Lighthouse

The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy

ISSN 2957-8842 (Print)

Vol. 3 (Issues 1&2), 2024

©ZEGU Press 2024

Published by the Zimbabwe Ezekiel Guti University Press
Stand No. 1901 Barrassie Road,
Off Shamva Road
P.O. Box 350
Bindura, Zimbabwe

All rights reserved.

DISCLAIMER: The views and opinions expressed in this journal are those of the authors and do not necessarily reflect the official position of funding partners

Typeset by Divine Graphics

Printed by Divine Graphics

EDITOR-IN-CHIEF
Dr Ellen Sithole, Zimbabwe Ezekiel Guti University, Zimbabwe

MANAGING EDITOR
Dr Noah Maringe, Zimbabwe Ezekiel Guti University, Zimbabwe

EDITORIAL ADVISORY BOARD
Dr Sithabile Manyevere, University of Zimbabwe, Zimbabwe
Dr Tinotenda Chidawu, University of Zimbabwe, Zimbabwe
Dr Prolific Mataruse, University of Zimbabwe, Zimbabwe
Dr Carren Pindiriri, University of Zimbabwe, Zimbabwe
Dr Kiriana Magaya-Dube, Great Zimbabwe University, Zimbabwe

SUBSCRIPTION AND RATES
Zimbabwe Ezekiel Guti University Press Office
Stand No. 1901 Barrassie Rd,
Off Shamva Road
P.O. Box 350
Bindura, Zimbabwe
Telephone: ++263 8 677 006 136 | +263 779 279 912
E-mail: zegupress@zegu.ac.zw
http://www.zegu.ac.zw/press

About the Journal

JOURNAL PURPOSE

The purpose of the *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy Journal* is to provide a forum for urban solutions based on a systems approach and thinking as the bedrock of intervention.

CONTRIBUTION AND READERSHIP

Lawyers, criminologists, economists, public policy experts, bureaucrats, students, researchers and many other experts located in both the private and public spheres.

JOURNAL SPECIFICATIONS

Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy

ISSN 2957-884 2(Print)
ISSN 3007-2182 (Electronic)

SCOPE AND FOCUS

The journal is a forum for the discussion of ideas, scholarly opinions and case studies on law and policy, statutes, constitutions, general rules of the game (institutional mechanisms) and policy pronouncements or declared positions that are put to scrutiny, weighed, interpreted and evaluated. In all these matters, the intention and context usually define the outcomes and impact. The journal is produced bi-annually.

Guidelines for Authors for the *Lighthouse* Journal

Articles must be original contributions, not previously published and should not be under consideration for publishing elsewhere.

Manuscript Submission: Articles submitted to *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy* are reviewed using the double-blind peer review system. The name(s) of author(s) must not be included in the main text or running heads and footers.

Total number of words: 5000-7000 words and set in 12-point font size with 1.5 line spacing.
Language: British/UK English
Title: must capture the gist and scope of the article and must be succinct
Names of authors: beginning with the first name and ending with the surname
Affiliation of authors: must be footnoted, showing the department and institution or organisation.
Abstract: must be 200 words
Keywords: must be five or six containing words **that are not in the title**
Body: Where the authors are more than three, use *et al*.
Italicise *et al., ibid.* and all words that are not English, not names of people or organisations, etc. When you use several authors confirming the same point, state the point and put them in one bracket in ascending order of dates and alphabetically, separated by semi-colon e.g. (Falkenmark, 1989, 1990; Reddy, 2002; Dagdeviren and Robertson, 2011; Jacobsen *et al.,* 2012).

Referencing Style: Please follow the Harvard referencing style in that:
— In-text, citations should state the author, date and sometimes the page numbers.
— The reference list, entered alphabetically, must include all the works cited in the article.

In the reference list, use the following guidelines, religiously:

Source from a Journal

Anim, D.O. and Ofori-Asenso, R (2020). Water Scarcity and COVID-19 in Sub-Saharan Africa. *The Journal of Infection*, *81*(2), 108-09.
Banana, E, Chitekwe-Biti, B. and Walnycki, A. (2015). Co-Producing Inclusive City-Wide Sanitation Strategies: Lessons from Chinhoyi, Zimbabwe. *Environment and Urbanisation*, *27*(1), 35-54.
Neal, M.J. (2020). COVID-19 and Water Resources Management: Reframing our Priorities as a Water Sector. *Water International*, *45*(5), 435-440.

Source from an Online Link
Armitage, N., Fisher-Jeffes, L., Carden, K., Winter, K. (2014). Water Research Commission: Water-sensitive Urban Design (WSUD) for South Africa: Framework and Guidelines. Available online: https://www.greencape.co.za/assets/Water-Sector-Desk-Content/WRC-Water-sensitive-urban-design-WSUD-for-South-Africa-framework-and-guidelines-2014.pdf. Accessed on 23 July 2020.

Source from a Published Book
Max-Neef, M. (1991). *Human Scale Development: Concepts, Applications and Further Reflections*, London: Apex Press.

Source from a Government Department (Reports or Plans)
National Water Commission (2004). Intergovernmental Agreement on a National Water Initiative. Commonwealth of Australia and the Governments of New South Wales, Victoria, Queensland, South Australia, the Australian Capital Territory and the Northern Territory. Available online: https://www.pc.gov.au/inquiries/completed/water-reform/national-water-initiative-agreement-2004.pdf. Accessed on 27 June 2020.

The Source being an Online Newspaper Article
The Herald (2020). Harare City Could Have Used Lockdown to Clean Mbare Market. *The Herald*, 14 April 2020. Available online: https://www.herald.co.zw/harare-city-could-have-used-lockdown-to-clean-mbare-market/. Accessed on 24 June 2020.

Changes in the Data and Information Systems in Zimbabwe: Lessons from Legislation and Policy Post-2018

ABEL MOYO[1], JUSTIN MAKOTA[2] AND FERDINAND KABOTE[3]

Abstract

While freedom to access and dissemination of information and data are critical pillars of effective communication and data transparency, there is, however, consensus that people of capable age and competent understanding are not completely free to access data and information, sensitive or not, due to the overriding principle of data protection. This article critically explores the changes that have occurred in Zimbabwe's data and information cycles and how the changes of rules and regulations have been of immense benefit to the country's socio-economic and political advancement. Furthermore, it traces the changes in data and information systems in Zimbabwe. This article is alive to the fact that the legislature has made strides in amending section 162 of the Criminal Law Codification (Codification and Reform) Act (Chapter 9:23), to provide clarity on issues to do with the procedure regarding the collection of evidence, illegal data collection and procedure for the admissibility of electronic evidence. For data collection, the study used qualitative data and textual analysis. Further, the article unpacks the changes that have occurred and provides a critical analysis on whether there is an inherent alignment with the Constitution of Zimbabwe (2013). This article provides and recommends effective ways Zimbabwe needs to implement towards data and information protection and

1 Department of Data Science and Computer Technology, Zimbabwe Ezekiel Guti University. Orcid ID: 0009-0003-5359-9723, abelmoyo@gmail.com

2 Department of Data Science and Computer Technology, Zimbabwe Ezekiel Guti University. Orcid ID: 0009-0006-8648-115X, jmakota@gmail.com

3 Department of Information Systems, Zimbabwe Ezekiel Guti University. Orcid ID: 0000-0002-6389-0237, fkabote@gmail.com

ascertain whether the protection of sensitive data or not will not affect the freedom to access of information.

Keywords: critical database, data, information electronic communication network, sensitive data

INTRODUCTION

Because of hackers, con artists and fraudsters attacking other information systems users, there is an increased risk of cybercrime owing to technological advancement. A significantly increasing number of legal issues around the matter of data protection has been brought about globally by the rapid advancement of technology (Musa Zimbabwe, 2020). Computer-related crimes, better known as cybercrime, which genre of crimes manifest themselves especially in card cloning, identity theft and fraud involving mobile money, have increased in Zimbabwe. Understanding the risks involved in using data and information systems in a way that is more technologically advanced, the Zimbabwean government has been working to define the guidelines pertaining to how these technologies should be used (Mago, 2012). The Cyber Security and Data Protection Bill was enacted to reduce the risk of cybercrime in the dynamic world of data and information technologies. Tsokota (2020) alleges that the risk of cybercrime is increasing as more people take advantage of e-commerce. Thus, it is good that the legislature is taking legislative action to address cybersecurity vulnerabilities by reviewing laws and passing new legislation to reduce the adverse effects of cybercrime. Every economy depends heavily on data and information systems that are often seen as the foundation of the economy (Pearlson *et al.*, 2024).

Since data and information systems are vital to trade and every economic activity, it is necessary to continuously assess Zimbabwe's data and information systems and find creative and innovative ways of aligning them with international best standards (Kabanda, 2014). The main goals of the study were to evaluate the current state of

data and information systems in Zimbabwe, identify the sector's challenges, look at market competition for fixed, mobile and internet services, evaluate the results of policy and offer solutions to issues impeding the nation's ability to fully implement data and information systems.

STUDY OVERVIEW

The 2016 information and communication technology (ICT) policy noted that Zimbabwe's data and information systems were in significantly worse shape than expected (Veritas, 2020). The results also show that the ICT sector has encountered numerous obstacles preventing it from growing at an exponential rate. These obstacles include a lack of foreign exchange for the purchase of infrastructure, high rates of inflation that reduce users' disposable income, a lack of knowledge and a high rate of brain drain, electricity load shading and a lack of infrastructure in rural areas (*ibid.*). There are four separate pieces of legislation that have a bearing on the regulatory environment for the ICT industry in Zimbabwe: he Postal and Telecommunications Act of 2000, the Broadcasting Services Act of 2001, the Access to Information and Protection of Privacy Act of 2002 and the Interception of Communications Act of 2007.

Currently, regulation of the ICT sector is divided among the Broadcasting Authority of Zimbabwe (BAZ), the Postal Telecommunications Regulation Authority Zimbabwe (POTRAZ) and the Media and Information Commission (MIC). POTRAZ is accountable to the Minister of Transport and Communications, while BAZ and the MIC report to the Minister of Media, Information and Publicity. The Cybersecurity and Data Protection Bill was gazetted on May 15, 2020, demonstrating the excellent implementation of a progressive upgrade of cybersecurity law reform to improve the protection of consumer rights.

METHODOLOGY

Secondary data was gathered from books, Internet, government records, past academic studies and observations. In this study, both

qualitative and quantitative methods of data analysis is utilised. The study primarily employs a qualitative methodology, drawing on secondary sources like books, policy statements, annual reports, Internet and previous research publications. The study is based on systematic empirical research, which relies on experiences or observations often without due regard for a system theory, although prior theories cannot be disregarded. After the textual analysis of the systematic and empirical research and canvassing of theoretical frameworks, some recommendations are proffered with the aim of addressing key areas.

LITERATURE REVIEW.

ICT is defined by Tsokota (2012) as computers, the Internet, CD-ROMs, email, telephones, radios, televisions, videos, digital cameras and media for the collection, storage, processing, transmission and presentation of information in any format (such as voice, data, text and image). This essentially means that data and information systems are not just restricted to a small number of things; rather, they entail several features essential to all aspects of the economy to increase service delivery efficiency. The World Bank (2002:1) defines data and information systems as constitutive of hardware, software, networks and media collection, storage, processing, transmission and presentation of information (voice, data, text, images). However, data and information systems are described by the Government of Zimbabwe (2005:11) as a "…generic term referring to technologies that are used for collecting, storing, editing and disseminating information in various forms". Van der Merwe *et al*. (2016) argue that cybersecurity has grown in significance due to the inherent traits of cybercrime and crimes involving computers. Cybersecurity has become more important in Zimbabwe because of the country's growing reliance on data and information systems, mobile money, online banking and shopping - especially during the COVID-19 lockdowns, with statistics showing a spike of 25% between 2018 and 2020 (Shava, 2020). Cybercrime and computer-related crimes have increased in Zimbabwe, including identity theft, card cloning and fraud involving mobile money.

At regional level, there is evidence of legislative efforts to enact cyber legislation. The Southern African Ministers of Telecommunications and Information (SADC ICT Ministers) met in May 2008 to discuss and fashion a roadmap wherein they sought to standardise ICT laws and policies. During the conference, the ministers agreed on a reference framework for the unification of ICT laws and policies. Moving forward, in December 2008, in Addis Ababa, they officially endorsed the "Support to the Harmonisation of ICT Policies in Sub-Sahara" project under the Harmonisation of ICT Policies in Sub-Saharan Africa (HIPSSA) initiative (Nguimkeu and Okou, 2021).). At their meeting in Mauritius in November 2012, the ministers approved a draft version of the SADC Model Law (2013). The legislature's attempt to ratify the SADC Model Law through the Republic of Zimbabwe's Cybersecurity and Cybercrime Draft Bill, 2017 is evidence of Zimbabwe's admission and understanding that cybersecurity laws and policies should align with those in SADC

Ndlovu (2009) postulates that poverty has many forms and manifests itself in furthering inequalities among different people and is not always caused by a lack of fundamental resources. Lack of data and information systems can also be a driver of poverty. As a result, information is the foundation of Zimbabwe's economy and should be made available to all citizens to help them escape poverty (Tsokota, 2020). Tsokota (*ibid.*) also claimed that the nation's reliance on conventional ICT hardware and software was hurting its ability to compete globally. ICT is now being utilised only for very basic purposes, as argued by Shoko (2012) and people are still using the Internet for non-commercial activities, like social networking, entertainment and browsing news websites — uses which have evolved over time as organisations and businesses have. But over the past three years from 2021, due to lack of liquidity, there has been a sharp increase in the use of mobile money services by all three of Zimbabwe's mobile service providers for sending and receiving money and making payments for services via mobile phones.

Policy, Legal and Regulatory Frameworks in Zimbabwe

Pursuant to the ICT policy of 2016, POTRAZ and BAZ are the regulatory bodies in Zimbabwe that oversee the ICT industry. They not only set the industry pace by formulating time-bound and crucial objectives, but they also regulate the way ICT operates in Zimbabwe (POTRAZ, 2016). The Zimbabwean government created the National ICT Policy Framework in 2005 after realising the potential of ICTs. A review of the policy was completed in May 2012. Since ICT development is evolving quickly, a 2007 revision to the policy was implemented and the 2012 ICT policy took these changes into account. The second ICT strategy for the years 2016-2020 gave direction and guidance to the development and execution of data and information systems, plans and programmes across all economic sectors. This policy framework was established. Although businesses used computers and the Internet, most of the Internet usage was still limited to sending emails and faxes, looking for suppliers and visiting websites (Marumbwa, 2013).

Section 62 of the Constitution of Zimbabwe provides for the right to access to information by stating that every Zimbabwean citizen or permanent resident, including juristic persons and the Zimbabwean media, has the right of access to any information held by the State or by any institution and every person, including the Zimbabwean media, has the right of access to any information held by any person, including the State, in so far as the information is required for the exercise or protection of a right and a right to the correction of information, or the deletion of untrue, erroneous or misleading information held by the State or any institution or agency of the government at any level and which relates to that person (*ibid.*).

Freedom of Information Act (Chapter 10:33).

The Access to Information and Protection of Privacy Act (AIPPA) was repealed and replaced with the Freedom of Information Act (Chapter 10:33). The act's goal is to implement section 62 of the Constitution of Zimbabwe that guarantees the right to information access. A

person's race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and place of birth are all included in the definition of personal information and has been expanded to include sensitive data and identifiable individuals. In accordance with AIPPA, personal information include data about the person's education, health, criminal and work histories, details about any financial transactions they have taken part in, any unique identification number, symbol or other detail assigned to the person, the person's address, fingerprints or blood type, the person's personal preferences, opinions, or views, with the exception of those pertaining to another person or a proposal for a grant, award or prize to be given to another person. It also includes correspondence from the person that is clearly or tacitly private or secret and any additional correspondence that might make the contents of the first correspondence public, views or opinions expressed by another person about the individual; views or opinions expressed by another person regarding a proposal for a grant, award or prize to be given to the individual, and the name of the individual when it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been deceased for more than 20 years (Chitumba *et al.*, 2024).

Information protected or privileged from disclosure in victim-friendly courts and discussions or actions of the Cabinet and its committees are now explicitly included in the definition of protected information. Thus, information offered by minors in these courts is privileged and legally protected from disclosure. Requests for access to public records must go through a rigorous process, and the public office must reply to requests for access to information within 21 days. The officer must advise the applicant if the information is not available or cannot be located. The opportunity to inspect the information, copies of the information, appropriate arrangements for its reproduction, written

transcripts of sound recordings and computerised information made readable are all included in the actual access process. There is no single piece of legislation that controls data security and privacy yet (Omer, 2022).

The following statutes, together with any industry specific requirements, are in place to regulate data privacy and security: the Access to Information and Protection of Privacy Act (Chapter 10:27), the Census and Statistics Act (Chapter 10:29); the Consumer Protection Act (Chapter 14:14); the Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04); the Interception of Communication Act (Chapter 11:20); and the National Registration Act (Chapter 10:17).

THE DATA PROTECTION ACT (CHAPTER 12:07)

The Data Protection Act (DPA) aims at implementing the right to privacy guaranteed by Zimbabwe's Constitution and to align data protection laws in Zimbabwe with those of the rest of Sub-Saharan Africa. The SADC Model Law for Data Protection was implemented for Zimbabwe to harmonise legislation, bringing Zimbabwe's legal system into compliance with globally acknowledged data protection standards. Therefore, the Act is designed to control how public and private entities process personal information, stop illegal or arbitrarily use of information and regulates the collecting, processing, transmitting and storing of data about identifiable individuals, seeks to regulate data protection and provides for the setting up of a data protection authority (Chitumba *et al*., 2024)

The DPA also amended the Criminal Procedure and Evidence Act, the Interception of Communications Act and the Criminal Law (Codification and Reform Act), three laws that are currently in place under the Zimbabwean Constitution (Veritas, 2020). Data controllers are required by the DPA to process data legally and equitably. They must make sure that data is gathered only for clearly defined,

explicit and legal objectives, while accounting for all pertinent variables and they must make sure that the DPA's rules are followed. Any establishment, whether founded in Zimbabwe or outside, is subject to the DPA, if the tools used to process the data are based there and the processing is not done for data transit. However, this regulation does not apply to data being acquired solely for the purpose of transiting it from Zimbabwe. Additionally, if a data handler is not technically formed or registered in Zimbabwe, they must appoint a representative within the country (Poshai *et al.*, 2023).).

Data Protection Impact Assessment

Data handlers are not required to perform recurring impact assessments on data protection. Nonetheless, since the DPA gives the regulatory body the ability to conduct additional inspections and evaluations of the legislative and security measures used by a data controller (POTRAZ, 2019). To make sure that their procedures comply with the DPA's obligations, it is therefore strongly advised that all data handlers carry out their own impact assessments, particularly for high-risk data processing operations.

Penalties for Non-compliance

To comply with Zimbabwe's recently passed DPA, any government can do so by making sure it complies with certain requirements, like hiring a qualified representative in Zimbabwe if the data handler is not officially registered there; disclosing the manner and purpose of data collection through an open and transparent privacy policy; having a strong consent management system in place to guarantee that consent is obtained legally; conducting regular data mapping exercises to create a comprehensive structure of all data being collected, stored and transferred to guarantee compliance; and conducting regular data protection impact and risk assessments to make sure they are complying with the new laws (Mhandu, 2020).

THE CRIMINAL LAW JURISDICTION.

As previously mentioned, Chapter VIII of the Criminal Law Codification and Reform Act (hereinafter referred to as the Codification) was specifically created by the legislature in 2004 to address offences relating to computers. Under section 163 of the Codification, hacking now constitutes a crime. Similarly, section 167 of the Codification defines card cloning as the illegal use or possession of a credit or debit card, while section 168 prohibits the illegal use of a password or pin number. Despite being created to address cybercrimes, Chapter VIII of the Codification excludes some of the most prevalent ones that are already widespread in e-commerce, such as fraud using mobile money transactions. The typical crimes section of the Codification addresses certain cybercrimes that are not covered by Chapter VIII. However, positivists contend that the government must specifically pass explicit cybercrime laws to establish a clearly defined charge for the purpose of prosecuting those accused of cybercrime. Mugari *et al*. (2023), state that academics have argued that punishing illegal access to a computer system with a specific criminal goal is the fundamental principle of cybercrime since it ultimately prevents harm or alteration to systems and the data on them. This argument highlights the necessity of passing laws that clearly define cybercrimes and begs the legislature to be deliberate in their provisions so that litigants are not left to fend for themselves when their rights — whether they be to data privacy, dignity, or any other constitutional right — are violated.

CONCLUSION AND RECOMMENDATIONS

This article suggests that ICT education should start at a local level across the nation, even in rural areas. This study also recommends that to foster competition and enhance service delivery, the government must develop policies that will draw in additional investors into the ICT industry. The report also suggests encouraging the development of regional hardware, software and infrastructure. It also underlines the necessity of raising the quality and accessibility of services and the creation of new ones through privatisation and

de-monopolisation. Zimbabwe's government should create an infrastructure that facilitates the development of ICT networks in the most vulnerable rural communities. The government should understand that it is ultimately responsible for fostering an environment that encourages the use of ICTs for the country's advantages. To make this possible, the fundamentals of economics must be established. Furthermore, there is need to encourage ICT adoption in all communities, particularly rural ones and include ICTs in educational curriculum, starting at the early childhood education level. It should be the goal of rural residents' training to improve their proficiency with contemporary technology.

Additionally, efforts must be made to revive and enhance the capacity of power generation, transmission and distribution. It is abundantly clear that Zimbabwe must investigate and enhance current power generation techniques that may include, but are not limited to, solar, wind, water, biogas and even nuclear energy, to augment the thermal and hydropower generated electricity. Additionally, where it does not negatively affect competition, a well-regulated programme for the full use of infrastructure sharing must be promoted. Sharing network infrastructure helps to lower production costs and frees up service providers' resources to concentrate more on other innovative initiatives that will enhance service delivery.

Promoting local ICT product creation is also necessary to guarantee content relevance and the adoption of suitable, international standard-compliant technology. The government may encourage that by allocating funds for the advancement and innovation of ICT. It can assist local ICT product development by encouraging the use of domestically produced hardware and systems. Reducing operator licensing fees is also necessary because they are now prohibitively expensive for many. This will encourage more players to enter the market and, in the long run, improve ICT industry relations that will help service providers stay competitive.

The new DPA in Zimbabwe can be complied with by any establishment by making sure that certain requirements are mandatory, like hiring a qualified representative in Zimbabwe if the data handler is not formally registered there, disclosing the manner and purpose of data collection through an open privacy policy, having a strong consent management system in place to guarantee consent is obtained legally, conducting regular data mapping exercises to create a comprehensive structure of all data being collected, stored and transferred to guarantee compliance and conducting regular data protection impact and risk assessments to make sure they comply with the new laws.

REFERENCES

Chitumba, P. and Mupanedemo, F. (2024). Harness ICT to improve service delivery'. https://www.google.com/amp/s/www.herald.co.zw/harness-ict-to-improve-service-delivery/amp/ (Accessed 25 March 2024).

Chitumba, P. and Mupanedemo, F. (2024). Harness ICT to improve service delivery'. https://www.google.com/amp/s/www.herald.co.zw/harness-ict-to-improve-service-delivery/amp/ (Accessed 25 March 2024).

Davis, F. D., Bagozzi, R. and Warshaw, P.R (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science, 35*(8), 45-56.

Davis, F. D., Bagozzi, R. and Warshaw, P.R (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science, 35*(8), 45.

Government of Zimbabwe (2005). Criminal Law (Codification and Reform) Act [Chapter 09:23]

Government of Zimbabwe (2005). Criminal Law (Codification and Reform) Act [Chapter 09:23]

Government of Zimbabwe (2013). Data Protection Bill, Electronic Transactions and Electronic Commerce Bill, 2013; and the Cybercrime and Cybersecurity Bill, 2017 of the Republic of Zimbabwe.

Government of Zimbabwe (2013). Data Protection Bill, Electronic Transactions and Electronic Commerce Bill, 2013; and the Cybercrime and Cybersecurity Bill, 2017 of the Republic of Zimbabwe.

Kabanda, G. (2014). The impact of ICTs on customer service excellence in Zimbabwe. *International Journal of Emerging Technology and Advanced Engineering, 4*(5), 312-324.

Kabanda, G. (2014). The impact of ICTs on customer service excellence in Zimbabwe. *International Journal of Emerging Technology and Advanced Engineering, 4*(5), 312-324.

Mago, S. (2012). The Impact of Information and Communication Technologies (ICTs) on Rural Livelihood: The Case of Smallholder Farming in Zimbabwe (Doctoral dissertation, University of Fort Hare).

Mago, S. (2012). The Impact of Information and Communication Technlogies (ICTs) on Rural Livelihood: The Case of Smallholder Farming in Zimbabwe (Doctoral dissertation, University of Fort Hare).

Marumbwa, J. (2013). A pragmatic assessment of the determinants of consumer brand preferences in the mobile telecommunications services market in Masvingo Urban, Zimbabwe. *Management and Administrative Sciences Review, 2*(2), 144-155.

Mhandu, R. (2020). An Analysis of Cyberlaws in Zimbabwe: A Note on the Cyber Security and Data Protection Bill. Available online: https://www.mmmlawfirm.co.zw/analysis-cyberlaws-zimbabwe - note-cyber-security-data-protection-bill/ (Accessed 27 March 2024)

Mhandu, R. (2020). An Analysis of Cyberlaws in Zimbabwe: A Note on the Cyber Security and Data Protection Bill.https://www.mmm lawfirm.co.zw/analysis-cyberlaws-zimbabwe-note-cyber-security -data-protection-bill/ (Accessed 27 March 2024)

Mugari, I. *et al*. (2023). Trends, Impacts and Responses to Cybercrime in the Zimbabwean Retail Sector, 22(4), 254-265.

Safer Communities. Available online: https://doi.org/10.1108/SC-03-2023-0011.

Mugari, I. *et al*. (2023). Trends, Impacts and Responses to Cybercrime in the Zimbabwean Retail Sector, Vol. 22 No 4 pp 254-265. Safer Communities .https://doi.org/10.1108/SC-03-2023-0011.

Musa Zimbabwe (2020). Unpacking the Freedom of Information Regulations | MISA Zimbabwe.https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/ (Accessed 25 March 2024)

Musa Zimbabwe (2020). Unpacking the Freedom of Information Regulations | MISA Zimbabwe.https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/ (Accessed 25 March 2024)

Nguimkeu, P., & Okou, C. (2021). Leveraging Digital Technologies to Boost Productivity in the Informal Sector in Sub-Saharan Africa. *Review of Policy Research*, *38*(6), 707-731.

Omer, M. (2022). Overview of Zimbabwe New Data Protection Act. https://securiti.ai/zimbabwe-new-data-protection-act/ (Accessed 26 March 2024)

Omer, M. (2022). Overview of Zimbabwe New Data Protection Act. https://securiti.ai/zimbabwe-new-data-protection-act/ (Accessed 26 March 2024)

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2024). *Managing and Using Information Systems: A Strategic Approach*. John Wiley & Sons.

Poshai, L., Chilunjika, A., & Intauno, K. (2023). Examining The Institutional and Legislative Frameworks for Enforcing Cybersecurity in Zimbabwe. *International Cybersecurity Law Review*, *4*(4), 431-449.

Shava, E.T., Maramura, C. (2020). Assessing the Implementation of Information Communication Technology (ICT) for Sustainable Development in NGOs in Zimbabwe. *Journal of Communication, 7*(2), 208-215.

Shava, G.N. (2020). Quality Education for Sustainable Development in Zimbabwean Higher Education: Towards UNDP 2030 SDG. The Education Systems of Africa, pp.1-26.

Shava, G.N. (2020). Quality Education for Sustainable Development in Zimbabwean Higher Education: Towards UNDP 2030 SDG. The Education Systems of Africa, pp.1-26.

Shoko, A (2012). Retrieved from techzim: http://www.techzim.co.zw/2012/08/thedespairing-state-of-ecommerce-in-zimbabwe/

Tsokota, T. and Solms, R., 2013. ICT and the turning-around of the Zimbabwean Economy. In International Conference on ICT for Africa (pp. 20-23).

Tsokota, T. and Solms, R., 2013. ICT and the turning-around of the Zimbabwean Economy. In International Conference on ICT for Africa (pp. 20-23).

Van der Merwe, D.P. *et al*. (2016). *Information and Communications Technology Law. 2nd edn*., 1, South Africa: LexisNexis.

Van der Merwe, D.P. *et al*. (2016). *Information and Communications Technology Law. 2nd edn*., 1, South Africa: Lexis Nexis.

Veritas, D. B. Y (2020)/ Zimbabwe National Policy for Information and Communications Technology (ICT)', 1-44.

Veritas, D. B. Y (2020)/ Zimbabwe National Policy for Information and Communications Technology (ICT)', 1-44.