition 1 74
5.3 Discussion pertaining to Proposition 2 81
5.4 Discussion pertaining to Proposition 3 85
5.5 Theoretical alignment of findings 89
5.6 Conclusion 91

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS 93

6.1 Introduction 93
6.2 Conclusions regarding research question 1 93
6.3 Conclusions regarding research question 2 94
6.4 Conclusions regarding research question 3 94
6.5 Recommendations 95
6.6 Suggestions for further research 96

REFERENCES 99

APPENDIX A: Participant Information Sheet 114

APPENDIX B: Participant Agreement Form 115

APPENDIX C: Interview Questionnaire 116

LIST OF TABLES

Table 1 ..... **26**

Table 2 ..... **27**

Table 3 ..... **29**

Table 4 ..... **29**

Table 5 ..... **31**

Table 6 ..... **46**

Table 7 ..... **51**

Table 8 ..... **54**

Table 9 ..... **56**

Table 10 ..... **58**

Table 11 ..... **58**

Table 12 ..... **64**

Table 13 ..... **67**

Table 14 ..... **68**

Table 15 ..... **69**

Table 16 ..... **70**

Table 17 ..... **73**

Table 18 ..... **97**

LIST OF FIGURES

Figure 1 1

Figure 2 19

Figure 3 39

Figure 4 40

Figure 5 75

Figure 6 89

LIST OF ACRONYMS

CCPA – California Consumer Privacy Act

CIPA – Critical Infrastructure Protection Act, No. 8 of 2019

ECT Act - Electronic Communications and Transactions Act, No. 25 of 2002

GDPR – General Data Protection Regulation

LGPD – Lei Geral de Protecao de Dados (Brazil)

NCPF – National Cybersecurity Policy Framework

PAIA - Promotion of Access to Information Act, No. 2 of 2000

POPIA – Protection of Personal Information Act, No 4 of 2013

RICA - Regulation of Interception of Communications and Provision of Communication-related information Act, No 70 of 2002

TIB – Theory of Interpersonal behaviour

TTP - Tactics, techniques, and procedures

UNCITRAL - United Nations Commission on International Trade Law

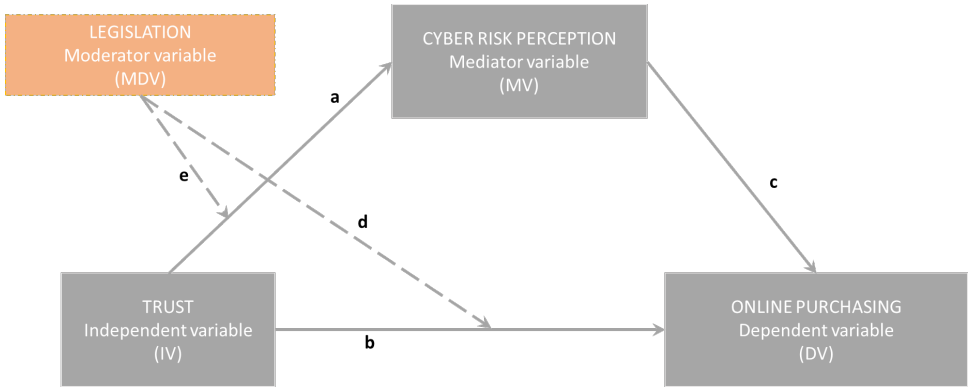
CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This qualitative study investigates the impact, specifically the adequacy and effectiveness of South African cybercrime legislation (the moderator), in reducing perceptions of online risk and increasing consumer trust in the use of e-commerce platforms for purchases.

Figure 1

Variables relationship



Note. Adapted from Peck & Smitherman (2015)

Figure 1 depicts cyber risk perception (moderator variable) as a way in which trust, the independent variable, impacts online purchase behaviour, the dependent variable. This study investigates the effect of the South African legislation, as moderator variable (d)(e) on the direction and strength of the relationship between trust and the intention to shop online.

1.2 Background of the study

The widespread use of the internet has altered how nations do business internationally. Since its inception in the 1990s, e-commerce is forcing

businesses to adoption of new hybrid business models and cater for changes in consumer expectations in the South African markets (Freeme & Gumede, 2012; Makhitha, 2014). E-commerce refers to a business model where a retailer and consumer use a digital platform to sell and purchase goods. E-commerce plays an important role in enhancing economies in developing countries (Corbitt et al., 2003; Lim et al., 2021).

E-commerce in South Africa is growing at a fast pace, the adoption acceleration particularly took place during the Covid-19 lockdown. South African e-commerce market grew by 19% in 2021, generating a revenue of US$5 billion and placing the country as the 41st largest e-commerce market in the world, with the biggest players being Takealot, Superbalist, Woolworths, Mr Price, and Amazon.com (The eCommerce market in South Africa, n.d.). With e-commerce, these retailers were able to reach markets in secluded geographical areas, and improve their productivity and efficiencies (Lim et al., 2021). Online shopping however presents a challenge in that the consumer is unable to touch and feel the products, they are unable to take possession of the purchases immediately (Makhitha & Ngobeni, 2021).

Corbitt et al. (2003) suggest trust as the cornerstone of e-commerce. Moreover, the perceived risks on an e-commerce platform affect consumers' trust and subsequent purchasing decisions (Glover & Benbasat, 2010; Netshirando et al., 2024; Makhitha & Ngobeni, 2021). Several concepts are associated with consumer interactions with the e-commerce platform, i.e. security, usefulness, ease of use, and convenience (Netshirando et al., 2024).

Security risks in e-commerce are complex due to affecting organisational, human and technical aspects (Netshirando et al., 2024; Warren & Hutchinson, 2003). Risk, specifically risk perception, is one's intuition, feelings, and judgment of the severity of consequences (Wilson et al., 2019), whilst a cybercrime can be loosely defined as an abuse of the e-commerce platform by performing transactions that are unauthorised (Akinyede et al., 2020).

As e-commerce adoption continues to rise, security risks and related cybercrimes in South Africa are also expected to rise and negatively impact consumers' trust. E-commerce is prone to risks of financial loss, product/service risk, privacy risk, delivery risk and security risk among others (Malapane, 2019; Makhitha & Ngobeni, 2021). Research shows that there is low trust in e-commerce in South Africa as compared to the traditional brick-and-mortar environment (Barnard & Wesson, 2005; Malapane, 2019; Makhitha & Ngobeni, 2021).

Retailers generally apply technical cybersecurity controls to minimise the actual security risks and reduce consumers' perception of the risk of transacting on their e-commerce platforms (Akinyede et al., 2020). E-commerce users also have certain practices they need to abide by such as using secure sites, and deletion of personal information when using public computers (Ezeji et al.,2018). This however is not enough as cybersecurity controls can be bypassed by determined cybercriminals.

The role of legislation

The law organises society and protects citizens' rights. The law only has value if there is a discipline in its application and its enforcement (De Jager, 2000). Conducting e-commerce transactions requires a law that recognises such transactions as valid and legally equivalent to paper money-based transactions. The law also has to stipulate the practice obligations of the e-commerce retailers towards consumer protection against cybersecurity risks and related crimes (Barkatullah, 2018) and, it needs to criminalize breaching of security controls and give powers to the relevant authorities to investigate and prosecute (Akinyede et al., 2020; Malapane, 2019; Ezeji et al.,2018).

This paper focuses on the quality of the South Africa's policy, legislative and regulatory frameworks related to e-commerce security risks (e.g. data protection and privacy, transaction safety, platform security) and e-commerce related crimes. The National Cybersecurity Policy Framework (NCPF) was adopted by the South African cabinet in 2012. The NCPF recognises the existence of cyberspace and considers cyber-attacks as an act of undermining the functioning

of information systems in both government and private sectors. It therefore declares the cybercrime acts of crime. The NCPF addresses the regulatory framework, coordination between government structures, awareness and skills and IT capacity.

No less than 6 Acts operationalise the NCPF. The Cybercrimes Act 19 of 2022 (Cybercrimes Act) aims to promote cybercrime reporting, investigation, criminalise, and penalise cybercrimes. The country also leverages the Electronic Communications and Transactions Act (ECT Act) of 2002 and the Protection of Personal Information Act 4 of 2013 (POPI Act) to promote trust in consumers engaging in electronic transactions.

1.3 Research problem

Risk management is an important aspect of successful e-commerce on which both the consumer and the retailer are focusing, with retailers continuously investing in cybersecurity controls to mitigate the risk and sustain their businesses (Toleuuly et al., 2020). On the other hand, Ezeji et al. (2018) argue that the prevention of cybercrimes has several role players and that it will take well-coordinated planning and investment to prevent cybercrimes in South Africa. Role-players include the legislative framework, criminal justice system and community.

According to Malapane (2019), one of the challenges facing South Africa is the inadequate direction and enforcement from the government in dealing with e-commerce cybersecurity risks and crimes. Ezeji et al. (2018) also found that the legislative framework is not a sufficient deterrent for cyber criminals in conjunction with a lax enforcement thereof.

With an emergent cybersecurity and cybercrime legislative framework in South Africa, there is however a limited understanding to whether this emerging legislative framework can mitigate the cybersecurity risks in the e-commerce domain.

1.4 Research questions

Can South Africa mitigate e-commerce cybersecurity risks and successfully prosecute cybercrimes? Is the legislative framework bringing confidence to the consumer and promoting e-commerce?

Previous research has largely focussed on identifying factors affecting consumer trust, identification of e-commerce risks, and how to increase consumer trust worldwide and in South Africa (Lim et al., 2021; Barnard & Wesson, 2005; Malapane, 2019; Makhitha & Ngobeni, 2021; Glover & Benbasat, 2010; Bramall et al., 2004). Furthermore, the inadequacy of the legislative framework in cybersecurity in South Africa has been mentioned by various authors, notwithstanding the promulgation of the Cybercrimes Act. The obvious question relates to whether the Cybercrimes Act brings confidence to e-commerce consumers, or if South Africa is wedged in a web of legislative complexity?

A good or complex legislative framework is characterised by volume (i.e. number of legislations and policies to address a need; average number of pages, etc), quality (i.e. addresses political, social, legal objectives, harmonious, integrated and identifies basic principles), perception of its consistency, and effect on user's experience (When Laws Become Too Complex: A review into the causes of complex legislation, 2013).

In domains such as Quality Management and Health, Nenadal (2016) uses adequacy, suitability, effectiveness, and efficiency factors to assess the ISO 9001:2015 standard used for Quality Management Systems. The World Health Organization (WHO) developed several self-assessment tools for countries to evaluate their public health operations (WHO, nd). Molinuevo & Sez (2014) developed the Regulatory Impact Assessment (RIA) Toolkit. And this has been used extensively throughout the world, including in South Africa. These tools have in common the ability to identify weaknesses for strengthening the laws, standards, or operations in areas they are applied in.

This study aims to answer the following questions:

Research question 1: To what extent does the South African regulatory framework address e-commerce security risks

Research question 2: To what extent does the South African regulatory framework address the prosecution of cybercrimes?

Research question 3: How does the cybercrime legislation build South African consumers' trust in e-commerce?

1.5 Delimitations of the study

This study covers South African cybersecurity-related legislation to identify e-commerce retailers' and experts perceptions of their adequacy in addressing cybersecurity risks and crimes in the e-commerce domain. The aim is to seek insight into legislative volume, quality, consistency, and experience toward reducing their perceived e-commerce risks and prosecution of crimes.

The study will be conducted in South Africa with e-commerce consumers and retailers.

1.6 Definition of terms

Consumerism is defined as an encouragement of consumer interest to consume goods or services (Siyanbola et al., 2022)

1.7 Assumptions

The study focuses on the perceptions of e-commerce retailers and experts on the legislation's ability to reduce perceived risk and drive e-commerce consumerism. The following assumption is made:

E-commerce utilitarian and hedonic values do not affect consumers' perception of government legislation.

1.8 Chapter Summary

This chapter presented a high-level view of the role of the South African legislation in relation to the reduction of perceived online risks and fostering consumer trust in e-commerce. It highlighted the rapid growth of e-commerce in South Africa, especially following the Covid-19 pandemic, and notes ongoing concerns about security risks and low consumer trust compared to traditional retail environments. It further explored the law's ability to successfully protect users and deter cybercrimes.

Three key research questions emerged as follows:

- How well does South Africa's regulatory framework address e-commerce security risks?
- To what extent does it enable the successful prosecution of cybercrimes?
- Does legislation improve consumer trust in e-commerce?

1.9 Report Outline

The remainder of this paper is structured as follows: Chapter 2 presents the literature review and findings regarding the South African cybersecurity legislation and e-commerce together with the theory of interpersonal behaviour. Based on this theory, the theoretical and conceptual frameworks are outlined. The chapter concludes with the proposition statements for consideration.

Chapter 3 explains the research paradigm, methodology and methods to be used for collection and analysis of data this research study.

Chapter 4 presents the data from the interviews conducted whilst the analysis is done in Chapter 5, followed by conclusion and recommendations in Chapter 6.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This chapter starts off by explaining the literature search strategy, and this is followed by a detailed discussion of concepts of trust, perceived risk, use of e-commerce, and their relationship to e-commerce. Following that, a discussion is presented from a South African perspective on the e-commerce cybersecurity risks and crime and different legislations that affect these concepts by zooming into each legislation's content. Following this, an international view of how Africa at large, the United States & North America, Asia and Europe address e-commerce cybersecurity risk and crimes from a legislative point of view. This chapter concludes with a summary and reiterates the proposition statements.

2.2 Background discussion

Literature Search Strategy

The first step involved identifying the main concepts related to the research topic, such as "cybercrime legislation," "online purchasing behaviour," "South Africa," "e-commerce security," and "consumer trust". A list of relevant keywords and phrases, including synonyms and related terms, was developed to ensure a broad search. For example, terms like "cybersecurity," "data protection," "e-commerce regulation," "consumer protection," and "digital trust" were used (Aromataris & Riitano, 2014).

The search was conducted using Wits University Library's academic databases and Google Scholar to find peer-reviewed journal articles, conference papers, and research reports. Legal databases like LexisNexis were accessed for legislation, case law, and legal commentary. Additionally, government and

institutional websites, such as the South African Government, African Union, and United Nations, were included for official documents and reports.

The second step was to conduct a search in the databases and sources using the identified keywords and phrases. Boolean operators (AND, OR, NOT) were used to refine search results and ensure comprehensive coverage. For example, searches like "cybercrime legislation AND e-commerce" or "data protection OR privacy laws" were performed. Filters were applied to narrow down results to the most relevant and recent publications, focusing on the last 10 years to ensure up-to-date information (Aromataris & Riitano, 2014).

The abstracts and summaries of the retrieved articles were reviewed to assess their relevance to the research topic. Literature that provides insights into the impact of cybercrime legislation on online purchasing behaviour, implementation of law, the effectiveness of regulatory frameworks, and the role of consumer trust in e-commerce was selected. Studies conducted in South Africa, the African continent or similar contexts were prioritised to ensure the applicability of the findings. The selected literature was categorised into themes, summarised and propositions statements developed as outlined in the rest of this chapter (Aromataris & Riitano, 2014).

Trust

The construct of trust is defined by Gefen et al. (2003) as the trustor’s willingness to engage in risky behaviour, furthermore, the author suggests that there is a difference between trust and trustworthiness, that the latter being a perception of how trustworthy the trustee is to the trustor. Ganesan & Hess (1997) views level of trust as being either interpersonal or organisational, and that trust can be conceptualized as a belief or expectancy held by either an individual or a group. Gefen et al. (2003) and Ganesan & Hess (1997) agree that trust is both a unidimensional and multidimensional construct. Trust has been associated with dimensions such as credibility, commitment, benevolence (Ganesan & Hess, 1997), belief (Hussain et al., 2008), surety, honesty (Alsharif et al., 2018),

confidence, reliability (Mofokeng, 2021) and, vulnerability acceptance (Bramall et al., 2004).

Trust is important in e-commerce as it is not tangible and cannot be seen by the consumer but determines their willingness to purchase online. It, therefore, becomes imperative that the seller creates an impression and gives out those signals that drive the consumers' willingness to purchase. Corbit et al. (2003) give examples of creating these trust impressions. The seller can drive a positive consumer experience on their website, by providing competent technical support, and by having a quality website.

Risk

The construct of risk perception also affects consumers' behaviour and their willingness to buy. Geffen et al. (2003) argue that general research has confused the relationship between trust and risk perception. Literature offers three relationship scenarios: 1) That risk perception is a mediator between trust and willingness to purchase. A mediator affects the outcomes of willingness to purchase (Peck & Smitherman, 2015). 2) That risk perception is a moderator between trust and willingness to purchase. A moderator enhances the understanding of the relationship between trust and willingness to purchase (Netshirando et al., 2024; Walsh et al., 2008). And 3) That the trust and risk perception are independent.

Risk perception is a synthesis of positive and negative outcomes expected from the desired action; probabilities of a certain outcome during uncertain conditions; and individual perception of uncertainty and adverse consequences (Netshirando et al., 2024; Gefen et al., 2003; Hussain et al., 2008; Glover & Benbasat, 2010). From the literature, trust and risk perception are negatively correlated and like the trust construct, risk perception is both a unidimensional and multidimensional construct.

E-commerce

The use of e-commerce is imploding worldwide and in South Africa despite the perceived risks. This implosion is brought upon by the diversification of companies moving from brick-and-mortar stores to online stores to pursue growth opportunities offered by e-commerce platforms (Makhitha & Ngobeni, 2021). Barnard & Wesson, 2005; Mofokeng, 2021; and Netshirando et al., 2024 highlight the imperativeness of South African companies to build trusted relationships with their consumers. In their view, this relationship-building consists of retailers providing enough and correct information for decision-making by the consumer, company policies and guarantees, and linking to reputable sources – for example, trusted payment gateways such as PayPal, PayFast, Visa etc. South African research shows that consumers know the risks of transacting online. When they perceive the risk to be high, they are most likely to use the e-commerce platform for information gathering, then proceed to make the purchase in a traditional store where possible, where not possible, the value of the purchase will be lower based on their tolerance level to the risk of losing money (Barnard & Wesson, 2005).

Glover & Benbasat (2010) and Knuth et al. (2014) make a distinction between objective and perceived risk. Objective risk is the actual existing risk or hazard, for example, an e-commerce website that lacks security controls such as a digital signature, whilst perceived risk is subjective and based on personal judgement. Objective risk affects risk perception.

The South African literature has identified several e-commerce risks. Netshirando et al. (2024) note that data breaches at companies, academic institutions and government entities continue to erode consumers' confidence in handling cyber risks. Malapane (2019) categorised the risks into data corruption, denial of services, data exposure, system penetration and financial loss. Ezeji et al. (2018) though referring to these terms as cybercrimes, mention identity theft, distributed denial of services attacks, hacking, phishing, and malware, amongst others, whilst Barnard & Wesson (2005) refers to financial security risk. Against this backdrop, this study investigates the ability of the legislations as an instrument

that establishes trustworthiness, cooperation, enable information sharing and provides security direction for the e-commerce stakeholders and promoting use of e-commerce.

2.3 To what extent does the South African regulatory framework address e-commerce security risks?

This section critically assesses cyber risks prevalent in South Africa, furthermore, it focuses on various South African legislations in their current form and to what extent they address e-commerce cybersecurity risks.

2.3.1 *General South African e-commerce consumer experience and trends*

2022 South African Digital Customer Experience Report presents e-commerce adoption and spend trends for the past for years of over 22 000 survey participants. 87% of the participants made an online purchase in 2022. Over half of the participants had a household income of less that R10 000, dispelling the notion that only the wealthy shop online. The trend shows a 5% increase in e-commerce adoption and a 40% increase in spending between 2021 and 2022 hitting the R56,8 billion mark. Local websites (67%), retailer apps (63%) and social media (48%) are the firm preferences versus the 33% international websites for the same period. New online shoppers were mostly attracted by specials specifically driven by Black Friday and Cyber Monday marketing campaigns (ZA CX Report, 2022).

According to extrapolation in this report, the online product research in the top four economic sectors—groceries, fashion, medicine/toiletries, and furniture/hardware—influence physical retail sales to the tune of R293.8 billion. One of the contributors in the report exhorts businesses to re-evaluate their strategies, warning that neglecting other channels and transactions that contribute to the greater structure of online buying is risky. That the definition of

e-commerce has been re-defined by the consumer behaviour making social selling, online marketplaces, customer reviews and search engines part of E-commerce ecosystem (ZA CX Report, 2022).

1% of the surveyed South Africans have interacted with the Metaverse, with 79% stating they will use it in the future (ZA CX Report, 2022). Metaverse is “a seamless convergence of our physical and digital lives, creating a unified, virtual community where we can work, play, relax, transact and socialize” (J.P Morgan, 2022). Big and small companies are venturing into this digital world with a potential to become an alternative world and offer same real-life activities including digital shopping.

Convenience (i.e. access to credit cards, various payment methods, multi channels, etc) is a key driver for e-commerce adoption however, online customer experience is what keeps the consumer buying over and over again (ZA CX Report, 2022; Gulfraz et al, 2022; Liu et al., 2022).

Customer experience can be interpreted as trust in the online platform, that their expectations will be met, throughout the purchasing process (Gulfraz et al, 2022). Demand delivery for example, has become a new commercial battle according to the report. For consumers that demand or expect same-day delivery, The winners will be the ones who can provide quick, seamless and reasonably priced deliveries. On the other hand, 22% of the survey participants prefers shopping on Takealot due to its product offering and reliable delivery. Amazon is set to enter the South African market in 2023 rendering them Takealot’s biggest competitor in the country. In a bid to protect its market share, Takealot is expanding into townships through partnerships (ZA CX Report, 2022; Dludla, 2022).

South African e-commerce consumer Based on the cases mentioned above, the survivors will be brands that can build a positive perception, and lock in consumers into their brand (ZA CX Report, 2022).

As alluded by the report in its fourth year of research, it shows that South Africans are more knowledgeable about how to use the internet. They are technology

savvy, they hold brands accountable for their price, speed and post-sale promises, and have expectations of outstanding service delivery – failing which, they switch between brands (ZA CX Report, 2022). Is the regulation able to keep up with ensuring secure practices?

2.3.2 *E-commerce security risks in South Africa*

Cybersecurity is defined by ISO/IEC 27032:2012 (n.d.) as the protection of privacy, integrity, and accessibility of data and information in Cyberspace. There are interactions in cyberspace, there is people, software, and technology at play. Security in cyberspace is made up of various security functions, i.e., the security of the network where the infrastructure sits, the security of the internet, the security of the infrastructure running on the network and the security of the information being shared cyberspace (ISO/IEC 27032:2012, n.d.).

Advances in the adoption of technologies, the digital transformation have also increased the threat landscape and attack tactics, techniques, and procedures (TTPs) (Ezeji et al., 2018). South Africa is an attractive target for cyber-attacks, a safe haven (Cassim, 2011; Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020). Cybersecurity risks faced by South African e-commerce retailers are: Distributed denial of service attacks, malware and ransomware infections, data theft and fraud (Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020); identity theft, hacking and phishing (Ezeji et al., 2018). Malapane (2019) categorises the risks into data corruption, denial of services, data exposure, penetration of the system and financial loss.

Cybercrime is a lucrative business, with cybercriminals raking in atleast $1.5 trillion annually. Focus on risk management by both retailers and the government is therefore critical (Ilyin, 2014; Polk, 2021; Greig, 2020; Goodchild, 2019). Risk management enables an organisation to prepare for a cyberattack by putting in place measures for preventing the attack, or minimizing the impact thereof, and resilience (ISO/IEC 27032:2012, n.d.).

2.3.3 *Prevalence of e-commerce cybercrimes in South Africa*

During a cybercrime, the computer objects become both the object of crime and the subject of crime. Cybercrimes are borderless and require no physical presence between the perpetrator and the victim (Cassim, 2011). Herselman & Warren (2004) agrees and further argue that cybercrimes have very little difference from other crimes and that some murders can also be attributed to cybercrime, for example, if a hacker were to successfully take control of a flight control system of a flight full of passengers and plunge that flight into its demise, that can be considered a cybercrime.

Cassim (2011) alludes to the inability of African leaders to give proper focus to cybercrimes due to being pre-occupied with other priorities such as eradication of poverty, reducing AIDS infections, fighting traditional crimes, and political- and ethnic instability amongst others. This has led to cybercrimes thriving in Africa. This problem is compounded by a general lack of cybersecurity education and insufficient supporting legal frameworks in Africa.

South Africa is no different. In President Cyril Ramaphosa's 2022 State of the Nation Address (SONA), the economic recovery post the Covid19 pandemic, the strengthening of democracy, job creation through small, medium and micro enterprises, electricity crisis, infrastructure development, immigration laws, spectrum auction, state capture, the state of state-owned enterprises, social grants, youth employment, land expropriation and civil unrest were the highlights of his speech (President Cyril Ramaphosa: 2022 State of the Nation Address | South African Government, 2022). A National Budget traditionally follows the SONA speech, outlining financial priorities that enable items of the president's speech. Cybercrime was not in the president's 2022 SONA speech and it did not feature in the 2022 finance minister's budget speech. 2023 SONA was no different. Loadshedding, employment stimulus, crime, and access to quality education were high on the agenda and the fiscal budget (President Cyril Ramaphosa: 2023 State of the Nation Address | South African Government, 2023).

Some notable cybersecurity attacks launched on South African platforms are Garmin South Africa in 2019, where customer payment data was stolen on their e-commerce platform. Malicious code was injected onto their e-commerce platform leading to 6700 South African customers' data which included their card numbers and CVV codes being stolen (Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020). A prepaid electricity provider was infected by ransomware also in 2019 which encrypted their data leaving customers unable to make electricity purchases on the e-commerce website (Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020). In March 2022, TransUnion, a credit bureau, suffered a data breach that exposed 54 million personal records of citizens whilst Dischem, a pharmacy retail giant, suffered an attack in April same year that resulted in exposure of over 3,6 million customer records. Both these incidents triggered a notification to the Information Regulator as required by Protection of Personal Information Act (POPIA) (ITWeb, 2022).

Interpol, via African Joint Operation against Cybercrime (AFJOC), whose objectives includes collection and analysis of cybercriminal activity, found that South Africa accounted for more than half of Business Email Compromise (BEC) that happened in Africa. Africa represented 0.75% of global BEC attempts between 2021 and 2022, furthermore, it was found that South Africa is the most targeted with ransomware attacks in Africa, accounting for 42% of the detected attacks. Government agencies, education entities, energy, retail and consumer goods were the most attacked (Interpol, 2023).

Cybercrimes are detrimental to South African businesses. Victims of crime often lose millions through theft, unavailability of services, recovery of services and brand reputational damage. Businesses are also unwilling to discuss these attacks in public due to the risk of further eroding consumer trust in the company (Herselman & Warren, 2004).

It was only after the enactment of ECT Act in July 2002 were these acts prosecutable in the court of law (Herselman & Warren, 2004).

2.3.4 *The regulatory framework for the security of E-commerce in South Africa*

Adopted by the South African Cabinet in 2012, The National Cybersecurity Policy Framework (NCPF) is the epicentre of cybersecurity. It is the national cybersecurity strategy and provides focus and coordination of cybersecurity activities against cyber threats for the organs of state within the Justice Crime Prevention and Security (JCPS) cluster, i.e., Ministries of Police, Defence and Military Veterans, Justice and Correctional Services, Home Affairs, State Security and Finance. One of the outcomes expected from the JCPS is the combatting and investigation of cybercrimes so that “All people of South Africa are and feel safe” (Malatji et al., 2021; Ntsaluba, 2017; Sutherland, 2017; The Presidency, 2014, Fowler & Maranga, 2022).

The JCPS objective of “All people of South Africa are and feel safe” (The Presidency, 2014) aligns with the e-commerce factors of consumer perceived risk that is uncertainty and adverse consequences (Glober & Benbasat, 2010; Liebermann & Stashevsky, 2002). Perceived risk in e-commerce is a major factor in decision making and a potential barrier to e-commerce. Some notable concerns from consumers' perspectives are the privacy and security of e-commerce platforms (Liebermann & Stashevsky, 2002).

According to Fowler & Maranga (2022), the NCPF policy is comprehensive and proactive. Its key strengths are its emphasis on public-private partnerships, education, promotes fundamental rights of the citizens through privacy, dignity and freedom of expression, and international cooperation. It brings coherent approach to cybersecurity measures, management, and response activities to bring trust in the use of country’s ICT infrastructure. Furthermore, its aim is to establish trust and confidence in secure use of ICT.

NCPF requires that a risk assessment of threats be conducted, and security measures be identified and prioritised accordingly. The implementation requires mobilisation of numerous state organs, clusters, state agencies and reference to

other legislations and policies (Malatji et al., 2021; Ntsaluba, 2017; Sutherland, 2017) Further downsides are highlighted by Fowler and Maranga (2022) that the NCPF neglects to establish trust-building initiatives, does not cover emerging technologies such as cloud and internet of things security, and neglects to hold manufacturers accountable to international security standards.

NCPF draws from international legislations such as North Atlantic Treaty Organisation (NATO) and concerns have been raised on its suitability, administrative and technological capabilities for use in the South African context. Some of the concerns emanate from its design using foreign legislative texts and experiences (Sutherland, 2017).

To support the implementation of NCPF, South Africa has a plethora of cybersecurity legislations promoting the general security of cyberspace. Malatji et al. (2021) identified no less than 37 pieces of policies and legislations that drive the implementation of NCPF and several organs of state within and outside of the Justice Crime Prevention and Security (JCPS) cluster, these are: Ministry of State Security, State Security Agency, Communication and Digital Technology, Department of Defence, Higher Education, Science and Innovation, South African Police Service, Justice, and National Prosecuting Authority. The private sector and civil society are also part of the national cybersecurity system. They form a collaboration with the government.

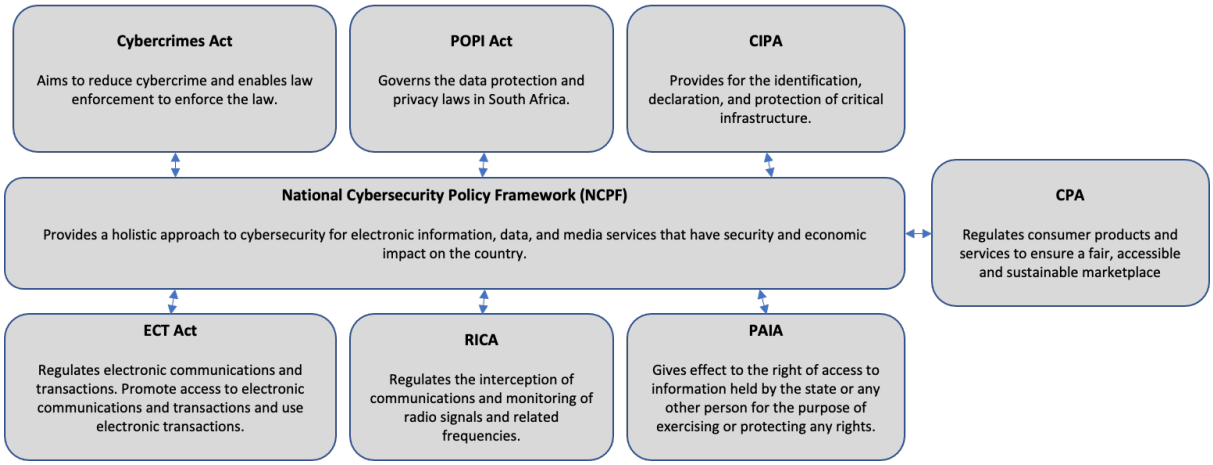
7 key legislations are key to the implementation of the NCPF as stipulated in figure 2 below, and these forms the scope of legislations under review for this study (Malatji et al., 2021).

- Cybercrimes Act, No.19 of 2020
- Promotion of Protection of Personal Information Act (POPIA), No. 4 of 2013 (herein referred to as POPIA)
- Critical Infrastructure Protection Act, No. 8 of 2019 (herein referred to as CIPA)

- The Regulation of Interception of Communications and Provision of Communications-Related Information Act, No. 70 of 2002 (herein referred to as RICA)
- Electronic Communications and Transaction Act, No. 25 of 2002 (herein referred to as ECT Act)
- Promotion of Access to Information Act, No. 2 of 2000 (herein referred to as PAIA)
- Consumer Protection Act, No. 68 of 2008 (herein referred to as CPA)

Figure 2

National cybersecurity policy and key legislations in South Africa



Note. Adapted from Malatji et al. (2021)

2.3.5 *ECT Act and e-commerce security*

According to Snail (2008) before the ECT Act was enacted in 2002, prosecution of cybercrimes was based on statutory and common laws although there was a limitation when it came to application of adjudication of online crimes. The statutory and common laws could be applied to online crimes such as cyber fraud and child pornography but unable to be applied on other online crimes like phishing, theft, and extortion (Ntsaluba, 2017).

ECT Act's focus is on e-commerce, however, it cannot be read and applied in isolation from common law. It applies to any form of electronic communication including emails, telephone, videos and internet. It defines how online contracting and transactions should be carried out. According to Ntsaluba (2017), the ECT Act is based on United Nations Commission on International Trade Law (UNCITRAL) which is a legal framework for international trade. It provides legislative and non-legislative texts used for negotiating transactions and harmonization of trades. Unlike the NCPF, the responsibility of implementation of this act falls on the Ministry of Communications.

Several salient points to note with regards to e-commerce in this act:

- The legislation scope is wide, complex, and requires application in conjunction with other acts such as CPA and PAIA
- Consumer protection contains several assurances for the e-commerce consumer to enable them to trust the retailer and assurances related to protection of personal information during transactions. This contributes to the consumer's level of perceived risk.
- There is provision for managing objective risk through controls set for protection of critical infrastructure (databases), cryptography and authentication service provisioning.
- Fraud was raised by several literatures as a concern for e-commerce, the legislation specifically addresses this concern.

2.3.6 *POPIA and e-commerce security*

The Protection of Personal Information Act (POPIA), No. 4 of 2013 is an equivalent of European Union General Data Protection Regulation (GDPR), which imposes obligations to companies that collect personal data and issue fines for violations (Jones, 2021). POPIA also defines minimum standards to organisations collecting, processing, and sharing personal data. Like GDPR, POPIA violations can result in a fine of up to R10 million or imprisonment of up to 10 years. These standards are meant to protect consumer from being victims of

identity thefts, fraud and protect their privacy (Protection of Personal Information Act 4 of 2013 | South African Government, n.d.).

POPIA defines personal information as the information that can positively identify a person for example identity number, email address, physical address, online identities, criminal records, financial information and employment and salary information (Protection of Personal Information Act 4 of 2013 | South African Government, n.d.).

POPIA requires organisations to be responsible, exercise control, and that consumers' personal data be protected and consumer's privacy respected. POPIA necessitates that the data subject (person) must provide consent prior to their information being processed and this information be used solely for the purpose the data subject consented to (Jones, 2021). But what does it mean for security of e-commerce?

E-commerce retailers are obliged by the Act to protect consumer data from cyberattacks risks and misuse. Furthermore, the e-retailers need to keep the data accurate and can only use the consumer's data for the purpose it was collected for. Sharing of consumer data can only be done where there is a lawful need to, for example passing on credit card details to a bank for payment purposes.

Some salient points to note with regards to e-commerce in this act are that:

- e-commerce consumers leave behind a lot of data footprint when clicking and shopping away online, hacking incidents may mean breach of their privacy.
- Companies are required to notify the consumers when a breach takes place, this gives power to the consumer to take security measures such as blocking credit cards or changing passwords on the breached platform.

2.3.7 *CIPA and e-commerce security*

Critical Infrastructure Protection Act (CIPA) 8 of 2019 requires that critical infrastructure be identified, and measures put in place to protect it and basic public services. Basic services relate to public services such as transport, water, sanitation, health, energy, etc, that are required to maintain the ability to function of the public or ensure economic activity (Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government, n.d.).

The Act creates the Critical Infrastructure Council, which will evaluate any requests for the designation of infrastructure as critical infrastructure and advise the Minister on such requests. The Act also outlines the National Commissioner's duties as well as requirements to declare infrastructure as critical. How does this act apply to e-commerce security? Hardly. E-commerce infrastructure is privately owned; however, the implementation of E-government by the South African government may very well change the landscape.

2.3.8 *RICA and e-commerce security*

Regulation of Interception of Communications and Provision of Communications-Related Information Act (RICA) 70 of 2002 aims to regulate the interception and monitoring of certain forms of communication signals and radio frequency spectrums. Interception infringes on a right to privacy and RICA defines the circumstances where a limited infringement is allowed with prior written consent, or for business purposes, or where the interceptor is party to a communication. Non-compliance to the act carries penalties such as revocation of license to provide electronic communication services, forfeiture of equipment and court conviction (Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 | South African Government, n.d.).

By implication, RICA enforces the constitutional right to privacy of the e-commerce consumer. For e-commerce retailers, this statute allows business

related communication interception within the RICA framework, provided the retailer has gone through some important procedural steps such as obtaining consent from the consumer or in terms of another law requirements.

2.3.9 *PAIA and e-commerce security*

Promotion of Access to Information Act (PAIA) 8 of 2019 promotes effective access to information that is held by public and private organisations. It is regulated by the Information Regulator. Non-compliance to PAIA will result in a litigation (Promotion of Access to Information Act 2 of 2000 | South African Government, n.d.). How is this act applicable to e-commerce security?

Transactional records held by retailer will only be accessible to the requestor through following a request to access information process. Retailer cannot refuse to disclose consumer's transactional records unless the request is unreasonable. Furthermore, the retailers will need to classify their records and meet the retention periods required by the law. This means that the consumer cannot request their records to be destroyed.

2.3.10 *CPA and e-commerce security*

Consumer Protection Act, 68 of 2008 (CPA) sets a framework for consumer rights protection. It stipulates minimum requirements to protect and promote consumer interests in South Africa. The act addresses supplier's accountability to consumer marketing and privacy, right to choose, misleading representations, product and service quality, record keeping, franchise agreements, auction advertising, payments, information that can be disclosed by an intermediary, and institutions that should be established for consumer protection (South African Government, n.d.).

In practice, CPA protects an e-commerce consumer by requiring the supplier to provide comprehensive information on the product or service. The consumer may inspect products upon delivery for quality issues enabling consumers to rescind

a transaction without penalty if they so choose. There are however exclusions in the CPA for e-commerce users. According to Consumer Goods & Services Ombud (CGSO) (2021), exclusions will apply to transactions that are regulated by the ECT Act, transactions with financial institutions and organs of state.

2.3.11 *Cybercrimes Act in the context of e-commerce security*

Before the passage of specific laws making some forms of cybercrime illegal, common law principles were historically applied as far as feasible to aid in the apprehension and conviction of online offenders. It was suggested that common law might still apply to dealing with online conduct. In common law, for instance, inserting a Trojan horse, worm, or virus into a computer system could be seen as malicious harm to property. Overtime, the use of common law proved to be insufficient to address cybercrimes. ECT Act was then promulgated in 2002. Due to technological advancement and modern-day challenges, the Cybercrimes Act was enacted in 2021, taking into consideration the Budapest Convention and Malabo Convention (Snail ka Mtuze and Musoni, 2023).

The Cybercrimes Act, No. 19 of 2020 creates new cybercrime offences, criminalises and prescribes penalty for them. These are related to unauthorised access to or interference with computer systems, storage mediums, data, or computer programs; unauthorised interception of data and processing thereof; fraud, forgery and extortion; theft of incorporeal property; hacking and cracking of passwords and access codes; unauthorised disclosure of intimate images, malicious communications; and conspiring to commit an offence. These acts can result in penalties or jail convictions (Snail ka Mtuze and Musoni, 2023; Cybercrimes Act of South Africa | Easy access online, 2021).

The Act further gives power to investigate, search, access or seize to South African Police Services (SAPS) and for electronic communications service providers and financial institutions to report cybercrimes and provide evidence to the SAPS within 72 hours of being aware of an offence. Furthermore, the Act permits the National Head of the Directorate or the National Commissioner of

Police to support a foreign state's law enforcement agency by supplying any information gathered during an investigation into an offence (Snail ka Mtuze and Musoni, 2023; Cybercrimes Act of South Africa | Easy access online, 2021). A salient point to note is that the Act is post-incident focussed, it does not address required controls for cybersecurity, it was one of the areas removed during the bill revisions in 2018.

The Cybercrimes Act addresses e-commerce by making illegal several cyber-related offences that can happen during online transactions, such as cyber fraud, forgery, extortion, and unauthorized access to data, and in turn, protecting the consumer.

2.3.12 *Legislative frameworks around the world*

There is a great deal of focus on cybersecurity by the world at large as the dependence on digital infrastructure increases. This section focuses on adoption of cybersecurity and related legislations in various parts of the world and what general directive and content they serve. Some of the key concepts that keep emerging are privacy, fraud, forgery, interference of systems and self-regulation.

Cybersecurity legislative frameworks in Africa

Africa, though embracing digital transformation, is considered to have particularly weak internet network and security. Cyber threats faced by African countries include online scams, extortion, ransomware, botnets (including DDoS attacks) and email compromise. Mobile banking is particularly popular in Kenya, Nigeria and South Africa despite the digital divide challenge. Transformation is taking place, however as of 2021, 90% of the businesses operating in Africa are without the necessary cybersecurity practices, leaving them vulnerable to cyberattacks and potential millions of dollars in losses. (Interpol, 2021; Interpol, 2023; Quarshie & Martin-Odoom, 2012). Fowler & Maranga (2022) notes that several African countries have enacted Internet censorship and surveillance laws. These laws are often designed to enable governments to retain control over citizens'

Internet usage within specific regions. While some of these laws aim to protect citizens, many are primarily focused on maintaining governmental control.

In East Africa, a multi-stakeholder approach was adopted and a cyber security management task force which was chaired by Kenya. This task force was made up of five countries, viz. Burundi, Rwanda, Uganda, Tanzania, and Kenya. This task force plan was to establish a Computer Emergency Response Teams (CERTs) through the help of International Telecommunications Union (ITU). Part of the task force mandate was to establish the legal frameworks required in each country (Quarshie & Martin-Odoom, 2012).

West African countries like Ghana and Nigeria have passed bills to protect internet users and criminalise any unlawful acts on Information Technology systems. Ghana passed the Electronic Transactions Act in 2008 whilst Nigeria enacted Cybercrimes Act in 2015 (Quarshie & Martin-Odoom, 2012).

As depicted in Table 1 below, 39 of the 54 African countries have enacted cybercrime legislations, 2 countries have draft legislations whilst 12 countries have no legislations at all. Furthermore, 61% of the African countries have enacted e-transaction laws and data protection and privacy laws, whilst 52% have enacted consumer protection laws (UNCTAD, 2021).

Table 1

Legislation enactment in Africa

	Cybercrime Legislation	E-transaction Laws	Data Protection and Privacy Laws	Consumer Protection Laws
Legislation enacted	39 countries (72%)	33 countries (61%)	33 countries (61%)	28 countries (52%)
Legislation in draft	2 countries (4%)	6 countries (11%)	6 countries (11%)	3 countries (6%)
No legislation	12 countries (22%)	6 countries (11%)	10 countries (19%)	8 countries (15%)

Note. Sourced from UNCTAD (2021)

Cybersecurity legislative frameworks in Europe

Europe, made up of 45 countries, has the highest adoption rates of cybercrime, e-transaction and data protection and privacy laws in the world (UNCTAD, 2021). Table 2 below shows that 91 percent of European countries have cybercrime laws in place, 98% of the countries have e-transaction laws, 98% have data privacy laws whilst 78% have consumer protection laws in place.

Table 2

Legislation enactment in Europe

	Cybercrime Legislation	E-transaction Laws	Data Protection and Privacy Laws	Consumer Protection Laws
Legislation enacted	41 countries (91%)	44 countries (98%)	44 countries (98%)	35 countries (78%)
Legislation in draft	0 countries (0%)	0 countries (0%)	0 countries (0%)	0 countries (0%)
No legislation	3 countries (7%)	0 countries (0%)	0 countries (0%)	0 countries (0%)

Note. Sourced from UNCTAD (2021)

Fowler & Maranga (2022) note the willingness to work internationally and build global stability against cybercrime as one of the strengths of European laws. On the other hand, Calderoni (2010) purports that Europe's biggest challenge when it comes to fighting cybercrimes being the inconsistencies of the criminal justice systems due to the virtual nature of cybercrimes, for example, the perpetrator may be in a country where the act is not considered a crime whilst the victim is in a country where the act is considered a crime. Furthermore, the author affirms that cybercriminals are most likely to concentrate their efforts on the most lenient judicial regimes and the most helpless victims, and that convergence of European legislations (and possibly with other countries as well) is required to remediate this.

Council of Europe's Convention on Cybercrime is an international treaty which includes United States and other countries. The Convention aims to strengthen international collaboration, harmonize national laws, enhance investigative skills, and better combat cybercrime. Title 1 of the Convention defines core offences such as unauthorised access to systems and tampering with programs and data, and misuse of interference devices. Title 2 of the Convention criminalizes offences such as computer forgery and fraud (Council of Europe, n.d).

According to Calderoni (2010) and The Congressional Research Service (2006), there are two school of thoughts on this treaty, supporters contend that the Convention will increase deterrence, while detractors respond that without the involvement of nations where cybercriminals may operate freely, the Convention won't have much of an impact. This is against the backdrop of countries such as Russia, one of the few European countries that have not signed the treaty as it proclaims that this treaty threatens its sovereignty. Russia has a sticky history of allegations of initiating cyberattacks against other countries for political reasons. The implication of this is that Russia is not obliged to cooperate in investigation, extradition of cybercrimes offenders or prosecution of cybercrimes (Uchenna Jerome, 2012).

Cybersecurity legislative frameworks in Asia-Pacific

Asia-Pacific, made up of 60 countries, has cybercrime legislation enacted in 77% of its countries, 83% of them have e-transaction laws, 57% of them has data protection and privacy laws whilst only 45% of the countries have consumer protection laws as presented in table 3 below (UNCTAD, 2021).

Table 3

Legislation enactment in Asia-Pacific

	Cybercrime Legislation	E-transaction Laws	Data Protection and Privacy Laws	Consumer Protection Laws
Legislation enacted	46 countries (77%)	50 countries (83%)	34 countries (57%)	27 countries (45%)
Legislation in draft	7 countries (12%)	3 countries (5%)	7 countries (12%)	4 countries (7%)
No legislation	7 countries (12%)	2 countries (3%)	15 countries (25%)	7 countries (12%)

Note. Sourced from UNCTAD (2021)

Cybercrimes are on a rise in Asia, specifically Southeast Asia. Top cyberthreats include phishing, email compromise, ransomware, crimeware-as-a-service, e-commerce data interception, scams, and crypto-jacking (Interpol, 2021)

Cybersecurity legislative frameworks in the US and North America

Made up of 35 countries, 86% of America has enacted cybercrime laws, whilst 89% have enacted e-transaction laws as per Table 4 below. (UNCTAD, 2021).

Table 4

Legislation enactment in America

	Cybercrime Legislation	E-transaction Laws	Data Protection and Privacy Laws	Consumer Protection Laws
Legislation enacted	30 countries (86%)	31 countries (89%)	26 countries (74%)	25 countries (71%)
Legislation in draft	1 country (3%)	4 countries (11%)	4 countries (11%)	3 countries (9%)
No legislation	4 countries (11%)	0 countries (0%)	5 countries (14%)	2 countries (6%)

Note. Sourced from UNCTAD (2021)

According to McKenzie (2021), the simplest way to describe the American government's attitude to e-commerce regulation is as "soft touch". Consumer protection laws have been enacted by the Federal Trade Commission (FTC) with a focus on online advertising to customers and consumer transactions. Credit card numbers and personal information about consumers are protected by federal and state legislation. In the US, federal legislation applies to all US's 50 states whilst state law applies to the individual state of the US.

Computer system abuse is prohibited by the cybersecurity law - Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. Computer system abuse acts include committing fraud, password trafficking, hacking, spreading malware, damaging a government computer, and conspiring to committing any of these acts. Non-compliance carries hefty jail terms (The United States Department of Justice, n.d).

2.3.13 *E-commerce and the concept of self-regulation*

Boss (1999) argued that security, whether real or perceived, cannot be legislated but that security is a combination of technology used, implementation within a business and overall legal structure; and that security comes in a form of political, social, economic and a legal system.

The concept of self-regulation pops up in various cognitive studies literature. Self-regulation involves several things legislation typically would address, i.e., e-commerce, domain name management, and content controls (Price & Verhulst, 2000). Self-regulation advocates for community handling of issues related to the use of the internet. The government, private sector and users bear the responsibility. Self-regulation is not de-regulation (removal of regulations), but rather instead of the government defining and enforcing the regulation, it is defined by private actors. This is said to address the limited resources and capabilities that exist within the government (Price & Verhulst, 2000; Chang et al., 2018).

The concept of “neighbourhood watch” is coproduced by citizens, it is encouraged by law enforcement as a way of augmenting the police services, it improves interactions between police services and the public, even though sometimes it yields unintended consequences. It is said that the first “hackers” practised “good faith research”, they would identify vulnerabilities and provide feedback towards the improvement of cybersecurity (Chang et al., 2018).

Chang et al. (2018) applies self-regulation principle in cybersecurity. Self-regulation can be applied in cybersecurity and e-commerce by sharing within their community’s intelligence on cyberspace crimes using communication systems such as Whatsapp, Twitter; establishing citizenry run cybersecurity incident response centres which includes industry experts such as Kaspersky, Symantec, etc, Internet Services Provides, and retailers; private investigation and prosecution of cybersecurity criminals. The downside of self-regulation includes skilled hackers pretending to do “good faith research”, erosion of state legitimacy, interference with the application of the law, and lack of accountability (Chang et al., 2018).

2.3.14 *Proposition 1*

Cybersecurity and crimes legislative requirements are spread across at least six legislations. Complexity can create uncertainty about the understanding of rights, obligations and how to apply the law. Table 5 below illustrates the risks highlighted by the literature and the different laws that make provisioning for such a risk.

Table 5

Law provisions for the cybersecurity risks

E-commerce Risk	Reference	Provisions in the South African Law
Privacy	• Luck (2014) • Shanapinda (2019)	• RICA • POPIA

	• Reddy & Singh (2022)	• CPA
Distributed Denial of Service attack	• Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020 • Malapane (2019)	• Cybercrimes Act
Malware and ransomware infections **Crimeware-as-a-service**	• Insight Into the Cyber Threat Landscape in South Africa | Accenture (2020) • Interpol (2023)	• Cybercrimes Act
Data theft and corruption	• Malapane (2019)	• Cybercrimes Act • ECT Act
Fraud and scams	• Malapane (2019) • Insight Into the Cyber Threat Landscape in South Africa | Accenture (2020) • Interpol (2023)	• Cybercrimes Act
Identity theft	• Ezeji et al. (2018) • Interpol (2023)	• POPIA • PAIA • ECT Act
Hacking, system penetration and data exposure	• Ezeji et al. (2018) • Malapane (2019)	• Cybercrimes Act • ECT Act
Phishing	• Ezeji et al. (2018) • Interpol (2023)	• Cybercrimes Act
Cyber Extortion	• Interpol (2023)	• ECT Act

Furthermore, the law is not clear on its application to e-commerce, assumptions will have to be made leading to possible complex implementation. Furthermore, several countries are purporting the harmonisation of cybersecurity legislative frameworks and activities; however, state resources are limited and unable to enforce the law. Self-regulation by social systems closes this gap and can help deter cybercrimes. The following propositions is thus formulated:

- Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce.
- Proposition 1(P1.2): Adoption of a self-regulation increases use of e-commerce.

- Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in intention to shop online.

2.4 To what extent does the South African regulatory framework address e-commerce prosecution of cybercrimes?

This section critically assesses the policing and prosecution of cybercrimes in South Africa.

2.4.1 *Policing of cybercrimes in South Africa*

Dlamini and Mbambo (2019) found that many South African organizations and individuals tend to consider cybercrime policing as an afterthought. In contrast to "traditional crime," which has geographical boundaries and restrictions regarding jurisdiction, this kind of crime has no regional, national, or international borders. Furthermore, there is no globally acceptable definition of cybercrime. This adds to the difficulty of identifying, looking into, and stopping it. The same sentiments are alluded to by Radebe and Kyobe (2021) when relating the difficulty of addressing cyberbullying. They attribute this to the lack of face-to-face contact with victims.

Several challenges face South Africa in their fight against cybercrimes. Firstly, the lengthy process of developing and implementing policies and mechanisms is the biggest problem (Dlamini & Mbambo, 2019). Secondly, shortage of skills (Gillespie, 2024), and that some provisions have not been operationalized yet, possibly because of preparatory work required prior to enforcement (Snail ka Mtuze and Musoni, 2023)

The South African Police Service (SAPS) has established Standard Operating Procedures (SOPs) in terms of Section 26 of the Cybercrimes Act. These SOPs must be observed by SAPS and any other authorized person or agency investigating offences under the Cybercrimes Act. It lists seven guiding principles, such as preserving the validity, dependability, and integrity of cyber articles;

making sure that they are proportionate and necessary; and keeping an audit trail. Data, computer programs, computer systems, and computer data storage media are all included in the definition of a cyber article. When these articles are related to committing a crime, provide evidence, or are meant to be utilized in committing a crime, they are considered relevant. It outlines the procedures for investigating, searching, accessing and seizing these cyber articles. Furthermore, it provides guidelines for determining the jurisdiction of a court to try an offence and the scene of a cybercrime. They also outline the process for applying for a search warrant as well as the creation of a Designated Point of Contact in SAPS (South African Police Service, 2023).

In operation, cybercrimes are investigated by the SAPS unit called the South African Police Computer Crime Unit (SAPS CCU). This unit works with other law enforcement agencies and the private sector to investigate crimes (Gillespie, 2024). SAPS has also collaborated with the Council for Scientific and Industrial Research (CSIR) to establish a Designated Point of Contact. This initiative is aimed at CSIR providing support to enable SAPS to develop cybercrimes investigative capabilities (Mdaka, 2023). Strategic partnerships and cooperation is pivotal to tackling cybercrimes (Dlamini and Mbambo, 2019).

2.4.2 *Prosecution of cybercrimes in South Africa*

According to Snail ka Mtuze and Musoni (2023), law enforcement agencies continue to face jurisdictional challenges when prosecuting cybercrime due to the internet's borderless nature. Unsurprisingly, SAPS seldom secures a successful prosecution of cybercrimes (Gillespie, 2024).

In the court of law, Jones (2006), as cited by Brown (2015), defines evidence as “the means by which the prosecuting authority seeks to establish the guilt of the accused party, and also the means by which the defense teams seek to establish their client’s innocence”. The legal definition of best evidence is that which provides the highest level of assurance regarding the matter under consideration. In the case of cybercrimes, evidence may be in another country. When criminal

acts shift from the physical to the digital realm, like in policing, there is a growing demand for skilled prosecutors knowledgeable about electronic evidence sources. To acquire the knowledge necessary to make strong arguments in court, prosecutors in particular need specialized training. However, a common issue in many criminal justice systems is understaffing and conflicting caseloads. Many prosecutors lack the time required to anticipate and refute new arguments put forth by opposing counsel (Brown, 2015).

Interestingly, Arnell & Faturoti (2023) says that the use of global and multinational jurisdiction as standard or accepted elements of the response to cybercrime is inappropriate, flawed, inefficient and leads to injustice and that subjective territorial jurisdiction is effective. The authors point out several factors, including human rights, complexity, cost and foundations of international law, as the causes of misplacement. The alternative approach (subjective territorial jurisdiction) arguably increases ratification of the Budapest Convention, enables capacity building, enhances private sector collaboration and enables opportunities to sanction cybercrime havens.

2.4.3 *Proposition 2*

Furthermore, Because of the internet's global reach, which enables criminals to operate from any area, South African law enforcement agencies continue to encounter jurisdictional difficulties while pursuing cybercrime. It is therefore propositioned that:

- Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.

2.5 How does the cybercrime legislation build South African consumers' trust in e-commerce?

In this section, the concept of trust is examined and whether legislation is a suitable instrument in building consumer trust on e-commerce.

2.5.1 *Elements of trust*

Trust consists of four interconnected elements as follows: "*I* trust *you* regarding *x* in certain *circumstances*" (De Jager, 2017). For iteration, the elements are: 1) I, 2) you, 3) x, and 4) circumstances. Hult (2018) similarly, conceptualises trust as "A trusts B to do X if A believes that B has the competence to perform X and will do so out of benevolence towards A". It should be noted that "I" and "you", or "A" and "B" can refer to the same object/person.

The element of "I" is personalised. This demonstrates the concept of trust is different from person to person and driven by a natural propensity to trust (De Jager, 2017). The element of "you" is an object being trusted. According to De Jager (2017), this could be an organisation, a person or an e-commerce platform and there are different levels to trusting. This can be illustrated in e-commerce as the level of trust the consumer has in the retailer brand, the retailer employees, the word of mouth and reviews regarding the retailer, etc. The third element, x, represents the trust in something that x offers or their level of competence in providing the service, or their intentions. Nooteboom (2002), as cited by De Jager (2017), reckons causality of trust should be taken into consideration, for example, the consumer trusts a retailer because their relative has had a positive experience with the same retailer. Lastly, the element of circumstances refers to conditions applicable for trust to exist. (De Jager, 2017; Hult, 2018).

De Jager (2017) notes that there is a difference between trust and reliability, that is to say a consumer can rely on the retailer to deliver their products even though the consumer has no trust in them. Moreover, trust exists where there is uncertainty (risk) but it is important because it is linked to positive expectations. Trust is situational, subjective and psychological (Hult, 2018).

2.5.2 *Legislation as a means to create trust*

“Trust is needed to reduce complexity to manageable levels” Hult (2018). The problem with legislation as a trust instrument is that it is a form of control, and any form of control can lead to mistrust.

De Jager (2017) suggests that the EU legislation is an instrument used to regain consumer and investor trust in the financial sector. It is used in the financial sector to enforce certain standards by financial services providers. They are forced to honour the promises they have made to their customers by the legislation and there is oversight to ensure that they do. Hult (2018) holds the same view, referring to the words used to define the regulatory objectives, for example “Creating trust and confidence” and suggests that there are two dimensions to trust, i.e competence and benevolence. Competence refers to the ability of someone/something to perform a task, whilst benevolence refers to the motive of performing the task. Both competence and benevolence are necessary and cannot compensate for each other (Hult, 2018).

According to Hult (2018), legislation is seen as a political tool for bringing about social change, that is to say legislation turn politics into law whilst court-made laws are perceived to grow slowly to become a societal norm even though that was not the primary intention. Testing of the rationality of the legislation will then become the focus point.

2.5.3 *Proposition 3*

Following the elements of trust, i.e. *“I trust you regarding x in certain circumstances”* and that “A trusts B to do X if A believes that B has the competence to perform X and will do so out of benevolence towards A”. Therefore, it can be propositioned that:

- Proposition 3(P3.1): High legislative competence has a positive effect on intention to shop online.

- Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online.
- Proposition 3(P3.3): Habit has a significant impact on online shopping.
- Proposition 3(P3.4): Intention has a significant impact on online shopping.

2.6 ANALYTICAL FRAMEWORK

2.6.1 *Theoretical Framework*

The theory of interpersonal behaviour (TIB) was developed by Harry Triandis in 1977. This theory is similar but also contrasts with the theory of planned behaviour (TPB). Both theories are behaviour theories, and that behaviour is influenced by intentions and intentions are determined by a range of variables. TPB main factors affecting intention are subjective norms, behavioural attitude, and perceived behavioural control. TPB's main problem is being static, that intention is an immediate cause of people's behaviour and excludes emotional and any other factors outside of people's control. This means that consumers' perceived risk toward e-commerce would have no bearing on their purchase intention. TIB contrasts TPB in that people's behaviour is a combination of social and emotional factors, that there are other things that are outside of a person's control, that affect their behaviour. (Kupfer et al., 2019; Taherdoost, 2018; Attiq et al., 2021).

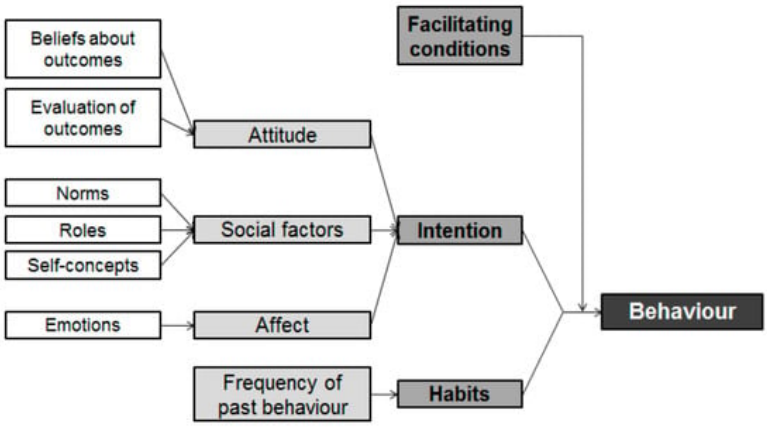
There are several applications of the theory of interpersonal behaviour (TIB). In quantitative research, Robinson (2010) applies it to understand software piracy behaviour in South Africa. The theory is used in a quantitative study to determine objective factors that exist in the environment that affects the person's intention to pirate software. Kupfer (2019) uses the theory in another quantitative study to identify determinants of hand hygiene. It is further used by Mumtaz et al. (2022) in a quantitative study to determine consumer behaviour regarding food waste reduction, recycling, and reuse. Mixed methods studies, it is applied by Attiq et

al. (2021) to investigate the role of a few consumer factors (emotional, cognitive, financial) in food waste reduction, recycling, and reuse behaviour development. Moody & Siponen (2013) uses the theory to explain non-work-related personal use of internet at work.

The theory of interpersonal behaviour (TIB) is rooted in three factors: Habit, behavioural intention and facilitating conditions as per Figure 3 below (Tudela et al., 2013; Salonen et al., 2014; Sung et al., 2019).

Figure 3

Theory of Interpersonal Behaviour adapted by Jackson



Note. Figure by Sung et al. (2019)

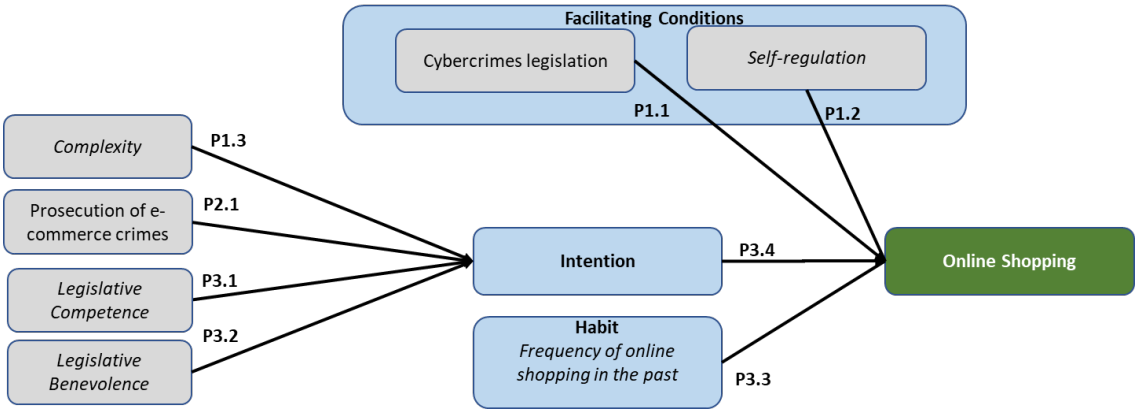
Triadis (1977) as cited by Tudela et al. (2013) and Salonen et al. (2014), proposes that behaviour in every circumstance, is a function of intention as well as the degree to which behaviour is ingrained in one's habits (through repetition) and the many enabling circumstances.

2.6.2 *Conceptual Framework*

Figure 1 depicts the study's conceptual context with the arrows representing the proposition statements and hypotheses on the basis of the previously cited literature.

Figure 4

Conceptual Framework



This study explores legislation and self-regulation as facilitating conditions that makes is easy (enable) for the e-commerce. There were five legislations that were prominent in literature, i.e Cybercrimes Act, POPIA, ECT Act, RICA and CPA. It could therefore be propositioned that:

- *Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce.*
- *Proposition 1(P1.2): Adoption of a self-regulation increases use of e-commerce.*
- *Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in intention to shop online.*
- *Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.*

Theory of Interpersonal Behaviour further perpetuates that intention is driven by attitude, social factor and emotions. Furthermore, habit affect intention and that intention affect the behaviour. The following proposition are made by the study:

- *Proposition 3(P3.1): High legislative competence has a positive effect on intention to shop online.*
- *Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online.*
- *Proposition 3(P3.3): Habit has a significant impact on online shopping.*
- *Proposition 3(P3.4): Intention has a significant impact on online shopping.*

2.7 Conclusion of Literature Review

E-commerce is globally on an increase and South Africa is no exception. Consumer data and footprint is generated with each transaction that take place online increasing consumer's risk of exposure to cybercriminals and their criminal activities. Common e-commerce security threats include malware, fraud, scams, data theft, hacking and denial of services. South Africa does not have an omnibus regulation on e-commerce however, the government has enacted various legislations to curb the activities of the perpetrators including the development of a National Cybersecurity Policy Framework which sets out guidelines for establishment of various policies and capabilities to respond to cyber-attacks at a national level. The enactment of the Cybercrimes Act further enabling the Minister of Justice to make regulations on various aspects of cybercrimes.

Analysis was done on the content of the regulatory framework and the prosecution of cybercrimes. South African legislative framework is complex. Various issues surrounding cybercrimes in e-commerce are spread across at least 6 enacted Acts. It was argued that this complexity will introduce another complexity in implementation and enforcement. The following proposition statements are stated:

2.7.1 *Proposition 1.1*

An implementation of cybercrimes legislation increases use of e-commerce.

2.7.2 *Proposition 1.2*

Adoption of a self-regulation increases use of e-commerce.

2.7.3 *Proposition 1.3*

A decrease in regulatory framework complexity causes an increase in intention to shop online.

2.7.4 *Proposition 2.1*

An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.

Looking externally to South Africa, various legislations, command centres and signed treaties exist in recognition of the importance of cybersecurity. The objective was to discuss a question of alignment of the South African legislation to the international peers. Even though South African legislative framework is on par with the existence of the legislations other countries have, there is potential limitation of state resources which will see the country unable to enforce the law. A proposal on the concept of self-regulation is brought forth as a result. The following proposition statements are stated:

Finally, the concept of legislation as an instrument of trust was explored starting off with looking into the various elements of trust, the political connotation built into the existence of legislation and concluded that for a legislation to bring trust, it needs to be rational through demonstration of legislative competence and benevolence. The following hypothesis statements are made:

2.7.5 *Proposition 3.1*

High legislative competence has a positive effect on intention to shop online.

2.7.6 *Proposition 3.2*

A positive legislative benevolence has a positive effect on intention to shop online.

2.7.7 *Proposition 3.3*

Habit has a significant impact on online shopping.

2.7.8 *Proposition 3.4*

Intention has a significant impact on online shopping.

A refined Theory of Interpersonal Behaviour (TIB) supports this study. The theory uses three determinants of behaviour intention, i.e. habits, intention, and environmental conditions.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Research approach

This study adopted an interpretivism worldview. Interpretivism holds that reality is subjective and the understanding of this reality is based on individual perspective. It focuses on context and is not meant to make predictions (Nickerson, 2023). The goal of this research was to get a thorough understanding of the cybercrime regulatory framework, prosecution of cybercrimes, and how this influences consumer behaviour from the perspective of various experts and professionals.

The drawbacks of interpretivism typically have to do with its subjectivity and high likelihood of researcher bias. Data generalization is unlikely in this kind of research because representativeness and reliability are compromised. Advantage is that the data used in interpretivism studies tends to be reliable and honest, primary data obtained through these studies may have a high level of validity (Dudovskiy, n.d).

3.2 Research design

Qualitative research answers the how's and why's. It is used in a study where human behaviour and functioning is concerned by gathering their experiences, perceptions, and behaviour. It helps researchers to gain access to thoughts and feelings of their participants. Qualitative research has the advantage of being able to describe human behavior patterns and processes that might be challenging to quantify. It is naturally an open-ended research. It looks for themes and patterns (Tenney et al., 2022; Sutton & Austin, 2015).

3.3 Data collection methods

According to Tenney et al. (2022) and Sutton & Austin (2015), various sources of evidence exist for data collection in qualitative research, i.e. interviews, observations, and focus groups. “In-depth interviews represent a subset of interviewing techniques characterized by the collection of highly detailed and rich information, flexible interview protocols, and open-ended questions” (Faulkner & Trotter, 2017). In-depth interviews are suitable for studying invisible processes and personal and delicate issues (Faulkner & Trotter, 2017; Sutton & Austin, 2015).

Interviews were used to collect data for this research. Typed notes or voice recordings were taken during these sessions. Where recordings were used, these were uploaded and transcribed verbatim using TurboScribe.ai website before the commencement of data analysis.

3.4 Population and sample

3.4.1 *Population*

Laws (Acts) in South Africa are guided by the Constitution of South Africa. Parliament is the national law-making body. The applicable executive (the Minister), Deputy Minister, a parliamentary committee or any Member of Parliament (MP) can introduce a draft law (A Bill) to the Parliament. Parliament consists of two houses who are critical to the process of making law, i.e. the National Assembly (NA) and the National Council of Provinces (NCOP). Both these houses debate the draft laws and passes or rejects the contents (“How a law is made”, n.d)

Laws can be made at both national and provincial levels. Draft laws are published in the Government Gazette for public comment followed by discussions at the relevant Parliamentary committee prior to being approved and enacted. The President of the Republic declares enactment by publishing the Act's effective

date in the Government Gazette. Laws can only be enacted when the responsible Department has indicated that they are ready and have the capacity to enforce the law (“How a law is made”, n.d; “The Legislative Process”, n.d.). Legislation is law enacted by a state organ with the authority to do so (Department of Justice and Constitutional Development, n.d.).

Interpreters, implementors and enforcers of South African laws lie in courts, government institutions, academic institutions, different corporate institutions and the society at large.

3.4.2 *Sample and sampling method*

Table 6

Sample Frame

	Sample frame	Description	Strategy used
1	South African legal experts	These are law experts specialising in laws regarding data privacy, e-commerce, electronic communication, etc.	Non-probability purposive sampling (Snowball method)
2	South African cybersecurity in e-commerce specialists	These are specialists in the development and commercialisation of e-commerce platforms and information security	
3	South African legal academics	These are law experts in an academic setting.	

A non-probability purposive sampling technique was used using a snowball sampling method. This technique was selected based on respondents' accessibility and the researcher’s assessment of their expertise or utility. This a method used to identify and reach research respondents through a “referral” system within a network of people. The method began with a convenience sample of the initial respondent, and the rest of the respondents were recruited (Etikan, Alkassim & Abubakar, 2016)

The sample for this research was South African legal experts, academics specialising in cybersecurity-related laws, and e-commerce security specialists. The researcher was acquainted with the initial three respondents, and the

subsequent respondents were recruited through referral by asking for references from the respondents after each interview. Introductory emails, phone calls, WhatsApp messages and self-introduction using contacts obtained from other respondents was used to introduce and gain access to follow-up participants. The aim was to identify and interview at least 10 respondents to gain a general view of their experiences.

3.5 The research instrument

Semi-structured interviews are exploratory and used when a unique perspective is sought. They have an ability to focus interviews yet allowing the researcher ability to explore relevant ideas that may arise during the interview (Adeoye-Olatunde & Olenik, 2021).

For this study, interviews were conducted to better comprehend the content and application of South African law on e-commerce cybercrimes. The interviewer had a list of questions prepared for this type of interview as per Annexure C. The target topics included but were not limited to the legislation process, gaps in the legislation, cybersecurity education, and law enforcement.

To keep the interview at an acceptable length, a maximum of 7 questions were asked, and the focus was given to theoretically important variables.

3.6 Procedure for data collection

An email was sent, and a phone call was made to the targeted respondent to introduce the researcher, highlight where the contact details were obtained from and briefly explain the research request and the objectives of the research. When the potential respondent agreed to the interview, the researcher would then check for available slots to schedule an interview appointment.

7 of the interviews were conducted online using Microsoft Teams or Zoom. Permission was sought to record most of the sessions, where it was possible, for

ease of notetaking and to improve the interaction between the interviewer and the interviewee. These recordings were transcribed verbatim for analysis. Where recording was not possible, typed notes were taken.

1 interview was conducted over the phone. Typed notes were taken as the recording was not possible. These notes were used for analysis.

2 interviews were conducted in person. Typed notes were taken and used for analysis.

3.7 Data analysis strategies and interpretation

The researcher went through the interview recordings and created a transcript. A Microsoft Excel sheet was created with the questions that were asked typed out in one column going down and the names of the responders typed as headers in a row going to the right of the spreadsheet.

From the transcript, the responses were copied and pasted into Microsoft Excel, aligned to each question asked and the name of the responder. Typed notes were also cleaned up, copied to Microsoft Excel and aligned to the questions asked and the name of the responder in preparation for conducting both thematic and narrative analysis.

Thematic analysis entailed identifying patterns in the data (Sutton & Austin, 2015). For this part of the analysis, the researcher created a tab listing the respondents and their answers to each question in the same Microsoft Excel spreadsheet. Their responses were grouped and colour-coded based on the similarity of the responses and assigned a “topic code”. From the topics, a further grouping was done and further reduced the number of topics into a theme.

Narrative analysis entailed interpreting the interviewees' stories and drawing attention to crucial elements discovered (Bamberg, 2020). The key findings were divided into those that stand alone (contrasting) and those that are supported by

other respondents (comparing), this gave the research a clear picture of the outcome (Lindgren, 2015).

3.8 Possible limitations and challenges of the study

The following limitations impacted this study

- Sample size and selection was limited to willing participants from the referrals received
- Limited time of the availability of the participants
- Limited research studies on legislation impact on cybersecurity in general
- Limitations in access to cyberattacks data due to concerns related to brand reputation for e-commerce retailers

3.9 Quality Assurance

3.9.1 *Transferability*

To increase transferability, findings are described in detail in the next chapter (Frambach et al., 2013).

3.9.2 *Credibility*

To enhance credibility for the study, data collected through the interviews were transcribed verbatim to ensure the findings are trustworthy (Frambach et al., 2013).

3.9.3 *Dependability*

Dependability is concerned with the consistency of results and replicability of study (Frambach et al., 2013).

To increase dependability, data was analysed until no further themes were identified (Frambach et al., 2013).

3.9.4 *Objectivity and confirmability*

Confirmability is concerned with the neutrality of evidence. It requires a reduction in personal biases when data is gathered and analysed (Frambach et al., 2013).

To increase confirmability, during analysis of data, evidence invalidating or confirming the findings was sought and referenced (Frambach et al., 2013).

3.10 Ethical considerations

According to Sanjari et al. (2014), ethical considerations in qualitative studies exist to govern the interaction between a researcher and respondent. All phases of the study, from planning to reporting, provide ethical concerns to researchers. These include respondent confidentiality, anonymity, informed consent, and the researchers' possible influence on them as well as the other way around (Sanjari et al., 2014).

To limit ethical challenges, this study used and referenced publicly available data as much as possible and where interviews were carried out, no personal data was collected from the respondents. Voluntary participation was key for the study. An option was given to the respondents to withdraw from the study at any moment, even if they had consented to participate. An informed consent form was used to ensure respondents fully understood the risks and benefits of participating in the study. The form included the description of the study, research methods, risks, contact details of the researcher and the institution, and reiteration that the respondent has a right to withdraw without penalty.

CHAPTER 4. PRESENTATION OF FINDINGS

4.1 Introduction

In this chapter, the results of the study are presented in a way that is aligned with the aim of the study. The study's objective was to investigate the impact of the cybercrime legislation framework on online purchasing behaviour in South Africa. This objective was achieved firstly by determining to what extent the South African regulatory framework addressed the cybersecurity risks and crimes and secondly by determining how the legislation is framed to build the trust of the consumers in the use of e-commerce technology. Two propositions (with sub-propositions) were made and described in detail in Chapter 2.

10 respondents were interviewed using a set of open-ended questions. The responses were recorded, transcribed and analysed. For each proposition, the findings are presented and the conclusion.

4.2 Demographic profile of respondents

A total of 10 respondents were interviewed with areas of practice varying as follows:

Table 7

Respondents demographics

Group	Respondent's area of expertise	Total
A	South African legal experts	2
B	South African cybersecurity in e-commerce specialists	5
C	South African legal academics	3

1 respondent is an international trade lawyer, and 1 respondent leads an industry governing body and actively participates in the development of South African laws

governing IT, including cybersecurity. These two respondents are tagged under Group A as “South African legal experts”. Respondents are referred to as Respondents A1 and A2 in the study.

Group B consists of 5 participants currently working in private and public entities either actively engaged in any of the areas of development, implementation, security or commercialization of e-commerce platforms. These respondents are tagged as “South African cybersecurity in e-commerce specialists”. Respondents are referred to as Respondents B1, B2, B3, B4 and B5 in the study.

Group C consists of 3 participants who are actively in the academic space involved in teaching and/or development of South African law and/or cybersecurity at varying academic levels. These respondents are tagged as “South African legal academics”. Respondents are referred to as Respondents C1, C2, and C3 in the study.

4.3 Results Pertaining to Proposition 1

Proposition 1 sought to explore whether legislation and self-regulation as facilitating conditions enable the e-commerce platforms to thrive or become attractive to South African consumers. Several sub-proposition statements were put forward as follows:

- *Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce.*
- *Proposition 1(P1.2): Adoption of a self-regulation increases use of e-commerce.*
- *Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in intention to shop online.*

Using the interview questionnaire attached as Annexure A, the following questions were asked each participant in order to gain an overall understanding of proposition 1.

- *What is the role of legislation with regard to perceived cybersecurity risks in e-commerce?*
- *To what extent do these legislations achieve the above?*
- *Are there gaps you may have identified, and what are they?*
- *What is your view on self-regulation in e-commerce space?*

The sections below provide detailed responses per question.

Question 1: What is the role of legislation with regard to perceived cybersecurity risks in e-commerce?

One respondent said that legislation is necessary to improve internet commerce security. The respondent emphasized that laws establish guidelines for companies to conduct online transactions securely. These laws serve as a deterrence by establishing unambiguous guidelines and harsh penalties for violations. Online safety depends on specific legislation like the National Cybersecurity Policy Framework (NCPF) and the Cyber Crimes Act. Proper implementation and frequent revisions to address emerging cyber threats are essential to these regulations' efficacy. Furthermore, these rules safeguard customers by guaranteeing companies adhere to stringent data protection procedures.

Similarly, another respondent defined the role of legislation in cyberspace as offering an essential operational framework, defining roles and responsibilities, describing best practices, and directing risk management through evaluations, identification, and mitigation. Furthermore, it ensures responsibility at all levels while assisting law enforcement in crime prevention, evidence gathering, and prosecutions. By addressing issues and possibilities, safeguarding users, and enhancing the digital environment—especially in sectors like e-commerce—it also promotes innovation. For the respondent, laws provide a framework for stakeholders to negotiate and resolve problems in the digital sphere successfully.

The 10 respondents generally agreed, as outlined in the table below, that the legislation is necessary to improve e-commerce security and that the legislation’s

role is to establish guidelines and penalties for violations, which are enforced through specific laws.

Laws that were explicitly mentioned were the National Cybersecurity Policy Framework (NCPF), the Cyber Crimes Act, the Protection of Personal Information Act (POPIA), the Electronic Communications and Transactions (ECT) Act and the Consumer Protection Act. The respondents said these laws must have complete measures encompassing fines, security protocols, and proactive crime prevention techniques to address cybercrime, data protection, and security successfully. These laws should establish standard operating procedures for handling cyber incidents, which should clearly outline the roles and duties of different parties. Emphasizing ethics and transparency is necessary to increase customer confidence in digital services. Along with promoting self-regulation and mitigation initiatives by various e-commerce providers to improve overall cybersecurity resilience, the legislation should also incorporate deterrence mechanisms and remedial measures to stop future cybercrimes.

Table 8

Words and phrases used by the respondents to answer Question 1

Word/Phrase	Group	Respondent's area of expertise
• Framework • Cybercrimes Act, POPIA, ECT Act, RICA • Security • Penalties • Data Protection • Proactive	A	South African legal experts
• Operational Framework • Roles and responsibilities • Crime prevention • Cybercrimes Act, POPIA, ECT Act, RICA • Standard operating procedures • Transparency • Ethics • Consumer trust • Reliability • Deterrence	B	South African cybersecurity in e-commerce specialists
• Deterrence • Corrective • Preventative • Self-regulate • Mitigation	C	South African legal academics

• Cybercrimes Act, POPIA, ECT Act, RICA, Consumer Protection		

Question 2: To what extent do these legislations achieve the above?

Three respondents highlighted that the perceived cybersecurity risks include data theft, card fraud, and website disruptions during peak times. In this case, legislation facilitates the prosecution of wrongdoers and acts as a deterrent to induce compliance out of fear of legal repercussions. Legislation's effectiveness, however, frequently falls short since it can turn into a checklist exercise for businesses looking to comply with regulations in the most economical manner. Legislation that works involves more than simply governance-level regulations; it also demands pragmatic, implementation-focused thinking. Although laws don't always stop crimes, they can make them harder to commit by interfering with the "supply chain" of crime, much as gun restrictions can lessen murders involving firearms.

Another responder further explained that the effectiveness of legislation has little to do with the amount of work put in or the government's proactivity. Passing laws involves compromises and changes, making it slow and often lagging behind rapidly evolving technology. While traditional laws, like those defining murder or contracts, remain stable, technology-related laws constantly need updates as technology advances and people find ways to circumvent them. Furthermore, there is a constant need to catch up with technology. This global issue is not unique to any country or South Africa. The EU, UK, and other regions are also struggling with this. For example, AI brings new challenges related to intellectual property, contracts, and freedom of expression, which are still being debated. Despite efforts by international bodies like The United Nations Commission on International Trade Law (UNCITRAL) to create modern laws, countries often look at existing laws from other nations and adapt them to their needs. However, this can lead to issues when concepts from one legal system do not translate well into another due to legal language and context differences. The responder

emphasized the need for careful adaptation and acknowledged that this is an inherent challenge in the legislative process.

Two respondents believed that current legislation like the Cybercrime Act, POPIA, ECTA, and RICA generally aligns with international standards and provides a solid cyberspace framework covering processes, technology, and training. However, there are always gaps that need improvement, and the main issue lies in the implementation of these laws. While the laws themselves are adequate, the execution often falls short due to delays and the need for additional regulations and procedures. For example, the Cybercrimes Act mandates police to investigate cybercrime, but the effectiveness depends on their regulations and standard operating procedures.

The general view amongst the respondents, based on the table below, is that the South African legislative framework, though good, is struggling to achieve what it should and this is due to 1) Given the speed at which technology is developing and the growing complexity of cyberthreats, these rules are frequently reactive and slow to change; 2) Although user knowledge is important, there are often delays and insufficient enforcement in the application of these laws; and 3) Although a strong framework is in place, more rules and processes are required to handle the changing nature of cybercrimes. To provide complete security against cyberthreats, these regulations must incorporate effective deterrence, corrective, and preventative measures as well as mitigation solutions.

Table 9

Words and phrases used by the respondents to answer Question 2

Word/Phrase	Group	Respondent's area of expertise
• Reactive • Slow • User awareness • Technology advances • AI • Complexity • Implementation	A	South African legal experts

• Solid framework • Adequate • Lacks implementation • Delays • Needs additional regulations and procedures • Investigations by police	B	South African cybersecurity in e-commerce specialists
• Deterrence • Corrective • Preventative • Mitigation • Lacks implementation	C	South African legal academics

Question 3: Are there gaps you may have identified, and what are they?

Nine respondents felt that the South African legislative framework has made significant strides in enhancing cybersecurity in e-commerce, ongoing efforts are needed to keep up with emerging threats and ensure widespread compliance and consumer awareness. The general issues among the 9 respondents could be identified as follows: The first was that South Africa's cybersecurity and data regulation framework faces significant challenges in implementation and enforcement. While the POPI Act is well-implemented and has a strong Information Regulator ensuring accountability, its scope is limited to personal data protection. The ECT Act has been crucial for electronic transactions but contains impractical provisions, such as unenforceable and outdated cryptography regulations. Similarly, RICA aims to link SIM cards to users for traceability but is undermined by the widespread availability of "pre-RICA" SIMs and unenforced provisions requiring ISPs to retain records. Secondly, the legislative impact depends on the consumer's level of awareness and understanding. Thirdly, there is an inherent difficulty in identifying and prosecuting cybercrimes. Finally, two respondents felt that provisions for cross-border e-commerce regarding consumer protection and data protection across jurisdictions could present a challenge.

The final respondent stated that while they are not sure of the specific laws that protect e-commerce platforms, they are aware that the nation has many laws in place; the primary difficulty, however, is figuring out how they all work together.

There is much misunderstanding and confusion regarding the legal structure and its practical application. Because of this, many matters are ultimately left up to the courts for interpretation and decision-making, which may result in uneven legal applicability.

Table 10

Words and phrases used by the respondents to answer Question 3

Word/Phrase	Group	Respondent's area of expertise
• Jurisdictions • Cross-border crimes • Evolution of cyberattacks	A	South African legal experts
• Private sector involvement • Laws interpretation • Complexity • Confusion • Erosion of public confidence	B	South African cybersecurity in e-commerce specialists
• Consumer level of awareness • Difficulty of identification of cybercrimes	C	South African legal academics

Question 4: What is your view on self-regulation in e-commerce space?

All respondents generally said that self-regulation has a positive role and is essential in the South African legislative system. This is supported by the view that government entities lack the capacity and skills to implement and enforce the laws and that the industry is better equipped to handle new problems. The biggest issue that the respondents emphasized was the industry's motivation for self-regulation. The table below outlines some of the words and phrases used by the respondents in each group.

Table 11

Words and phrases used by the respondents to answer Question 4

Word/Phrase	Group	Respondent's area of expertise
• Motivation by private sector and government • Chilling effect • Practical self-regulation measures	A	South African legal experts

• Private sector is already self-regulating • Private sector is better equipped	B	South African cybersecurity in e-commerce specialists
• Private sector motivation • More relevant in commercial matters • Accountability • Clear responsibilities	C	South African legal academics

Group B respondents (Five respondents) said the industry was already self-regulating. It is a general practice to implement best practices such as those in NIST and certify against standards such as ISO27001. This is majorly driven by the need to protect the company against brand reputation risk. One of the respondents in this group pointed to a data breach incident that happened at Ashley Madison, a website targeted at people who are married or in relationships seeking to have external affairs.

Group C respondents (Three respondents) said self-regulation is essential in IT and cybersecurity because the industry is better equipped to handle new problems. However, ensuring that the industry has no choice but to address cybersecurity issues and has effective measures to prevent misuse is crucial. Self-regulation must be well-defined and consistently applied. Furthermore, it is critical to balance self-regulation and legislation in cyberspace. A combination of self-regulation for appropriate areas and robust legislation for essential protection requirements is essential to maintain cybersecurity, uphold accountability, and ensure the socio-economic stability of the country.

Interestingly, one Group C respondent felt that self-regulation is appropriate for commercial matters but not cybercrime, which requires state intervention. It's important to distinguish between public and private responsibilities.

One respondent in Group A referred to a court case, Hawarden v Edward Nathan Sonnenbergs Inc (2023), where Judith Hawarden’s email was hacked, and the hacker altered the conveyancer’s bank account details. Judith transferred R5,5 million to what she believed was the conveyancer’s bank account. The court found Edward Nathan Sonnenbergs Inc liable for failing to warn Judith of this cyber risk. This illustrates how trade customs can create law through self-regulation.

The respondents generally agreed that while self-regulation may be effective, government motivation and oversight are crucial to ensure success. Respondents in Groups A and C felt that while self-regulation works for commercial issues, the state must handle crimes. This distinction helps ensure effective regulation and enforcement. To provide uniform protection and responsibility, some areas—particularly data privacy—require legislation, even if many organizations voluntarily embrace best practices and international standards for activities like vulnerability assessments and website compliance. Regulations in e-commerce that are necessary to guarantee safe financial transactions and safeguard customer data are typical examples. Furthermore, regulatory control is required to integrate digital and physical operations, such as Amazon's shipping logistics; otherwise, the nation exposes itself to illicit transactions and the cross-border shipment of prohibited items. Strict restrictions are necessary to protect data privacy and guarantee adherence to international standards, as evidenced by the possible exploitation of customer information by e-commerce companies, including illegal data sales. Another example is that of content streaming. Platforms such as Showmax must secure the required broadcasting permits to operate in Europe. These regulations require authorizations to conduct business with foreign nations to protect local markets.

When businesses can independently manage risks and apply standards, self-regulation works well. However, it is ineffective when competing interests, such as profit objectives clash with society's rights. Without legislative restrictions, crucial issues like data privacy can cause chaos and inefficiency, making it challenging to combat crimes and ensure compliance.

Conclusion on Proposition 1

Proposition 1 aimed to explore whether legislation and self-regulation can help e-commerce platforms thrive and become attractive to South African consumers. Discussions with respondents highlighted five key points:

Firstly, South Africa has a robust legislative framework to address both e-commerce cybercrimes and general cybercrimes. However, the legislation is complex and primarily addresses First-world problems, requiring collaboration and coordination for effective implementation. These gaps highlight the need for practical, enforceable, and forward-thinking approaches to cybersecurity legislation.

Secondly, implementing various regulations is hampered by a lack of capacity and skills. Some respondents also raised concerns about political will and corruption as additional hindrances.

Thirdly, there is a strong need to reduce the laws' complexity and ambiguity and consolidate clauses for better clarity.

Fourthly, there is a strong need for awareness and training for both the implementors of the laws and the consumers. This was a recurring theme in the responses.

Lastly, while there is a role for self-regulation in the cybersecurity and e-commerce industries, there must be government oversight and complement the existing laws to be effective.

4.4 Results Pertaining to Proposition 2

Proposition 2 investigated the respondents' perception of South Africa's prosecution of cybercrimes and the ultimate implication of these bodies on the intention of the consumer to purchase online as per the sub-proposition statement below.

- *Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.*

The following question was posed to the respondents:

Question 5: How does the ecosystem (i.e. police, justice ministries, etc. – with regards to their intention, skills and capacity) enable e-commerce and affect the security of e-commerce?

All respondents stressed that government agencies must cooperate, communicate and collaborate instead of operating independently. There is a general view that there is a "protection of turf" approach regarding how the government operates. Despite existing expertise in these sectors, the respondents pointed out communication as a persistent problem.

Attention was drawn to the difficulty of combating cybercrime in South Africa, stressing that despite the country's current legal framework, there are notable obstacles ranging from a shortage of qualified staff and resources to a lack of chain of evidence to mishandling of crime scenes. At every stage of the legal process, a team of competent people is needed to build a case, which frequently entails identifying offenders and comprehending intricate technological procedures. There is a significant lack of knowledge regarding the practical implementation of security for online sites and within the legal system to understand and gather the right evidence. Like the UK's Cyber Essentials, a framework and assessment system is needed. Currently, protection for the average person from such crimes is virtually non-existent in South Africa.

One respondent contrasted Denmark's larger, better-equipped cybercrime team with South Africa's small one. Although capacity and experience are significant obstacles, the respondents also emphasized the significance of political will and leadership in prioritising digital challenges. They mentioned that digital challenges do not receive the same level of attention and resources as issues like poverty.

Another respondent highlighted the likelihood of a digital crime occurring and the police mishandling the crime scene by turning computers on and off or tampering with infrastructure. In that case, they are unintentionally breaking the law. The criminal gains from this mismanagement since a knowledgeable attorney can

claim that the police broke digital forensics regulations, jeopardizing the integrity of the evidence chain. Because of the obvious legal requirements, the court may dismiss the case regardless of the judge's opinion of the crime. Furthermore, despite South Africa's complicated legal system and sophisticated legislation, these measures frequently terminate at the courts and do not apply to the conduct of first responders and police. In cases of cybercrime, this disparity is a serious issue. Local police frequently lack the expertise to thoroughly examine digital crime scenes, which can result in errors that defense lawyers might exploit. In this sense, the law may unintentionally work in the criminal's favour.

Five of the respondents felt that the government has a great desire to prevent crime in South Africa and that everyone understands its importance, whilst the other five respondents lacked absolute confidence in the government, specifically the agencies responsible for combating crime. A general view was that corruption, lack of funding, and lack of cybercrime expertise in conjunction with rapid changes and advancement of cybercrimes complicates law enforcement and compliance. A mix of laws and expertise is required to build a world-class force. The respondents questioned the government's readiness to fund anti-cybercrime initiatives without exploitation and corruption. Attention was drawn to problems like government agencies being hacked and denying it and the police force not using computers or any form of technology in their daily work. "If they do not use computers for capturing affidavits, how can they possibly investigate cybercrime?" one respondent asked, "complaints about online scams are common in police stations, but the police often advise victims to be more careful next time".

They highlighted the necessity of new processing systems, knowledge transfer, and talent development, and they suggested that although system-wide adoption is difficult, a taskforce-level strategy would be possible. Furthermore, it will take significant infrastructure, technology, and training investment to address these problems. Effective leadership is essential to close these gaps and implement cybercrime laws appropriately and beyond the South African borders.

Word and phrase distribution were as follows:

Table 12

Words and phrases used by the respondents to answer Question 5

Word/Phrase	Group	Respondent's area of expertise
• Skills and capacity • Political meddling • Silo mentality • Lack of accountability	A	South African legal experts
• Corruption • Lack of funding (infrastructure, technology and training) • Prosecution process • Public vs private sector roles	B	South African cybersecurity in e-commerce specialists
• Collective effort required • Cross-border crimes • Criminal gains • Complexity of digital crimes • Legal system complexity	C	South African legal academics

Conclusion on Proposition 2

Proposition 2 aimed to investigate the respondents' perception of South Africa's prosecution of cybercrimes and the ultimate implication of these bodies on the intention of the consumer to purchase online. The following key points were highlighted

Firstly, that general prosecution of crimes is difficult in South Africa, and cybercrime prosecution is complex. Starting with the initial respondent and ending with legal teams interpreting the legislation, these experts must handle gathering digital evidence and applying conventional legal frameworks in novel and quickly changing technological situations. A lack of skill, communication and collaboration hinders government agencies' effectiveness.

Secondly, investment in infrastructure, technology and skills development is crucial to prosecuting cybercrimes. The South African government does not

prioritize spending in combating cybercrimes. The perception of the government prioritizing the interests of its citizens is crucial.

4.5 Results Pertaining to Proposition 3

Proposition 3 investigated, from the regulatory impact standpoint, the attitude, social variables, emotions, habits, benevolence and the implication of these variables on the intention of the consumer to purchase online as per the below sub-proposition statements.

- *Proposition 3(P3.1): High legislative competence has a positive effect on intention to shop online.*
- *Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online.*
- *Proposition 3(P3.3): Habit has a significant impact on online shopping.*
- *Proposition 3(P3.4): Intention has a significant impact on online shopping.*

The respondents were asked the following four questions:

- *With regards to e-commerce: Do legal norms create novel practices?*
- *How does the government demonstrate its benevolence through legislation in addressing and combating cybercrimes?*
- *Can the regulatory framework disrupt a habitual e-commerce user?*
- *Can an absence of an e-commerce regulatory framework or an ineffective regulatory framework decrease the intention of the consumer to use e-commerce platforms?*

Responses are recorded as per below:

Question 6: With regards to e-commerce: Do legal norms create novel practices?

Eight of the respondents agreed that legal norms create novel practices. One respondent jokingly cited an example, referring to how it is almost a South African "law" to offer traffic officers a "cold drink" (a euphemism for a bribe) when caught in violation of traffic regulations. This humorous observation highlights the public perception of corruption in law enforcement and how informal practices can also become ingrained in the culture.

“Legal norms can drive innovation and encourage adopting best practices by e-commerce retailers, ultimately enhancing consumer functionality and security”. For instance, Takealot, a popular e-commerce platform in South Africa, relies on third-party payment gateways such as PayFast, VISA, and Mastercard to process transactions. This approach allows Takealot to comply with legal requirements, such as the National Payment System Act (NPS), without directly handling payments—a process that would be both costly and time-consuming. By leveraging trusted payment processing platforms that consumers are familiar with, Takealot meets compliance standards and builds consumer trust, fostering a secure and reliable transactional environment. Secondly, legal norms can influence and reshape habitual behaviours. For example, if legislation mandated the implementation of two-factor authentication (2FA) for e-commerce transactions, users would need to log in with their username and password and then enter a code sent to their mobile phone to complete the login process. While this requirement could be relatively straightforward for e-commerce retailers to implement, educating consumers about its use is the challenge. User reactions could vary—some might appreciate the added security, while others might find the extra step inconvenient or frustrating, potentially discouraging them from using the platform. This underscores the need for effective communication and user education to ensure a smooth transition to new security measures. In this case, high legislative competence from the e-commerce provider may not necessarily yield a positive effect on the consumer.

One respondent took it a step further, saying that legal norms create novel practices, and the opposite is true. New practices frequently have an impact on

how legal standards evolve. Because of this dynamic interaction, the legal system is kept current and flexible in response to societal shifts. New practices frequently prompt legal revisions that draw attention to shortcomings or holes in the law. On the other hand, long-standing legal standards can direct and influence how practices change over time, making sure they reflect the goals and values of society as a whole. A fair and forward-thinking legal system depends on the interaction of legal norms and practices.

For legal norms to create novel practices, it was suggested that consumers need to be educated on protecting themselves, which would lead them to adopt behaviours that serve their best interests.

Words and phrases used are recorded in the table below.

Table 13

Words and phrases used by the respondents to answer Question 6

Word/Phrase	Group	Respondent's area of expertise
• Evolution of legal standards	A	South African legal experts
• Novel practices also create legal norms • Current and flexible legislations • Culture of "Cold drink"	B	South African cybersecurity in e-commerce specialists
• Collective effort • Innovation • Adoption of best practices	C	South African legal academics

Question 7: How does the government demonstrate its benevolence through legislation in addressing and combating cybercrimes?

Regarding benevolence, only two respondents emphasized that the South African government is highly engaged in developing and ensuring the regulatory framework meets its objectives. One respondent noted that the government actively funds the process of self-regulation, recognizing the public sector's role and capacity to implement these laws effectively. The other respondent said

South African laws are well-written to protect the citizens' constitutional rights. The problem is, in fact, user awareness.

Respondents described legislative benevolence in South Africa as a complex issue. On one hand, the process of establishing laws is transparent, involving multiple phases within the legislature before being passed. However, some laws are perceived as politically motivated or unconstitutional. For instance, the contentious Electoral Amendment Bill has been criticized for allegedly favouring the ruling party, leaving opposition parties dissatisfied. Such perceptions create an impression that legislation is not always designed with the public's best interests. For e-commerce consumers, this can amplify the perceived risks, undermining trust in the regulatory framework intended to protect them. Trust in the legislation and the government's intention is important for the consumer since cybercrimes are sometimes cross-border, and that law enforcement will pursue such cases if they happen outside of the border in the interest of the citizens of South Africa. One respondent suggested that a dedicated e-commerce regulation would be seen by consumers as a demonstration of commitment to safeguarding their interests, contributing to consumer trust and enforcing secure practices onto the e-commerce retailers.

Table 14

Words and phrases used by the respondents to answer Question 7

Word/Phrase	Group	Respondent's area of expertise
• Highly engaged • Consumer trust • Users' interests • Government perception by consumers	A	South African legal experts
• Suspicious • Dedicated e-commerce legislation • Commitment	B	South African cybersecurity in e-commerce specialists
• Government does what is necessary • Trust • Transparency	C	South African legal academics

Question 8: Can the regulatory framework disrupt a habitual e-commerce user?

Three respondents felt that “Social standards, cultural influences, and repetitive behaviours are the sources of habits, emotions and intention”. That “word-of-mouth” advertising utilizes those networks' trust and social connections. According to these respondents, consumers would still make purchases despite the lack of regulation due to other considerations like value, scarcity, cost, accessibility, and social ties. They highlighted that they had used e-commerce platforms since their inception in South Africa when no legislation governed such activities. Despite considering themselves mature IT users, this did not influence their decision-making—they proceeded to use the platforms regardless of the regulatory landscape. According to these respondents, the presence, absence, complexity, or regulation-related issues have little impact on users' intentions or online habits. They, however, noted that the law would help tremendously by reducing the risk.

Table 15

Words and phrases used by the respondents to answer Question 8

Word/Phrase	Group	Respondent’s area of expertise
• Risk appetite • Perception	A	South African legal experts
• Social standards • Repetitive behaviours • Cultural influences	B	South African cybersecurity in e-commerce specialists
• Vendor Trust • Security controls • Individual behaviour	C	South African legal academics

Seven respondents have observed that online consumers exhibit varying levels of risk appetite and behaviour. Those who take calculated risks often rely on the assumption that vendors have implemented basic security controls, thereby making an informed decision to proceed. In contrast, less informed users may make poor decisions, with outcomes depending mainly on chance. Misinformation and malicious rumors circulating in community chat groups,

erodes trust in law structures and discourage community members from engaging in general activities, particularly those as risky as e-commerce platforms. Trust in certain brands, for example, Takealot, reduces the perception of risk and increases the likelihood of a purchase with the hopes that the company would ensure basic security measures. Their comfort lies in knowing that there is a recourse available if they do not. This will influence their trust and habits in using the Takealot platform.

For these respondents, whether habitual users will be disrupted depends on how e-commerce retailers implement the controls required by the legislation. This underscores the importance of involving diverse stakeholders in the legislative process, including lawmakers, cybersecurity experts, e-commerce retailers, and consumers. This holistic approach ensures that the full lifecycle is considered, making the legislation practical and effective for all parties involved.

Question 9: Can an absence of an e-commerce regulatory framework or an ineffective regulatory framework decrease the intention of the consumer to use e-commerce platforms?

Table 16

Words and phrases used by the respondents to answer Question 9

Word/Phrase	Group	Respondent's area of expertise
• Security and integrity of online transactions	A	South African legal experts
• Encourages • Positive experience • Shoppers don't care about the legislation	B	South African cybersecurity in e-commerce specialists
• Encourages people to shop • Socio-economic impact	C	South African legal academics

All the respondents agreed that regulations are essential for ensuring the security and integrity of online transactions. For example, collecting and transferring money to banks must be strictly regulated to protect consumers and build trust in the system.

A notable case is Showmax, a South African streaming service. Due to regulations set by entities like the ETCA, Showmax cannot be accessed in Europe without the necessary licensing. For instance, to operate in countries like Denmark, Showmax requires specific permissions, highlighting how regulatory frameworks govern connectivity between physical and digital realms, such as cross-border shipping logistics and digital media distribution.

Moreover, the absence of stringent regulations can lead to companies exploiting loopholes, such as selling consumer information. This underscores the critical need for robust legal protections to safeguard consumer rights and ensure fair practices in the e-commerce sector. It's not a matter of the user experience, behaviour, or habits, it's a matter of ensuring that socio-economic impact is contained and happens within certain parameters.

A general view from the respondents was that even just the knowledge that an activity is regulated—encourages people to use the e-commerce platforms. Regulation provides a sense of safety and trust. For instance, COVID forced many people to shop online, but before that, South Africans hesitated to buy online. More South Africans are shopping online due to positive experiences, but caution remains. The level of trust in e-commerce in South Africa is not as high as in other countries. In countries with robust consumer protection laws, regulations ensure that people feel secure—they know they can return items or rely on protections if something goes wrong.

Crime in South Africa has caused individuals to become “generally pessimistic” about many things. Public perceptions of the police and court's inability to adequately investigate and prosecute crimes are the root cause of this distrust. In particular, South Africans' hesitancy in e-commerce stems from their emotions and intentions being thwarted by prior experiences rather than from a lack of competence in using the platforms. These encounters make people wary of and suspicious of internet purchases with or without the law.

Conclusion on Proposition 3

Proposition 3 aimed to investigate, from the regulatory standpoint, the attitude, social variables, emotions, habits, benevolence and the implication of these variables on the conduct of the consumer online. The respondents highlighted three things as follows: First, legal norms give rise to new practices, and new practices in turn have an impact on legal norms. Second, the intention to buy online is greatly influenced by attitude, social norms, habits, emotions and risk appetite. The legislative framework's role is to make e-commerce platforms safer. Third, consumer awareness and training are crucial for lowering the risk of using e-commerce platforms.

4.6 Summary of the results

This study aimed to investigate whether laws and self-regulation could support the growth and appeal of e-commerce platforms to South African customers, furthermore investigate, from the regulatory standpoint, the attitude, social variables, emotions, habits, benevolence, and the implication of these variables on the conduct of the consumer online. 10 respondents were interviewed, and the results were presented in this chapter.

Five main points emerged from conversations with respondents in answering Proposition 1. Two points emerged from the responses to Proposition 2 and three points to Proposition 3 as summarized in Table 17 below.

Generally, the respondents felt that South Africa has a strong regulatory framework in place to deal with both general and e-commerce cybercrimes. However, several inhibitors exist, such as law enforcement, political will, education, and awareness for e-commerce retailers and e-commerce consumers. Furthermore, variables of emotions, habits, benevolence and intention are critical, and the legislative framework ensures a safe environment that encourages consumers to engage in economic activity.

Table 17

Summary of propositions and outcome

Proposition	Summary of outcomes
Proposition 1: Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce. Proposition 1(P1.2): Adoption of a self-regulation increases use of e-commerce. Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in intention to shop online.	1. Robust legislative framework to address both e-commerce cybercrimes and general cybercrimes. However, the legislation is complex, impractical, and difficult to enforce. 2. Implementation efforts lacks capacity and skills. 3. Reduce the laws' complexity and ambiguity and consolidate clauses for better clarity. 4. Strong need for awareness and training for both the implementors of the laws and the consumers. 5. There is a role for self-regulation in the cybersecurity and e-commerce industries, there must be government oversight and complement the existing laws to be effective.
Proposition 2: Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.	1. Prosecution of cybercrimes is difficult and complex in South Africa due to the processes required to collect evidence and prosecute 2. Investment in infrastructure, technology and skills development is crucial to prosecuting cybercrimes
Proposition 3: Proposition 3(P3.1): High legislative competence has a positive effect on intention to shop online. Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online. Proposition 3(P3.3): Habit has a significant impact on online shopping. Proposition 3(P3.4): Intention has a significant impact on online shopping	1. legal norms give rise to new practices, and new practices in turn have an impact on legal norms. 2. Intention to buy online is greatly influenced by attitude, social norms, habits, emotions and risk appetite. 3. Consumer awareness and training are crucial for lowering the risk of using e-commerce platforms.

In Chapter 5, the researcher discusses these findings in depth.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter presents an analysis and discussion of the data gathered during the interviews of 10 respondents. During analysis, data was displayed in tables with the aim of coding and identifying themes. These themes are presented in the sections below, together with core narratives. The data was evaluated to answer the two research questions:

Research question 1: To what extent does the South African regulatory framework address e-commerce security risks

Research question 2: To what extent does the South African regulatory framework address the prosecution of cybercrimes?

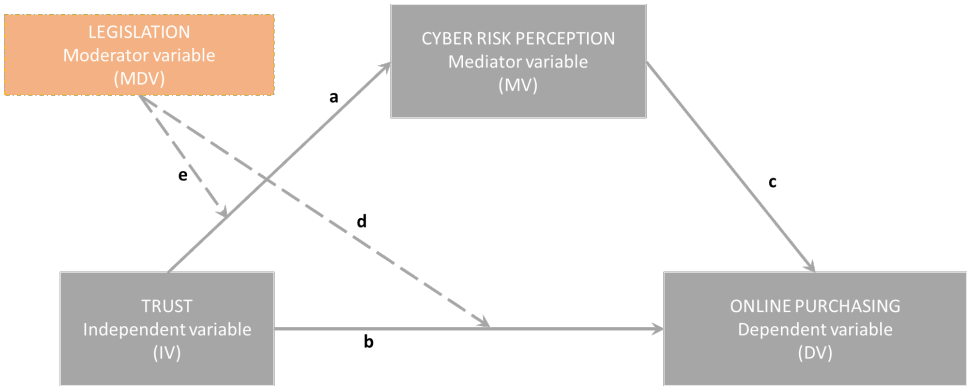
Research question 3: How does the cybercrime legislation build South African consumers' trust in e-commerce?

5.2 Discussion pertaining to Proposition 1

Proposition 1 sought to explore whether legislation and self-regulation (moderator variables) are intervening conditions to enable e-commerce platforms to thrive or become attractive to South African consumers. Moderator variables affect the relationship between the independent and dependent variables (figure 5). It is an intervener. Moderators can amplify or reverse the effect; they explain when and to who such effects occur (Peck & Smitherman, 2015).

Figure 5

Variables relationship



Note. Adapted from Peck & Smitherman (2015)

The role of the legislation

The question of the role of the legislation revealed that the respondents associated the words rules, guidelines, safety, security features, safer, enforcement, preventative measures, and transparency in relation to its role and emphasized how these elements are crucial for establishing a trustworthy and secure e-commerce environment.

For the respondents, legislation guarantees that e-commerce platforms function in an ethical and transparent manner by creating regulations that are both explicit and enforceable. This is demonstrated using words and phrases such as transparency, ethics, reliability and consumer trust when referring to the role of legislation. The legislation also requires e-commerce companies to meet quality and service requirements, which contributes to the development of a dependable and trustworthy online marketplace. To put it simply, strong laws serve as a basis for consumer confidence, which makes online shopping safer and more alluring for consumers. When consumers know that there are laws in place to safeguard their interests, they are more likely to trust and engage with e-commerce

platforms (Akinyede et al., 2020; De Jager, 2000; Malapane, 2019; Ezeji et al.,2018).

It should be noted that Group A (law experts) and C (academics) are mostly familiar with the laws, whilst Group B – Industry experts had a different level of understanding of the laws. Furthermore that the respondents in various groups presented different views on 1) the existence of any e-commerce regulatory framework, 2) the adequacy of the existing regulatory framework and 3) the need to have separate legislation for e-commerce security.

The respondents who were familiar with the laws highlighted ECTA, RICA, POPIA, Cybercrimes Act, and CPA as applicable laws for securing e-commerce platforms and protecting customers. Others felt that this numerous legislative referencing is complex and unworkable for South African context whilst others believed that there needs to be a separate, robust and simple legislation governing the security and use of e-commerce platforms.

POPIA, CPA, and ECTA strongly emphasize e-commerce consumer protection and trust, including topics like fair trade practices, data security, and privacy. In order to provide security for the larger digital environment in which e-commerce functions, RICA and the Cybercrimes Act place a greater emphasis on crime prevention and enforcement. Although POPIA and the Cybercrimes Act safeguard customer data, POPIA is more focused on consumers, while the latter is more focused on offences.

While POPIA and CPA are more regulatory, concentrating on consumer rights and privacy, respectively, ECTA is fundamental, allowing e-commerce by validating electronic transactions. Cybercrimes Act explicitly targets cybersecurity threats related to e-commerce platforms, RICA is more specifically focused on communication interception, with an indirect connection to e-commerce. ECTA deals with the technical validity of electronic transactions, POPIA stresses data privacy, and CPA stresses treating customers fairly (Ntsaluba, 2017; Snail, 2008; Protection of Personal Information Act 4 of 2013 | South African Government,

n.d.; Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 | South African Government, n.d.; CGSO, 2021; Cybercrimes Act of South Africa | Easy access online, 2021).

Self-regulation to bolster the implementation of the legislations

Words such as accountability, clear responsibility and the private sector's motivation define how the respondents felt about the principle. Respondent A1's job is actively in a regulatory body and alluded to effectiveness, government motivation and oversight being crucial to ensure its success. Respondent A2's experience with self-regulation led them to conclude that it is appropriate for commercial matters but not for cybercrime, which requires state intervention. Similar to Respondent A2, Respondent B1 felt it should be a combination of self-regulation for appropriate areas and robust legislation for essential protection requirements is essential to maintain cybersecurity, uphold accountability, and ensure the socio-economic stability of the country. According to Ma (2020), because of the long-held notion that a private organization can never accomplish effective and efficient market discipline because of conflicts of interest, the existence of self-regulation has long perplexed many people. This research also found that although the respondents believed that self-regulation adds value to the overall implementation of the legislation, they are weary of private companies' intentions.

In general, self-regulation is the process by which a sector of the economy creates a private entity with regulatory control over its members. The government's decision to give a regulatory authority determines its effectiveness (Ma, 2020). South Africa has six Chapter 9 institutions and various government and private regulatory bodies in food, education, security, health, finance, telecommunications, and other industries. The South African Constitution explicitly mandates Chapter 9 institutions to create checks and balances to preserve democratic values and safeguard the Constitution. On the other hand, government regulatory bodies (i.e., ICASA, Competition Commission, National Consumer Commission, etc.) are formulated by passing legislation by the

Parliament. The regulatory bodies oversee activities subject to legal or regulatory requirements (The South African Constitution, n.d.).

Private regulatory bodies, such as the South African Banking Risk Information Center (SABRIC), are regulatory bodies created by the specific industry to address sector-specific risks, promote best practices, and ensure compliance with relevant regulations. They play a key role in safeguarding industry standards, developing industry policies, enhancing stakeholder cooperation, promoting innovation and providing a platform for addressing emerging challenges within the sector (SABRIC, 2024).

Oke et al. (2017), defines collusion as “an unethical and disreputable agreement among parties of similar interests, with the intention of achieving a goal through immoral and dishonest means”. Various industries are known to collude - Insurance (Madubela, 2022), fast moving consumer goods (Flanagan et al., 2007), and construction (Oke et al., 2017). These industries have regulatory bodies, i.e. The South African Insurance Association, Consumer Goods Council of South Africa, and for construction, South African Council for the Project and Construction Management Professions (SACPCMP), the Construction Industry Development Board (cidb), and the National Home Builders Registration Council (NHBRC). These regulatory bodies often play a role in investigating scandals, non-conformances and blacklisting dubious people and companies.

Model legislation

One has to ask what a model legislation for securing e-commerce in South Africa would look like. One respondent pointed to the EU e-Commerce Directive, the Malabo Convention on Cyber Security and Personal Data Protection, and the SADC Model Law on Data Protection as exemplary frameworks.

The EU e-Commerce Directive, the Malabo Convention, and the SADC Model Law on Data Protection each provide a framework for regulating e-commerce and data protection, but they differ in their scope, structure, and focus. Each directive

provides a unique approach to regulating e-commerce and data protection, reflecting the specific needs and priorities of their respective regions.

In the EU internal market, EU e-Commerce Directive addresses several topics, such as the creation of service providers, business communications, electronic contracts, and intermediary liability. Transparency, consumer protection, and removing obstacles to cross-border online services are all emphasized in the Directive. To improve the application of its laws, it also discusses the necessity of Member States working together and creating codes of behavior. The Directive also specifies the circumstances in which Member States may deviate from its tenets to safeguard consumer interests, public health, and public policy. It is not applicable to domains like taxation, data security, or gambling (European Commission, 2022).

On the other hand, the Malabo Convention concentrates on data protection and cybersecurity throughout Africa. It seeks to encourage collaboration among African nations and standardize cybersecurity regulations. Cybercrime, personal data protection, and electronic transactions are only a few of the many topics covered by the Convention. It highlights the necessity of a unified strategy to address digital issues and guarantee cyberspace protection (African Union, n.d.). The legal framework is 37 pages long but easy to follow. Enforcement is through criminal provisions and by mandating that nations amend their domestic legislation to comply with the convention's requirements.

The project to harmonize ICT policies in Sub-Saharan Africa includes the SADC Model Law on Data Protection. It offers a data protection regional standard with the goal of bringing uniform regulations to all of the member states of the Southern African Development Community (SADC). The rights of data subjects, the responsibilities of data controllers, and the creation of data protection bodies are just a few of the topics covered by the Model Law. Consistency and conformity to international best practices are guaranteed by its design (ITU, n.d.). The model law is lengthy (54 pages) but comprehensive and easy to follow. Enforcement is through the Data Protection Authorities (DPAs) who are

empowered to impose fines and prosecute offenders in courts. In South Africa, DPA is the Information Regulator.

These references highlight the importance of comprehensive, unambiguous, flexible, technically neutral and well-structured legal guidelines that address various aspects of e-commerce security, from data protection to cross-border transactions as well as fundamental and procedural rules. Laws and policies generally build a reputation for trustworthiness and reliability. By drawing on these established models, a robust legislative framework can be developed for South Africa to ensure the safety, reliability and trustworthiness of e-commerce platforms.

Legal communication and awareness

The respondents highlighted a strong need for awareness and training for both the implementors of the laws and the e-commerce consumers alike. Respondent B2 said that South Africa has seen good improvement in the regulatory framework to address cybercrime, however, “for these laws to work well, consumers need to be aware and educated about the protections in place”. The same sentiments came from Respondent C3.

Understanding the legislation is a crucial component of e-commerce security. It helps organizations by allowing them to reduce risk, guarantee compliance, and identify roles and responsibilities, as they may be held criminally responsible or become a victim of crime if they fail to perform secure e-commerce transactions (Williams, 2000).

Legal expertise is crucial to e-commerce retailers to follow what the law requires in implementing, processing and managing their platforms. This will ensure that they protect their organizations from fraud, avoid penalties and gain the trust of their consumers. For consumers, legal knowledge is crucial to safeguard their rights, make wise purchasing decisions and protect their personal information.

Conclusion pertaining to Proposition 1

The role of the regulatory framework is clear, it is to provide guardrails and guidelines regarding the use of e-commerce platforms and the handlings of cybercrimes. Regarding the regulatory framework and its efficient implementation, there are several misconceptions and misunderstandings. As a result, a lot of issues are ultimately up to the courts for interpretation and decision-making, which could lead to inconsistent legal application and perplexed users and owners of e-commerce platforms. Their sometimes incomplete or delayed implementation is another issue further compounded by limited legal awareness amongst e-commerce retailers and consumers.

Self-regulation in South Africa is welcomed and, in some areas, seems to be working well; however, there are concerns about the priorities of the private sector in its development and implementation.

5.3 Discussion pertaining to Proposition 2

Proposition 2 sought to explore the extent the regulatory framework addressed the prosecution of cybercrimes.

Regulatory enforcement

Corruption, cooldrink, lack of accountability, delays, inefficiencies, lack of expertise, political will, lack of confidence, role of public sector and lack or readiness to deal with cybercrimes is what defines the views of the respondents when it comes to the ability of South African ecosystem (SAPS, Department of Justice, etc), to enforce cybercrimes regulations on e-commerce platforms in South Africa. Respondent A2 pointed out that crime in South Africa has caused individuals to become “generally pessimistic”, moreover the police and courts' ability to adequately investigate and prosecute any form of crime.

In reference to South Africa’s inability to enforce traffic laws, du Plessis et al. (2020) alludes to South Africa’s improper norms and values, the difficulty in

detecting and punishing traffic violations and the administrative and legal processes that function poorly. In alignment with the research respondents, Dlamini and Mbambo (2019) point to E-commerce cybercrimes as challenging to detect and prosecute due to their borderless nature.

According to Lutman & Damjan (2022), the high degree of protection that EU laws provide to consumers, irrespective of their location inside the EU, is a crucial component in bolstering their confidence in cross-border business-to-consumer (B2C) transactions. To avoid circumstances in which no national authority is able to look into and prosecute violations of consumer law, the CPC Regulation establishes a framework for cooperation that enables national authorities from every nation in the EU to work together to address violations of consumer laws when the trader and the consumer are based in different nations.

Contrasting this perspective is Respondent A1, who noted that the law enforcement process that is under ISPA's jurisdiction, has a 96% success rate and has been effective for over 20 years. The respondent further emphasized the importance of the industry's practical self-regulation measures, government motivation, and oversight, which are crucial to ensure its success.

Although South Africa has, on numerous occasions, been able to address illegal immigration, drug smuggling and other forms of crimes through neighbouring countries, the fight against cybercrimes on South African e-commerce platforms continues to be hampered by technological, financial, procedural, and resource limitations, making the incorporation of self-regulation by public entities particularly attractive. The approach proposed by Arnell and Faturoti (2023) could be a great start for South Africa, where efforts and the minimal resources available are channeled to investigate and prosecute cybercrimes within the country.

Investment in infrastructure, technology and skills development

Investing in infrastructure, technology, and skills development is crucial for combating cybercrimes (Anderson, 2020; Dlamini & Mbambo, 2019), as these

elements serve as the foundation for an effective defence against evolving digital threats. The use of sophisticated tools and strategies to exploit weaknesses is a sign of the growing sophistication of cybercriminals. In addition to making sure that their systems are safe from cyberattacks, governments and organizations should boost their technological infrastructure so that the appropriate government agencies can look into cybercrimes and reduce data and financial loss for consumers.

The respondents felt that the South African government lacks investment in advanced technology to detect and prevent cybercrimes. The rapid evolution of digital threats requires continuous development and deployment of cutting-edge cybersecurity tools. Artificial intelligence, machine learning, and data analytics are essential in identifying potential threats, predicting cyberattacks, and automating the response process. These technologies can significantly improve policing tasks by identifying and flagging signs of crime or performing crime prediction (Dlamini & Mbambo, 2019; Hayward & Maas, 2021).

Furthermore, the respondents also said that there is a lack of investment in skills and capacity to fight cybercrimes. In February 2023, South Africa was put on Financial Action Task Force (FATF) grey list. For the 2024/25 financial year, in his 2024 budget speech, the Finance Minister announced the plans to invest R765 billion to fight crime and corruption (Parliament, 2024). This targeted training 10,000 new police recruits, deploying soldiers in Mozambique and the Democratic Republic of Congo, and performing other critical missions. R628 million was allocated to Department of Justice and Constitutional Development to implement the FATF and State Capture Commission recommendations.

The Directorate for Priority Crime Investigation (The Hawks), have since collaborated with South African Banking Risk Information Center (SABRIC) and Banking Association South Africa (BASA) to establish a Digital and Financial Forensic Center which will train 40 senior investigators with financial forensic analysis skills (St. Claire, 2024). Developing human capital through skills training and education is indispensable in the fight against cybercrimes. As cyber threats

continue to grow, there is an increasing need for skilled cybersecurity professionals who can understand, mitigate, and respond to cyber threats effectively (Dlamini & Mbambo, 2019). By funding educational initiatives, certification courses, and continual professional development, governments and companies may give their employees the know-how to fight cybercrime. Public awareness initiatives can also lessen the general susceptibility of the populace by assisting people in identifying possible cyber threats. A strong defence against cybercrime is produced by a mix of knowledgeable citizens and qualified specialists, guaranteeing that these advancements match the human ability to manage technical improvements properly.

Conclusion pertaining to Proposition 2

Because of several factors, including corruption, the intricacy of cybercrimes, and severe deficiencies in infrastructure, technology, and expertise, the South African Police Service (SAPS) and related law enforcement agencies have difficulty implementing cybercrime laws. By erecting obstacles to accountability and trust, law enforcement corruption can compromise the efficacy and integrity of initiatives to prevent cybercrime. Furthermore, it is challenging to identify, investigate, and prosecute cybercrimes without specialist knowledge due to their dynamic and extremely sophisticated nature. The response to cybercrime is made more difficult by a shortage of appropriately qualified specialists since police may not be equipped to handle the sophisticated strategies employed by cybercriminals. Furthermore, SAPS's poor technology infrastructure makes it difficult to efficiently and promptly collect and evaluate digital evidence.

To strengthen the enforcement of cybercrime laws, the government needs to invest in cutting-edge technology and infrastructure, give its personnel thorough training, and deal with internal corruption problems that could obstruct advancement. Furthermore, their ability could be improved through international cooperation and alliances with specialized cybercrime units.

5.4 Discussion pertaining to Proposition 3

Proposition 3 investigates, from the regulatory impact standpoint, the attitude, social variables, emotions, habits, benevolence and the implication of these variables on the intention of the consumer to purchase on an e-commerce platform.

Legal norms create novel practices

According to some respondents, laws such as the ETCA have compelled or encouraged e-commerce companies to be creative in implementing stricter data security and enhancing online experiences for e-commerce customers. In fact, the South African Reserve Bank (SARB) issued a directive in May 2024 requiring a number of explicit cybersecurity controls to be implemented by payment processing institutions, such as Multifactor authentication, regular vulnerability scanning, application of security patches and many more (Reserve Bank, 2024). The application of legal norms greatly fosters innovation by enforcing accountability and openness. Encrypted payment gateways and user-friendly privacy settings are already widely used due to global legal requirements (e.g. Payment Card Industry Data Security Standard – PCI DSS) for data privacy and secure payment systems. These, in turn, allow consumers to confidently interact with platforms and make informed decisions since they know that their personal and financial information is protected. Deduction could be made that the legal norms indeed create novel practices.

Some respondents, however, further argued that legal norms can be developed because of innovative e-commerce practices, as regulators adjust to new trends, technology, and difficulties in the online marketplace. A good example is that of the amendment of Financial Advisory and Intermediary Services Act (FAIS Act) to regulate the use of cryptocurrencies in South Africa. This has been amended in response to cryptocurrency usage growth. Thompson (2012) demonstrates how literature was used as a tool for changing the law through a fictional book written by Charles Dickens, where he criticizes the legal system and self-serving

lawyers created by the British High Court of Chancery, leading to human suffering. It is believed this literature contributed to law reforms triggered around 1852. This standpoint implies that one can argue that e-commerce consumer actions can also drive the development of legal norms - consumer advocacy.

Attitude, social variables, emotions, habits and intention

Respondents pointed out that social standards, cultural influences, and repetitive behaviors are the sources of habits, emotions and intention. And that consumers would still make purchases despite the lack of regulation due to other considerations like value, scarcity, cost, accessibility, and social ties. Respondent B3 further supports this, “Regulations hardly impact a user who is hellbent on shopping online”. Respondent C3 felt that no comprehensive legislation exists, but despite this, they continue to shop even on risky platforms but take precautionary measures when shopping online.

Because consumers are still motivated by convenience, accessibility, and competitive pricing, a lack of e-commerce regulations to drive security measures may not stop them from purchasing online. Regulations, however, serve as a precaution to protect customers against possible dangers including fraud, data breaches, and unethical corporate activities.

Respondent A1 brought to attention “misinformation and how malicious rumours circulate in community chat groups”, further arguing that it has an implication on trust in law structures. According to Chelminski & Coulter (2011), as cited by Jayasimha & Billore (2016), argue that customers vent and spread unfavorable word-of-mouth about their bad experiences in the marketplace out of a sense of selflessness to save others from going through the same experience they did, not in reaction to feelings hurt by a service failure. Furthermore, consumer advocacy for moral and sustainable business practices has influenced laws about environmental issues in e-commerce supply chains (Ramalingam et al., 2024).

It can, therefore, be argued that the lack of a regulatory framework has no significant impact on the intention of e-commerce consumers to shop online.

However, the collective actions of e-commerce consumers who are increasingly vocal about their expectations force regulators to address new challenges, ensuring that the regulatory framework changes to promote fairness, openness, and trust in the e-commerce marketplace.

Perceived governmental benevolence

Two respondents found the South African government to be highly engaged in developing and ensuring the regulatory framework meets its objectives, whilst amongst other, Respondent C3 felt that the lack of harmony, overly complex, and ambiguous laws did not reflect well on a government that wants to build trust in a consumer and encourage economic activity.

Eight respondents were caught in between regarding the sufficiency of the government's benevolence. Some issues raised were the known history of corruption, lack of political will and lack of legal awareness. Renaud et al. (2023) highlight that government competence and benevolence are prerequisites for a responsible government, "trust builds over time, whenever our community or I face any unwanted situation including online matter our government handle it very swiftly and smoothly". Perceptions of government kindness can encourage people to follow rules established by the government or hamper policy support (Belkin & Kong, 2022; Kitt et al., 2021).

There is a serious lack of trust between the South African government and its people, as indicated by the fact that just 20% of respondents believed the government is competent and good. "Citizen trust depends on perceived competence, integrity, and value similarity" (Kitt et al., 2021). Public cooperation with governmental regulations and activities may be hampered by this lack of confidence, which may result from views of incompetence, corruption, or broken promises. In democratic countries where the national government cannot impose compliance by coercion, the government can only suppress public opposition and lessen hazards by persuading citizens to cooperate. To rebuild public confidence

and strengthen its relationship with the people, the government must prioritize transparency, accountability, and the delivery of concrete services.

Unintended consequences of the legislation

While legislation is often enacted with the best intentions, it can sometimes lead to unintended consequences that may undermine its original goals. For instance, over-deterrence can occur when laws designed to prevent cybercrimes inadvertently discourage legitimate online activities due to overly stringent regulations. This can lead to digital exclusion, where individuals or businesses avoid engaging in online transactions for fear of non-compliance, legal repercussions or the high cost of compliance (Earnhart & Rassier, 2016).

Additionally, the complexity and volume of legislative frameworks can create confusion and hinder effective implementation and adoption, as seen with the overlapping provisions in South Africa's cybercrime legislation (When Laws Become Too Complex: A review into the causes of complex legislation, 2013).

These unintended consequences highlight the need for a balanced approach that considers both the protective and restrictive impacts of legislation on consumer digital rights and protection.

Conclusion pertaining to Proposition 3

Laws like the ETCA in South Africa have pushed e-commerce businesses to be innovative in enforcing more stringent data security and privacy policies and improving online experiences for e-commerce clients. In addition, consumers' swift uptake of technology has fueled the creation of regulatory frameworks. It was discovered, therefore, that value, scarcity, cost, accessibility, and social linkages have a more significant influence on e-commerce consumers' intentions to purchase online than the regulatory framework. As a result, the regulatory functions as a risk reduction measure. Furthermore, there is a severe lack of faith in the ability and kindness of the government. This implies that a government must put accountability, transparency, and the provision of tangible services first

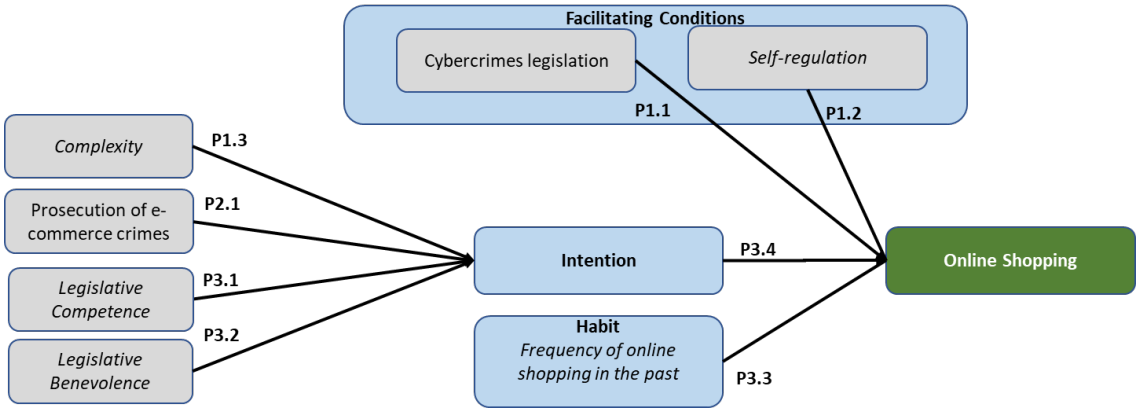
to compel the public to comply, whilst taking into consideration the unintended legislative consequences.

5.5 Theoretical alignment of findings

This research used the Theory of Interpersonal Behaviour that looked at legislative framework and self-regulation as facilitating conditions, i.e. they enable an environment that makes it easier for an e-commerce consumer to be comfortable to use the platforms. Theory of Interpersonal Behaviour further perpetuates that intention is driven by attitude, social factors and emotions and that habit affect intention and that intention affectively drives the behaviour of the e-commerce consumer.

Figure 6

Conceptual framework



Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce. This research supported this proposition and found that the legislation is associated with a positive effect on e-commerce users through the use of words and phrases such as – transparency, ethics, consumer trust, reliability, deterrence, corrective, and preventive.

Proposition 1(P1.2): Adoption of self-regulation increases the use of e-commerce. This research found self-regulation to have a positive effect on the use of e-commerce with a caveat on clear roles and responsibilities being defined and the government taking accountability for crime prevention.

Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in the intention to shop online. This research found that a reduction in the complexity of the legislation, or creating a separate legislation to address e-commerce, has a positive effect on the use of e-commerce by the consumer.

Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online. The research supported this proposition. It however found that in South Africa, investment in skills, technology and infrastructure is required to have a positive effect on the consumer.

Proposition 3(P3.1): High legislative competence has a positive effect on the intention to shop online. This research found high legislative competence to have a positive effect on e-commerce consumers. The respondents highlighted that although South Africa has world-class legislation, user awareness is lacking.

Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online. The research supported this proposition and found that government benevolence is crucial to public trust and confidence.

Proposition 3(P3.3): Habit has a significant impact on online shopping. This research did not support this proposition. It was found that consumers are motivated by convenience, accessibility, and competitive pricing. Lack of e-commerce regulations to drive security measures may not stop them from purchasing online

Proposition 3(P3.4): Intention has a significant impact on online shopping. This research found that e-commerce consumers are increasingly vocal about their expectations, forcing regulators to address new challenges and ensuring that

the regulatory framework changes to promote fairness, openness, and trust in the e-commerce marketplace.

5.6 Conclusion

In Proposition 1 the researcher sought to explore whether legislation and self-regulation (moderator variables) are intervening conditions to enable e-commerce platforms to thrive or become attractive to South African consumers. It was found that the regulatory framework for e-commerce in South Africa aims to provide guidelines and guardrails for platform use and cybercrime handling. The South African regulatory framework is comprehensive and contains the elements required in comparison to exemplary frameworks such as the EU e-Commerce Directive, the Malabo Convention on Cyber Security and Personal Data Protection, and the SADC Model Law on Data Protection. It, however, faces issues like delayed implementation and limited awareness among users. Self-regulation is effective in some areas where the private sector has collaborated with the government but raises concerns about private sector priorities in general.

In Proposition 2 sought to investigate the extent the regulatory framework addressed the prosecution of cybercrimes. The identification, investigation and prosecution of cybercrimes was highlighted as complex needing cybersecurity technical skills. However, the South African government was found to be lacking in investing in skills, infrastructure and technology for the purpose.

Regarding the outcomes of Proposition 3 which investigated, from the regulatory impact standpoint, the attitude, social variables, emotions, habits, benevolence and the implication of these variables on the intention of the consumer to purchase on an e-commerce platform. It was found that Laws such as the ETCA, POPIA, and RICA have driven businesses to enhance data security and improve online experiences, but consumer intention to shop online is influenced more by factors like value and accessibility than regulation. There is also a lack of trust in

the government's ability and integrity, necessitating accountability and transparency to ensure public compliance.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter outlines the conclusions and recommendations of the research study. Each research question is examined, and conclusions are drawn. The chapter ends with recommendations for additional study, emphasizing topics that can improve the regulatory structure even more.

6.2 Conclusions regarding research question 1

Research question 1: To what extent does the South African regulatory framework address e-commerce security risks and prosecution of cybercrimes?

Cybersecurity risks faced by South African e-commerce retailers and consumers were identified as distributed denial of service attacks, malware and ransomware infections, data theft and fraud (Insight Into the Cyber Threat Landscape in South Africa | Accenture, 2020); identity theft, hacking and phishing (Ezeji et al., 2018). Malapane (2019) categorises the risks into data corruption, denial of services, data exposure, system penetration, and financial loss.

These would have been among some risks that the South African regulatory framework would address. It became apparent during the study that the regulatory framework does not address granular cybersecurity risks and crimes. However, its role is to define holistic requirements to secure various data privacy and consumer protection aspects.

The regulatory framework consists of various legislations that address the security requirements and criminality of certain acts on e-commerce platforms – ECTA, RICA, POPIA, Cybercrimes Act, and CPA. The legislations were found to be comprehensive and on par with exemplary frameworks such as the EU e-

Commerce Directive. These are further enabled by self-regulations implemented by the private sector in collaboration with the government, providing an oversight role. Several weaknesses were identified in the areas of enforcement and awareness.

The legislation generally builds a reputation for trustworthiness and reliability. South Africa will need to draw on the established model laws to reduce complexity, demonstrate competence in implementation and enhance e-commerce retailer and consumer awareness to address e-commerce security risks and prosecution of cybercrimes adequately.

6.3 Conclusions regarding research question 2

Research question 2: To what extent does the South African regulatory framework address the prosecution of cybercrimes?

South Africa generally struggles with the investigation and prosecution of crimes; the nature of cybercrimes – evolving and cross-border - adds an additional complexity of this problem. This is compounded by a lack of skills, capacity, technology and infrastructure to investigate and prosecute. The South African government should adopt the subjective territorial jurisdiction approach proposed by Arnell and Faturoti (2023). This will focus efforts on what is within their control and build consumer confidence through prosecution of low-hanging fruit.

6.4 Conclusions regarding research question 3

Research question 3: How does the cybercrime legislation build South African consumers' trust in e-commerce?

Hult (2018) defined trust as having two dimensions i.e competence and benevolence. Competence refers to the ability of someone/something to perform a task, whilst benevolence refers to the motive of performing the task. Both

competence and benevolence are necessary and cannot compensate for each other.

This research found that e-commerce consumers are driven by the value, scarcity, cost, accessibility, and social linkages to shopping online. There is a portion of citizens who are willing to take risks of shopping on unsafe e-commerce platforms and another portion of society that sees the legislation playing a role in defining the security requirements for e-commerce platforms. However, there is no clear understanding of how the current regulatory framework achieves this. Furthermore, there is also a lack of trust in the government to implement laws and indifference to whether the government's intentions are good.

I therefore conclude that the regulatory framework as it stands currently does not build significant trust in e-commerce consumers to encourage usage.

6.5 Recommendations

- Define a separate law for the security of e-commerce based on the model law, including how cross-border cybercrimes will be handled. Model laws already exist to draw from.
- Roles and responsibilities to be defined on who should be ensuring the retailers and consumers understand their responsibilities and rights. This should be done continuously to ensure society's coverage and currency.
- Build capacity and skill to monitor and prosecute cybercrimes, with specific agreements or memorandum of understanding to address cross-border needs.
- Collaboration with the private sector to further enhance the laws and their implementation.

6.6 Suggestions for further research

It is recommended specific research be conducted to address the following areas:

- The complexity of cross-border crimes on e-commerce and the approach proposed by Arnell and Faturoti (2023)
- How to effectively conduct awareness of the regulations to the South African public
- The effectiveness of the use of sanctions for cybercrime havens
- Comparative study with other countries implementing similar cybercrimes frameworks
- Track and observer the longitudinal effects of the cybercrime frameworks in South Africa

Table 18

Consistency table: research questions, propositions, data collection and data analysis

RQ #		Research Question	Prop #	Proposition	Data collection detail	Data analysis method
1		To what extent does the South African regulatory framework address e-commerce security risks and prosecution of cybercrimes?	P1.1	An implementation of cybercrimes legislation increases use of e-commerce.	• Interviews • Open-ended questions 1 & 2	• Narrative analysis
			P1.2	Adoption of a self-regulation increases use of e-commerce.	• Interviews • Open-ended question 3	• Narrative analysis
			P1.3	A decrease in regulatory framework complexity causes an increase in intention to shop online.	• Interviews • Open-ended question 4	• Narrative analysis
2		To what extent does the South African regulatory framework address the prosecution of cybercrimes?	P2.1	An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.	• Interviews • Open-ended question 5	• Narrative analysis
3		How does the cybercrime legislation build South African	P3.1	High legislative competence has a positive effect on intention to shop online.	• Interviews • Open-ended question 6	• Narrative analysis

RQ #		Research Question	Prop #	Proposition	Data collection detail	Data analysis method
		consumers' trust in e-commerce?	P3.2	A positive legislative benevolence has a positive effect on intention to shop online.	• Interview • Open-ended question 7	• Narrative analysis
			P3.3	Habit has a significant impact on online shopping.	• Interview • Open-ended question 8	• Narrative analysis
			P3.4	Intention has a significant impact on online shopping.	• Interview • Open-ended question 9	• Narrative analysis

REFERENCES

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. Journal of the american college of clinical pharmacy, 4(10), 1358-1367.

African Union (n.d.). African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

Akinyede, R. O., Adegbenro, S. O., & Omilodi, B. M. (2020). A security model for preventing e-commerce related crimes. Applied Computer Science, 16(3).

Alsharif, N., Dahal, K., Pervez, Z., & Sureephong, P. (2018, December). *Multi-Dimensional E-commerce Trust Evaluation Method.* In 2018 12th International Conference on Software, Knowledge, Information Management & Applications (SKIMA) (pp. 1-7). IEEE.

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems. Wiley.

Aromataris, E., & Riitano, D. (2014). Constructing a search strategy and searching for evidence. Am J Nurs, 114(5), 49-56.

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime–why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, *37*(1), 29-51.

Attiq, S., Chu, A. M. Y., Azam, R. I., Wong, W., & Mumtaz, S. (2021). Antecedents of consumer food waste reduction behavior: Psychological and financial concerns through the lens of the theory of interpersonal behavior. International Journal of Environmental Research and Public Health, 18(23), 12457. https://doi.org/10.3390/ijerph182312457

Bamberg, M. (2020). Narrative analysis: An integrative approach. Qualitative analysis: Eight approaches for the social sciences, 243-264.

Barkatullah, A. H. (2018). Does self-regulation provide legal protection and security to e-commerce consumers?. Electronic Commerce Research and Applications, 30, 94-101.

Barnard, L. & Wesson, J. (2005). *A trust model for E-commerce in South Africa: Reviewed article.* South African Computer Journal = Suid-Afrikaanse Rekenaartydskrif, 2005(35), 10-19.

Belkin, L. Y., & Kong, D. T. (2022). Beliefs in government benevolence can promote individuals' compliance with government-issued guidelines: The role of positive affect and general construal level. *Journal of Applied Social Psychology*, *52*(2), 85-94.

Boss, A. H. (1999). Searching for Security in the Law of Electronic Commerce. Nova Law Review, 23(2).

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. Qualitative Research Journal. 9. 27-40. 10.3316/QRJ0902027.

Bramall, C., Schoefer, K., & McKechnie, S. (2004). *The determinants and consequences of consumer trust in e-retailing: a conceptual framework*. Irish Marketing Review, 17(1/2), 13.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. The Comparative and International Law Journal of Southern Africa, 44(1), 123-138.

Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. Crime, law and social change, 54(5), 339-357.

Cameron, R., & Miller, P. (2007, December). Mixed methods research: Phoenix of the paradigm wars. In 21st Annual Australian & New Zealand Academy of Management (ANZAM) Conference.

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. Regulation & Governance, 12(1), 101-114. https://doi.org/10.1111/rego.12125.

Chouhan, R., & Singh, M. (2021). The role of artificial intelligence in cybersecurity. *International Journal of Computer Science and Network Security, 21*(3), 45-53.

Coe, K. and Scacco, J.M. (2017). Content Analysis, Quantitative. In The International Encyclopedia of Communication Research Methods (eds J. Matthes, C.S. Davis and R.F. Potter). https://0-doi-org.innopac.wits.ac.za/10.1002/9781118901731.iecrm0045

Congressional Research Service. (2006). Cybercrime: The Council of Europe Convention. (https://www.everycrsreport.com/files/20060928_RS21208_9b5fe0ffca9f75f8fe97878249bc9df6e532364f.pdf

Consumer Goods & Services Ombud. (2021). Participants FAQ. https://www.cgso.org.za/cgso/participants-faq/

Content Analysis. (n.d.). Columbia University Irving Medical Center. Columbia University. https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). *Trust and e-commerce: a study of consumer perceptions*. Electronic commerce research and applications, 2(3), 203-215.

Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government. (n.d.). South African Government | Let's grow South Africa together. https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000

Council of Europe. (n.d.). Council of Europe – Convention on Cybercrime (ETS No. 185). https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Cuncic, A. (2022). Internal validity vs. external validity in research. Verywellmind. https://www.verywellmind.com/internal-and-external-validity-4584479

Curtis, E. A., Comiskey, C., & Dempsey, O. (2016). Importance and use of correlational research. Nurse Researcher (2014+), 23(6), 20. https://doi.org/10.7748/nr.2016.e1382

Cybercrimes Act of South Africa | Easy access online. (2021). Cybercrimes Act. https://cybercrimesact.co.za/

De Jager, C. E. (2017). A question of trust: The pursuit of consumer trust in the financial sector by means of EU legislation. Journal of Consumer Policy, 40(1), 25-49.

De Jager, H. (2000). Importance of legislation. Auditing SA, 2000(24), 3-4.

Department of Justice and Constitutional Development. (n.d.). African Charter on Human and People's rights – Chapter 2. Justice.gov.za. https://www.justice.gov.za/policy/african%20charter/afr-charter02.html.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404.

Dludla, N. (2022). Takealot expands in the townships as Amazon launch nears. TechCentral. https://techcentral.co.za/takealot-expands-in-the-townships-as-amazon-launch-nears/217009/

du Plessis, S., Jansen, A. & Siebrits, K. 2020, "The limits of laws: Traffic law enforcement in South Africa", *South African Journal of Economic and Management Sciences,* vol. 23, no. 1.

Dudovskiy, J. (n.d.). Interpretivism (interpretivist) Research Philosophy. Business Research Methodology. https://research-methodology.net/research-philosophy/interpretivism/.

Earnhart, D., & Rassier, D. G. (2016). "Effective regulatory stringency" and firms' profitability: the effects of effluent limits and government monitoring. *Journal of Regulatory Economics*, *50*(2), 111-145.

Etikan, I., Alkassim, R., & Abubakar, S. (2016). Comparision of snowball sampling and sequential sampling technique. *Biometrics and Biostatistics International Journal*, *3*(1), 55.

European Commission (2022). E-Commerce Directive. https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive.

Ezeji, C. L., Olutola, A. A., & Bello, P. O. (2018). Cyber-related crime in South Africa: extent and perspectives of state's roleplayers. Acta Criminologica: African Journal of Criminology & Victimology, 31(3), 93-110.

Faulkner, S.L. & Trotter, S.P. (2017). In-Depth Interviews. In The International Encyclopedia of Communication Research Methods (eds J. Matthes, C.S. Davis and R.F. Potter). https://0-doi-org.innopac.wits.ac.za/10.1002/9781118901731.iecrm0116.

Flanagan, L., Smillie, S. & Tromp, B. (2007). The great bread scandal. IOL. https://www.iol.co.za/news/south-africa/the-great-bread-scandal-378568

Fowler, B., & Maranga, K. (2022). *Cybersecurity public policy: SWOT analysis conducted on 43 countries*. CRC Press.

Frambach, J. M., van der Vleuten, C., Durning, S. J. (2013). AM Last Page: Quality Criteria in Qualitative and Quantitative Research. Academic Medicine, 88(4), p. 552. DOI: 10.1097/ACM.0b013e31828abf7f

Freedman, M. (2023). The 10 Largest E-Commerce Markets in the World by Country. Business.com. https://www.business.com/articles/10-of-the-largest-ecommerce-markets-in-the-world-b/

Freeme, D., & Gumede, P. (2012, September). Determining the maturity level of eCommerce in South African SMEs. In The European Conference on Information Systems Management (p. 91). Academic Conferences International Limited.

Gaille, L. (2020). 12 Advantages and Disadvantages of Correlational Research Studies. Vittana.org. https://vittana.org/12-advantages-and-disadvantages-of-correlational-research-studies

Ganesan, S., & Hess, R. (1997). Dimensions and levels of trust: Implications for commitment to a relationship. Marketing Letters, 8(4), 439-448. https://doi.org/10.1023/A:1007955514781

Gefen, D., Rao, V. S., & Tractinsky, N. (2003, January). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. In HICSS (p. 192).

Gillespie, G. (2024). Defending against rising credit application fraud. ENSAfrica. https://www.ensafrica.com/news/detail/9096/defending-against-rising-credit-application-f

Glover, S., & Benbasat, I. (2010). A comprehensive model of perceived risk of e-commerce transactions. International journal of electronic commerce, 15(2), 47-78.

Goodchild, J. (2019, December 31). Cybercrime's Most Lucrative Careers. Dark Reading. https://www.darkreading.com/edge-articles/cybercrime-s-most-lucrative-careers

Greig, J. (2020, March 12). Cybercriminals raking in $1.5 trillion every year. TechRepublic. https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-every-year/

Gulfraz, M. B., Sufyan, M., Mustak, M., Salminen, J., & Srivastava, D. K. (2022). Understanding the impact of online customers' shopping experience on online impulsive buying: A study on two leading E-commerce platforms. Journal of Retailing and Consumer Services, 68, 103000. https://doi.org/10.1016/j.jretconser.2022.103000

Gunter, B. (2008). Television Programming and Violence, International. Encyclopedia of Violence, Peace, & Conflict, 2, 2055 – 2068.

Hall, R. (2013). Mixed Methods: In search of a paradigm. Conducting Research in a Changing and Challenging World, chapter 7 (pp.71 - 78).

Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*, *17*(2), 209-233. https://0-doi-org.innopac.wits.ac.za/10.1177/1741659020917434

Herselman, M., & Warren, M. (2004). Cyber Crime Influencing Businesses in South Africa. Issues in Informing Science & Information Technology, 1.

Hillier, W. (2021). A guide to secondary data analysis. CareerFoundry. https://careerfoundry.com/en/blog/data-analytics/secondary-data-analysis/#how-to

How a Law is Made. (n.d). Parliament of the Republic of South Africa. https://www.parliament.gov.za/how-law-made.

Hult, D. (2018). Creating trust by means of legislation – a conceptual analysis and critical discussion, The Theory and Practice of Legislation, 6:1, 1-23, DOI:10.1080/20508840.2018.1434934

Hussain, O. K., Chang, E., Hussain, F. K., & Dillon, T. S. (2008). Quantifying the numeric and linguistic magnitude of perceived risk in E-Commerce Interactions for RDSS. In 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies (pp. 604-610). IEEE.

Ilyin, Y. (2014, December 2). Cybercrime, Inc.: how profitable is the business? Kaspersky Cyber Security Solutions for Home & Business | Kaspersky. https://www.kaspersky.co.za/blog/cybercrime-inc-how-profitable-is-the-business/15034/

Interpol. (2023). AFJOC – African Joint Operation against Cybercrime. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

Interpol. (2021, January 22). INTERPOL report charts top cyberthreats in Southeast Asia. INTERPOL | The International Criminal Police Organization. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

ISO/IEC 27032:2012. (n.d.). ISO. https://www.iso.org/standard/44375.html

ITU (n.d.). Establishment of Harmonized Policies for the ICT Market in the ACP Countries. Data Protection: Southern African Development Community (SADC) Model Law. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

ITWeb. (2022). Over 3.6m records exposed in Dis-Chem cyber attack. https://www.itweb.co.za/content/PmxVE7KEABOqQY85

ITWeb. (2022). Info Regulator reads riot act to TransUnion over hack. https://www.itweb.co.za/content/VgZeyqJo2eZvdjX9

Jayasimha, K. R., & Billore, A. (2016). I complain for your good? Re-examining consumer advocacy. *Journal of Strategic Marketing*, *24*(5), 360-376.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. Educational Researcher, 33(7), 14–26. https://doi.org/10.3102/0013189X033007014

Johnston, M. (2014). Secondary Data Analysis: A method of which the Time Has Come. Qualitative and Quantitative Methods in Libraries (QQML), 3(619 –626).

Jones, B. (2021). Is Popia Bad Business for South Africa? Comparing the GDPR to Popia and Analyzing Popia's Impact on Businesses in South Africa. Penn St. JL & Int'l Aff., 10, 217.

Joshi, S. (2013). Mixed Research Paradigm: A Parsimonious Approach! Journal of Institute of Medine, 35(78-81).

J.P Morgan. (2022). Opportunities in the metaverse. J.P Morgan. https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf

Ju, A., Guo, Y., & Li, T. (2020). MCKC: A modified cyber kill chain model for cognitive APTs analysis within enterprise multimedia network. Multimedia Tools and Applications, 79(39-40), 29923-29949. https://doi.org/10.1007/s11042-020-09444-x

Kähkönen, A. (2011). Conducting a Case Study in Supply Management. Operations and Supply Chain Management: An International Journal, 4(31-41). 10.31387/oscm090054.

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a Research Paradigm and Its Implications for Social Work Research. Social Sciences, 8(9), 255. MDPI AG. Retrieved from http://dx.doi.org/10.3390/socsci8090255.

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. Methodological Innovations, 13(2). https://doi.org/10.1177/2059799120937242

Kenya Law. (n.d.). Laws of Kenya. http://www.kenyalaw.org:8181/exist/kenyalex/index.xql.

Kitt, S., Axsen, J., Long, Z., & Rhodes, E. (2021). The role of trust in citizen acceptance of climate policy: Comparing perceptions of government competence, integrity and value similarity. *Ecological Economics*, *183*, 106958.

Knuth, D., Kehl, D., Hulse, L., & Schmidt, S. (2014). Risk perception, experience, and objective risk: A cross-national study with European emergency survivors. Risk analysis, 34(7), 1286-1298.

Kohlbacher, F. (2006). The Use of Qualitative Content Analysis in Case Study Research. Forum: Qualitative Social Research. 7.

Kotze, J. S., & Roberts, B. (2023). South Africans are fed up with their prospects, and their democracy, according to latest social attitudes survey. The Conversation. https://theconversation.com/south-africans-are-fed-up-with-their-prospects-and-their-democracy-according-to-latest-social-attitudes-survey-204566.

Kupfer, T. R., Wyles, K. J., Watson, F., La Ragione, R. M., Chambers, M. A., & Macdonald, A. S. (2019). Determinants of hand hygiene behaviour based on the Theory of Interpersonal Behaviour. Journal of Infection Prevention, 20(5), 232-237.

Kshetri, N. (2020). Cybersecurity and development: The role of technology and skills. Journal of Cybersecurity Policy, 15(2), 102-115.

Kyobe, M. (2008). The Impact of Entrepreneur Behaviors on the Quality of e-Commerce Security: A Comparison of Urban and Rural Findings. Journal of Global Information Technology Management, 11(2), 58-79. https://www.proquest.com/scholarly-journals/impact-entrepreneur-behaviors-on-quality-e/docview/275066494/se-2?accountid=15083

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. Qualitative Market Research: An International Journal.

Lim, S. C., Pan, X. Y., Lim, S. P., Lee, C. K., San Tan, J., & Lim, J. T. (2021, July). Factors Influencing Continuance Intention of Ecommerce among SMEs in Northern Region of Malaysia. In 2021 International Conference on Computer & Information Sciences (ICCOINS) (pp. 53-58). IEEE.

Lincoln, Y. S. & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation New Directions for Program Evaluation (pp. 73-84): Wiley Subscription Services, Inc.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology, 13, 4863.

Luck, R. (2014). RICA-walking a fine line between crime prevention and protection of rights: itc law. *De Rebus*, *2014*(538), 30-31.

Lutman, K., & Damjan, M. (2022). Administrative Enforcement of EU Consumer Law: A Disoriented Tiger in the Regulatory Jungle of E-Commerce. *Journal of European Consumer and Market Law, 11*(4), 130-138. https://www.proquest.com/scholarly-journals/administrative-enforcement-eu-consumer-law/docview/3125427421/se-2

Ma, C. (2020). Self-regulation versus government regulation: an externality view. *Journal of Regulatory Economics*, *58*(2), 166-183.

Madubela, A. (2022). The Competition Commission has eight insurance companies in its sights for collusion. Mail & Guardian. https://mg.co.za/business/2022-08-25-the-competition-commission-has-eight-insurance-companies-in-its-sights-for-collusion/

Makhitha, K & Ngobeni, K. (2021). The impact of risk factors on South African consumers' attitude towards online shopping. Acta Commercii. 21. 10.4102/ac.v21i1.922.

Makhitha, K. (2014). Factors Influencing Generations Y students' Attitude towards Online Shopping. Mediterranean Journal of Social Sciences, 5(21), 39. Retrieved from https://www.richtmann.org/journal/index.php/mjss/article/view/4175

Malapane, T. A. (2019, April). A risk analysis of e-commerce: A case of South African online shopping space. In 2019 Systems and Information Engineering Design Symposium (SIEDS) (pp. 1-6). IEEE.

Malatji, M., Marnewick, A. L., & von Solms, S. (2020). Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa. Sustainability, 13(1), 291.

McCombes, S. (2019). Survey Research | Definition, Examples & Methods. Scribbr. https://www.scribbr.com/methodology/data-collection/.

McKenzie, B. (2021, August). In brief: e-Commerce in USA. Lexology. https://www.lexology.com/library/detail.aspx?g=385c70d8-0dc5-40aa-8eb0-d3f52b55bbd4.

McKim, C. A. (2017). The value of mixed methods research: A mixed methods study. Journal of mixed methods research, 11(2), 202-222.

Mdaka, Y. (2023). CSIR collaborates with SAPS to strengthen cybercrime investigations. News24. https://www.news24.com/news24/xarchive/tech-and-trends/csir-collaborates-with-saps-to-strengthen-cybercrime-investigations-20230404

Mofokeng, T. E. (2021). An empirical study stepping towards ethnographic research for e-commerce websites: A perspective of user-centred design. African Journal of Science, Technology, Innovation and Development, 1-19. https://doi.org/10.1080/20421338.2021.1958987

Molinuevo, M., & Sez, S. (2014). Regulatory assessment toolkit: A practical methodology for assessing regulation on trade and investment in services. World Bank Publications.

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the internet at work. Information & Management, 50(6), 322-335. https://doi.org/10.1016/j.im.2013.04.005

Mumtaz, S., Chu, A. M. Y., Attiq, S., Hassan, J. S., & Wing-Keung Wong. (2022). Habit—Does it matter? bringing habit and emotion into the development of Consumer's food waste reduction behavior with the lens of the theory of interpersonal behavior. International Journal of Environmental Research and Public Health, 19(10), 6312. https://doi.org/10.3390/ijerph19106312

Nenadal, J. (2016). Adequacy, suitability, effectiveness and efficiency of quality management systems: how to perceive and assess them?. Quality Innovation Prosperity, 20(2), 39-52.

Netshirando, V., Kadyamatimba, A., & Munyoka, W. (2024). Effects of cyber-security and trust issues on consumers' intention to use E-commerce systems in rural South Africa. International Journal of Research in Business and Social Science, 13(7), 538-549. https://www.proquest.com/scholarly-journals/effects-cyber-security-trust-issues-on-consumers/docview/3159499288/se-2

Nickerson, C. (2023) Interpretivism Paradigm & Research Philosophy. SimplySociology. https://simplysociology.com/interpretivism-paradigm.html.

NG Cert. (n.d.). Nigeria Computer Emergency Response Team. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

Ntsaluba, N. (2017). Cybersecurity Policy and Legislation in South Africa (Doctoral dissertation, University of Pretoria).

Oluwole, V. South Africa, Egypt, Nigeria, Kenya, and Morocco hold over 50% of Africa's private wealth. Business insider Africa. https://africa.businessinsider.com/local/markets/south-africa-egypt-nigeria-kenya-and-morocco-have-over-90-of-africas-billionaires/c1zy9x5

Onwuegbuzie, A. J., Combs, J. P. (2011). Data Analysis in Mixed Research: A Primer. International Journal of Education, 3.

Östlund, U., Kidd, L., Wengström, Y., & Rowa-Dewar, N. (2011). Combining qualitative and quantitative research within mixed method research designs: a methodological review. International journal of nursing studies, 48(3), 369-383.

Oke, A., Aigbavboa, C., Mangena, Z., & Thwala, W. (2017). Causes of collusion among people in construction. *Journal of Construction Project Management and Innovation*, *7*(2), 2077-2087.

Owen, G. T. (2014). Qualitative Methods in Higher Education Policy Analysis: Using Interviews and Document Analysis. The Qualitative Report, 19(26), 1-19. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss26/2

Parliament. (2024). Godongwana allocates R765 Billion to fight crime and corruption. https://www.parliament.gov.za/news/godongwana-allocates-r765-billion-fight-crime-and-corruption

Peck, K. R., & Smitherman, T. A. (2015). Mediator variables in headache research: Methodological critique and exemplar using self-efficacy as a mediator of the relationship between headache severity and disability. Headache: The Journal of Head and Face Pain, 55(8), 1102-1111.

Polk, T. (2021, February 1). Council Post: Cybercrime: Nothing Personal; It's Just Business. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/02/01/cybercrime-nothing-personal-its-just-business/?sh=5dca281339bc

Price, M., & Verhulst, S. (2000). The concept of self-regulation and the internet. Accessed online at https://repository.upenn.edu/cgi/viewcontent.cgi?article=1143&context=asc_papers.

President Cyril Ramaphosa: 2022 State of the Nation Address | South African Government. (2022, February 10). South African Government | Let's grow South Africa together. https://www.gov.za/speeches/president-cyril-ramaphosa-2022-state-nation-address-10-feb-2022-0000

President Cyril Ramaphosa: 2023 State of the Nation Address | South African Government. (2023, February 22). South African Government. https://www.stateofthenation.gov.za/assets/downloads/State-of-the-Nation-Address-2023.pdf

Preston, V. (2009). Questionnaire Survey. International Encyclopedia of Human Geography, 46-52

Promotion of Access to Information Act 2 of 2000 | South African Government. (n.d.). South African Government | Let's grow South Africa together. https://www.gov.za/documents/promotion-access-information-act

Protection of Personal Information Act 4 of 2013 | South African Government. (n.d.). South African Government | Let's grow South Africa together. https://www.gov.za/documents/protection-personal-information-act

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. Computer Science and Engineering, 2(6), 98-100.

Radebe, F., & Kyobe, M. (2021). The response of social crime prevention police to cyberbullying perpetrated by youth in rural areas of South Africa. *International journal of environmental research and public health*, *18*(24), 13421.

Ramalingam, S., Kumar, L. M., Awoke, M. Y., Ramki, R., Ilyas, M. M., & Rajalakshmi, M. (2024). Sustainable Practices in e-commerce challenges and opportunities. Cahiers Magellanes-NS, *6*(1), 1185-1199.

Reddy, K., & Singh, S. (2022). Regulation of Nanotechnology and Nano-Enabled Products: The Implications of the Consumer Protection Act 68 of 2008 in South Africa. *African Journal of Inter/Multidisciplinary Studies*, *4*(1), 325-337.

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 | South African Government. (n.d.). South African Government | Let's grow South Africa together. https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

Renaud, K., Van Der Schyff, K., & MacDonald, S. (2023). Would US citizens accept cybersecurity deresponsibilization? Perhaps not. *Computers & Security*, *131*, 103301.

Reserve Bank. (2024). Directive in respect of cybersecurity and cyber-resilience within the national payment system. Government Gazette, 50665. https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Directive%20in%20respect%20of%20cybersecurity%20and%20cyber-resilisnce%20within%20the%20national%20payment%20system.pdf.

Robinson, J. (2010). Triandis' theory of interpersonal behaviour in understanding software piracy behaviour in the South African context (Doctoral dissertation, University of the Witwatersrand).

SABRIC. (2024). SABRIC Information Manual. https://www.sabric.co.za/media/twph1gb2/sabric-information-manual.pdf

Saleh, M. (2022). E-commerce in Africa – statistics & facts. Statista. https://www.statista.com/topics/7288/e-commerce-in-africa/#topicOverview

Salonen, A., Fredriksson, L., Järvinen, S., Korteniemi, P., & Danielsson, J. (2014). Sustainable consumption in Finland—The phenomenon, consumer profiles, and future scenarios. International Journal of Marketing Studies, 6(4), 59-82.

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research. A menu of Qualitative and Quantitative Options. Sage Publications. https://0-doi-org.innopac.wits.ac.za/10.1177/1065912907313077.

Seeram, E.(2019). An Overview of Correlational Research. Radiologic Technology, 91(2).

Shanapinda, S. (2019). Asymmetry in South Africa's Regulation of Customer Data Protection: Unequal Treatment between Mobile Network Operators (MNOs) and Over-the-Top (OTT) Service Providers. *The African Journal of Information and Communication*, *23*, 1-20.

Siyanbola, A. B., Oyinloye, M. A., Olayinka, A. A., & Sobowale, T. O. (2022). Impactful Consumerism in E-commerce Store Design and Development: A Case Study of Prototypical Craftsential. com. IIS Univ.J.A., 10(3), 373-87.

Snail, S. (2008). Cyber crime in the context of the ECT Act. Juta's Business Law, 16(2), 63-69.

Snail, S. L. (2007). South African e-consumer law in the context of the ECT Act (part 1). Juta's Business Law, 15(1), 40-46.

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299-323.

South African Government. (n.d.). Electronic Communications Act 36 of 2005. https://www.gov.za/documents/electronic-communications-act

South African Police Service. (2023). Standard Operating Procedures in terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles. Saps.gov.za. https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf

St.Claire. (2024).Cybercrime trends. Over 100 reported incidents per month in SA. Topco Media. https://news.topco.co.za/topco-news/internet-banking-cybercriminal-playground.

Story, D. A., Tait, A. R. (2019). Reader's Toolbox. Understanding Research Methods. Anesthesiology, 130, 192–202

Sung, K., Cooper, T., Kettley, S. (2019). Factors Influencing Upcycling for UK Makers. Sustainability. DOI: https://doi.org/10.3390/su11030870

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. The African Journal of Information and Communication (AJIC), 20, 83-112. https://doi.org/10.23962/10539/23574

Sutton, J., & Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. *The Canadian journal of hospital pharmacy*, *68*(3), 226–231. https://doi.org/10.4212/cjhp.v68i3.1456.

Swanepoel, A. P., & Jacolize, M. (2018). Adequacy of law enforcement and prosecution of economic crimes in South Africa. *Journal of Financial Crime, 25*(2), 450-466. https://doi.org/10.1108/JFC-12-2016-0081

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. Procedia manufacturing, 22, 960-967.

Taherdoost, H. (2017). Measurement and Scaling Techniques in Research Methodology; Survey / Questionnaire Development. International Journal of Academic Research in Management, 6(1).

Tenney, S., Brannan, J. M., Brannan, G. D. (2022). Qualitative Study. StatPearls. https://www.ncbi.nlm.nih.gov/books/NBK470395/.

The eCommerce market in South Africa. (n.d.). E-Commerce Market Analysis. https://ecommercedb.com/en/markets/za/all#:~:text=South%20Africa%20is%20the%2041st,for%20eCommerce%20continue%20to%20increase.

The Legislative Process. (n.d.). Parliamentary Monitoring Group. https://pmg.org.za/page/legislative-process.

The Presidency. (2014). Delivery agreement for outcome 3: All people in South Africa are and feel safe | South African Government. South African Government | Let's grow South Africa together. https://www.gov.za/documents/delivery-agreement-outcome-3-all-people-south-africa-are-and-feel-safe

The South African Constitution. (n.d.). The DoJ&CD. https://www.justice.gov.za/constitution/SAConstitution-web-eng-09.pdf

The United States Department of Justice. (n.d.). 9-48.000 – Computer Fraud and Abuse Act. https://www.justice.gov/jm/jm-9-48000-computer-fraud

Thompson, N. (2012). Follow the reader: literature's influence on the law and legal actors. *Honneursverhandeling, University of Otago*.

Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A., Zhanseitov, A., & Jumabaeva, S. (2020). Features of e-commerce risk management in modern conditions. Academy of Strategic Management Journal, 19(1), 1-6.

Tudela, A., Habib, K. M. N., & Idris, A. O. (2013). Semantic approach to capture psychological factors affecting mode choice: Comparative results from Canada and Chile. In Transport survey methods: Best practice for decision making. Emerald Group Publishing Limited.

Uchenna Jerome, O. (2012). Russia and the council of Europe convention on cybercrime. Computer and Telecommunications Law Review, 18(1), 16.

UNCTAD. (2021, December 14). Online Consumer Protection Legislation Worldwide | UNCTAD. Home | UNCTAD. https://unctad.org/page/online-consumer-protection-legislation-worldwide

Walsh, G., Evanschitzky, H., & Wunderlich, M. (2008). Identification and analysis of moderator variables: Investigating the customer satisfaction-loyalty link. European Journal of Marketing, 42(9), 977-1004. https://doi.org/10.1108/03090560810891109.

Warren, M., & Hutchinson, W. (2003). A security risk management approach for e-commerce. Information Management & Computer Security, 11(5), 238-242. https://doi.org/10.1108/09685220310509028

When Laws Become Too Complex: A review into the causes of complex legislation. (2013, March). Office of the Parliamentary Counsel. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/187015/GoodLaw_report_8April_AP.pdf

WHO (n.d.). Institutional Repository for Information Sharing. https://apps.who.int/iris/discover?query=self+assessment

Wilczek, B., Thäsler-Kordonouri, S., & Eder, M. (2024). Government regulation or industry self-regulation of AI? investigating the relationships between uncertainty avoidance, people's AI risk perceptions, and their regulatory preferences in europe. AI & Society, https://doi.org/10.1007/s00146-024-02138-0

Williams, D. (2001). The relevance of legal awareness in e-commerce security. *Journal of Database Marketing, 8*(3), 217-223. https://doi.org/10.1057/palgrave.jdm.3240037

Wilson, R. S., Zwickle, A., & Walpole, H. (2019). Developing a broadly applicable measure of risk perception. Risk Analysis, 39(4), 777-791. https://doi.org/10.1111/risa.13207

ZA CX Report. (2022). The 2022 South African Digital Customer Experience Report. Rogerwilco. https://www.cx-report.co.za/

APPENDIX A: Participant Information Sheet

Dear participant

You are invited to take part in an interview to discuss your experience and views on how South African cybercrimes regulatory framework enables e-commerce.

Who I am?

I am Maletsema Phofu, a student for Masters in Management: Digital Business at Wits Business School.

What research is being conducted?

The widespread use of the internet has altered how nations do business internationally and in South Africa. E-commerce in South Africa is growing at a fast pace. As e-commerce adoption continues to rise, security risks and related cybercrimes in South Africa are also expected to rise and negatively impact consumers' trust.

With an emergent cybersecurity and cybercrime legislative framework in South Africa, there is however a limited understanding of whether this emerging legislative framework can mitigate the cybersecurity risks in the e-commerce domain.

The aim is to seek out their insights on legislative volume, quality, consistency, and experience toward the reduction of their perceived e-commerce risks and prosecution of crimes.

What happens to my information?

The interview responses will be transcribed, anonymised and stored on access controlled cloud storage where only myself as the researcher, my supervisor, and the university can access it.

What happens next?

A phone call will follow to ask for your participation in this study, answer any further questions you may have and agree on a suitable timeslot to conduct the interview.

Do you have any concerns or complaints about the ethical procedures of this research study?

Please contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

I am contactable:

+27 83 212 5440 ; eMail: tsema.phofu@gmail.com

APPENDIX B: Participant Agreement Form

Research Title: **Investigating the impact of the cybercrime legislation on online purchasing behaviour in South Africa**

		YES	NO
1	I understand the objectives of this study, a copy of which I have received		
2	I have been given an opportunity to ask questions or seek clarity regarding this interview		
3	Data collected in this study will be stored in an access controlled online storage		
4	I agree to the interview being recorded for note taking purposes		
5	**I understand that I can withdraw from participating in this study at any time during the process without any obligation to give any reasons for withdrawing**		

Name of participant _____

Sign: _____ Date: _____

APPENDIX C: Interview Questionnaire

Name of the interviewee: _____ Profession: _____

Area of expertise: _____ Years of Experience: _____

Research Question	Description	Question #	Question
1: To what extent does the South African regulatory framework address e-commerce security risks and prosecution of cybercrimes?	Proposition 1(P1.1): An implementation of cybercrimes legislation increases use of e-commerce. Proposition 1(P1.2): Adoption of a self-regulation increases use of e-commerce. Proposition 1(P1.3): A decrease in regulatory framework complexity causes an increase in intention to shop online.	1	What is the role of legislation with regard to perceived cybersecurity risks in e-commerce?
		2	To what extent do these legislations achieve the above?
		3	Are there gaps you may have identified, and what are they?
		4	What is your view on self-regulation in e-commerce space?
2: To what extent does the South African regulatory framework address the prosecution of cybercrimes?	Proposition 2(P2.1): An increase in prosecution of e-commerce crimes causes an increase in intention to shop online.	5	How does the ecosystem (i.e. police, justice ministries, etc. – with regards to their intention, skills and capacity) enable e-commerce and affect the security of e-commerce?

3: How does the cybercrime legislation build South African consumers' trust in e-commerce?	Proposition 3(P3.1): High legislative competence has a positive effect on intention to shop online. Proposition 3(P3.2): A positive legislative benevolence has a positive effect on intention to shop online. Proposition 3(P3.3): Habit has a significant impact on online shopping. Proposition 3(P3.4): Intention has a significant impact on online shopping.	6	With regards to e-commerce: Do legal norms create novel practices?
		7	How does the government demonstrate its benevolence through legislation in addressing and combating cybercrimes?
		8	Can the regulatory framework disrupt a habitual e-commerce user?
		9	Can an absence of an e-commerce regulatory framework or an ineffective regulatory framework decrease the intention of the consumer to use e-commerce platforms?