Global Scientific JOURNALS

GSJ: Volume 12, Issue 5, May 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

Data Protection Challenges on Digital Platforms: A Case for Zambia

By

Mr. Nalumino Moola[1] (ZCAS University, SoCTAS, P O Box 35423, Lusaka. Email; nalumino.moola@zcasu.edu.zm)

Dr Sidney Kawimbe (ZCAS[2] University, School of Business, P O Box 35423, Lusaka. Email: sidney.kawimbe@zcasu.edu.zm

Abstract

This study investigates the data protection challenges confronting digital platforms in Zambia, focusing on issues such as online privacy practices, personal data breaches, regulatory frameworks, cybersecurity incidents, user awareness, and the impact of emerging technologies. Through a desk study approach, we conducted a thorough review and analysis of existing literature, reports, and regulatory frameworks to reveal key insights into Zambia's data protection landscape. Our findings highlight the regulatory framework governing data protection, including provisions of the Data Protection Act of 2021. Despite legislative efforts, challenges persist in implementation and enforcement, necessitating enhanced capacity building and public awareness initiatives. Privacy practices on digital platforms remain a concern, requiring greater transparency and accountability in data handling. Cybersecurity incidents pose significant risks to user data, emphasizing the importance of robust cybersecurity measures and incident response protocols. User awareness and empowerment are crucial for promoting data privacy and protection, underscoring the need for tailored educational initiatives and awareness campaigns. Additionally, the integration of emerging technologies such as blockchain holds promise for enhancing data security and transparency, although regulatory challenges and interoperability issues must be addressed. This study provides valuable insights and recommendations for policymakers, industry stakeholders, and researchers to address data protection challenges and foster trust in Zambia's digital environment.

***Key Words**: Digital Platform, Data Protection, Online Privacy, Data Governance.*

1. INTRODUCTION

The influence of technology continues to redefine our daily routines and the way we interact with each other in our various societies. Digital platforms, particularly the internet, have emerged as indispensable infrastructures facilitating global connectivity and service delivery (Castells, 2019). With an increasing universal accessibility, the internet enables seamless access to information and data exchange across geographical boundaries. In addition, advancements in computing technologies have endowed modern systems with enhanced storage capacities and processing capabilities, further catalyzing the digital revolution (Barroso & Holzle, 2019).

The advent of digital platforms has reshaped traditional business models, enabling companies to reach broader audiences and operate on a global scale. Platforms such as social media networks, e-commerce websites, and online service providers have become integral to daily life, fostering connectivity and economic opportunities (Hosseini & Rahim, 2020). Service delivery through digital platforms has witnessed exponential growth, driven by the convenience and efficiency they offer. With their global extensive reach and functionality, digital platforms amass vast amounts of user data, ranging from personal information to behavioral patterns. This increased delivery of service through digital platforms has led to the collection and accumulation of extensive datasets on individuals, encompassing a wide array of demographic, behavioral, and transactional information (Boyd, 2014). From e-commerce transactions to social media engagements, digital platforms have become integral to modern life, necessitating the collection and processing of vast amounts of personal data (Andrejevic, 2018).

The widespread collection and utilization of personal data on digital platforms have raised significant concerns regarding data privacy and protection. Individuals' personal data is often harvested, analyzed, and shared with various stakeholders, including data brokers and advertisers (Zuboff, 2019). This processing of personal data not only compromises individuals' privacy but also exposes them to risks of identity theft, surveillance, and targeted manipulation (Baruh et al., 2017). Mwansa & Simuyandi (2019) also adds by stating that “the collection, storage, and utilization of personal data present inherent risks, including unauthorized access, data breaches, and general misuse”. The processing of personal data has prompted a thriving global market for data trading, where individuals' data / information is bought, sold, and exchanged for various purposes (Acquisti & Grossklags, 2019).

2. LITERATURE REVIEW

The literature review presents an extensive examination of data protection challenges in the digital age, offering insights into various dimensions of the topic. This section synthesizes existing research and scholarly discourse to provide a comprehensive overview of key themes and finding pertinent to the case of Zambia. Abu Bakar (2017) underscores the widespread nature of this phenomenon, highlighting the prevalence of data brokerage practices worldwide. Such practices underscore the need for robust data protection frameworks to safeguard individuals' rights and mitigate potential harms arising from this trading of data. In the Zambian context, just like in many other developing nations, the rapid digitization of services has introduced unique challenges concerning data protection (Jalasi, 2023). While digital platforms offer immense opportunities for economic growth and innovation, they also raise concerns about privacy, security, and regulatory compliance. Despite efforts to enact legislation such as the Data Protection Act of 2021, implementation and enforcement remain inadequate, leaving individuals' data vulnerable to exploitation (Mwansa & Simuyandi, 2019). Resource constraints limited technical expertise, and a lack of public awareness regarding personal data rights, further increase the challenges of ensuring effective data protection measures in Zambia's digital landscape.

The implications of inadequate data protection extend beyond individual privacy concerns to encompass broader societal and economic repercussions. Users' trust in digital platforms diminishes in the face of data breaches and privacy infringements, leading to reduced engagement and potential economic losses for businesses (Hosseini & Rahim, 2020). Therefore, without robust data protection measures, Zambia's aspirations for digital innovation and economic growth may be hindered. The intersection of digital platforms and data protection presents a complex and evolving landscape laden with challenges and opportunities. By interrogating the unique dynamics at play within the Zambian context, this article endeavors to inform policy makers, industry stakeholders, and the public about the imperative of safeguarding data rights in the digital era. Through collaborative efforts and innovative solutions, Zambia can navigate the intricacies of data protection, fostering a digital environment that prioritizes online privacy, data protection and the trust from the users. Against this background, this article seeks to delve into the specific data protection challenges encountered by digital platforms operating within the Zambia context.

By examining regulatory frameworks, technological infrastructures, and socio-economic dynamics, the research seeks to identify key impediments to data protection and propose strategies for addressing them. Through empirical analysis and theoretical insights, we endeavor to

contribute to the discourse on enhancing online privacy and data protection in the Zambian digital platform. The following subsections delve into specific themes, connecting them to the broader discourse on data protection and digital platforms.

2.1 Service Delivery on Digital Platform

The rapid expansion of digital platforms has fundamentally reshaped the global business landscape, offering unprecedented seamless connectivity, service delivery, innovation, and economic growth (Castells, 2019). However, this transformation has also precipitated heightened concerns surrounding data privacy and protection. Zuboff (2019) discusses the emergence of surveillance capitalism, emphasizing the exploitation of personal data for commercial gain. This highlights the need for robust data protection frameworks to safeguard individuals' rights to online privacy. "Surveillance capitalism" refers to an economic system or business model in which companies collect and analyze vast amounts of personal data from individuals, often without their explicit consent, for the purpose of generating revenue and maximizing profits (Zuboff, 2019). This paradigm shift underscores the imperative of robust data protection frameworks to mitigate the risks of online privacy infringements and personal data exploitation.

In addition, the proliferation of Internet of Things (IoT) devices has introduced new challenges to data privacy. With the increasing interconnectedness of everyday objects, concerns regarding the collection, storage, and processing of personal data have become more pronounced. Research by Cavoukian & Jonas (2019) provides further emphasizes on the need for the “privacy-by-design principles” to be integrated into IoT systems from their inception to address these challenges effectively.

2.2 Data Governance Considerations

Across the globe, countries are grappling with the challenge of balancing innovation and economic competitiveness with the protection of individuals' online privacy and associated data rights. Acquisti & Grossklags (2019) observe the proliferation of data trading practices, where individuals' personal data is processed and exchanged in a thriving market. Such trends underscore the need for comprehensive data governance mechanisms encompassing legislative, regulatory, and ethical dimensions.

The evolving landscape of data governance presents both challenges and opportunities for emerging economies like Zambia, as they navigate the complexities of digital integration while striving to safeguard citizens' online privacy rights. Furthermore, international collaborations and agreements play a crucial role in shaping global data governance frameworks. For instance, the Budapest Convention on Cybercrime provides a framework for international cooperation in

combating cybercrime and protecting data across borders (Council of Europe, 2001). However, challenges remain in ensuring harmonization and alignment of data protection standards across jurisdictions to facilitate seamless data flows while upholding online privacy rights for the citizens.

2.3 Legal and Regulatory Frameworks

Efforts to address data protection challenges have been accompanied by the enactment of legislation and regulatory frameworks at both international and national levels. At the global level, international instruments such as the European Union's General Data Protection Regulation (GDPR) have set global standards for data protection, prompting calls for alignment and harmonization of domestic laws to ensure consistency and interoperability in cross-border data flows. In Zambia, the introduction of the Data Protection Act of 2021 represents a significant step towards enhancing data privacy and protection. However, Mwansa & Simuyandi (2019) highlight implementation gaps and enforcement challenges that undermine the effectiveness of existing regulations. The role of regulatory authorities in overseeing compliance and enforcing data protection laws is crucial in ensuring accountability and transparency in data processing practices. Research by Edwards & Bayley (2020) underscores the importance of regulatory oversight in addressing challenges such as data breaches and misuse of personal data, particularly in the context of emerging technologies and digital platforms.

2.4 Digital Advancements and Ethical Considerations

Advancements in technology, including artificial intelligence (AI) and machine learning algorithms, have introduced new dimensions to the data protection discourse. While these technologies hold immense potential for enhancing data protection and privacy, they also pose ethical dilemmas related to algorithmic bias, data discrimination, and surveillance (Crawford, 2016).

Other scholars, such as Nissenbaum (2010), emphasize the importance of integrating ethical considerations into the design and deployment of digital platforms to mitigate potential harms and ensure accountability in data processing practices. Furthermore, the emergence of decentralized technologies such as blockchain offers novel approaches to data protection and privacy. Research by Kuo et al. (2020) explores the potential of blockchain-based solutions in enhancing data protection, transparency, and user control over personal data. However, challenges such as scalability, interoperability, and regulatory compliance need to be addressed for widespread adoption of blockchain in data protection.

2.5 Socio-Economic Implications

The implications of inadequate data protection extend beyond individual privacy concerns to encompass broader societal and economic ramifications. Hosseini & Rahim (2020) adds by highlighting the erosion of trust in digital platforms resulting from data breaches and privacy infringements, which can lead to decreased user engagement and loss of business opportunities. Moreover, without robust data protection measures, countries like Zambia may face impediments to digital innovation and economic development, hindering efforts to leverage digital technologies which promote economic growth and prosperity.

2.6 In Summary

The literature review has exposed the nature of data protection challenges on digital platforms, with implications spanning legal, regulatory, technological, ethical, and socio-economic domains. This article provides a foundational understanding of the complexities inherent in safeguarding online privacy rights within the Zambian context. Building upon this foundation, this article goes into specific challenges and proposes strategies for addressing them, thereby contributing to the advancement of online privacy and data protection in Zambia's digital landscape. By synthesizing existing research, identifying gaps, and providing associated recommendations, this research contributes to the advancement of knowledge in the field.

3. METHODOLOGY

This study adopted a desk study approach to investigate data protection challenges on digital platforms in Zambia. The desk study approach was chosen due to its suitability for gathering and analyzing existing literature, reports, regulations, and other relevant sources of information related to the topic. This methodology allows for a comprehensive review and analysis of available materials, providing insights into the data protection landscape in Zambia.

By leveraging existing literature, reports, and regulatory frameworks, this study was able to uncover key insights and trends in data protection practices within the Zambian context.

3.1 Literature Review

Extensive searches were conducted in academic databases, online repositories, government websites, and other sources to identify scholarly articles, research papers, reports, and publications addressing data protection issues, digital platforms, and related topics in Zambia. Keywords and search terms such as "data protection", "digital platforms", “Online Privacy”, “Data Governance” and "cybersecurity regulations" were utilized to ensure comprehensive coverage of relevant literature.

3.2 Document Analysis

Identified documents, including academic papers, government reports, policy documents, and regulatory frameworks, were systematically reviewed and analyzed to extract key insights, trends, and findings related to data protection challenges on digital platforms in Zambia. Emphasis was placed on identifying relevant case studies, empirical evidence, and regulatory frameworks specific to the Zambian context.

3.3 Synthesis and Interpretation

The findings from the literature review and document analysis were synthesized and interpreted to gain a comprehensive understanding of the data protection landscape in Zambia. Themes, patterns, and emerging issues were identified, and insights were drawn to inform the discussion and analysis presented in the article.

4. Findings

The findings of the desk study revealed several key insights into the data protection challenges faced by digital platforms in Zambia. Through an extensive review and analysis of existing literature, reports, and regulatory frameworks, the following themes and patterns emerged:

4.1 Regulatory Landscape

The desk study identified the regulatory framework governing data protection in Zambia, with a focus on the Data Protection Act of 2021 (Mwansa & Simuyandi, 2019). Analysis of the legislation revealed provisions related to the collection, processing, and storage of personal data by digital platforms. Despite the enactment of the Data Protection Act of 2021, challenges persist in implementation and enforcement, as highlighted in the literature.

In addition, Chisenga & Muzimu (2024) adds by stating that limited resources, capacity constraints, and a lack of public awareness contribute to gaps in compliance and enforcement mechanisms. This poses significant challenges to effectively protect online privacy in platforms such as the Zambia's digital ecosystem. These findings underscore the need for enhanced capacity building and public awareness initiatives to strengthen compliance mechanisms.

4.2 Privacy Practices on Digital Platforms

The review of literature highlights concerns on the online privacy practices employed by digital platforms operating in Zambia. Despite growing awareness of data privacy issues, concerns remain regarding the transparency and accountability of digital platform operators in handling user data (Diggers.News, 2021). Research underscores the need for greater transparency and user control over personal data on digital platforms to enhance trust and mitigate privacy risks. The gap that has been identified emphasizes the importance of greater transparency and user empowerment to

mitigate privacy risks and foster trust. Furthermore, the proliferation of data-driven business models raises questions about the ethical implications of data collection, profiling, and targeted advertising practices employed by these digital platforms (Hosseini & Rahim, 2020).

4.3 Data Breaches and Cybersecurity Incidents

Instances of data breaches and cybersecurity incidents pose significant risks to user data on digital platforms in Zambia (Jalasi, 2023). The findings highlight the prevalence of data breaches and cybersecurity incidents affecting digital platforms in Zambia. Analysis of reported cases revealed instances of unauthorized access, data theft, and security vulnerabilities compromising the confidentiality and integrity of user data (Mwansa & Simuyandi, 2019). Research emphasizes the need for robust cybersecurity measures and incident response protocols to mitigate the risks of data breaches and protect user privacy. Furthermore, the implications of data breaches extend beyond individual privacy concerns to encompass broader economic and reputational impacts on affected organizations and stakeholders.

4.4 User Awareness and Empowerment

A recurring theme in the literature is the importance of user awareness and empowerment in promoting data privacy and protection on digital platforms. Despite efforts by the Zambian Government to enact legislation and regulatory frameworks, the effectiveness of data protection measures hinges on user understanding of their rights and responsibilities regarding personal data (CaseGuard.com, 2021).

Research emphasizes the role of digital literacy programs and public education campaigns in raising awareness about data privacy risks and empowering users to make informed decisions about their online activities (Andrejevic, 2018).

4.5 Emerging Technologies and Privacy Challenges

The desk study identified emerging technologies such as artificial intelligence (AI), Internet of Things (IoT), and blockchain as posing new challenges to data protection in Zambia. While these technologies offer transformative opportunities for innovation and economic development, they also introduce complexities and risks related to data privacy and protection (Kuo et al., 2020). Research explores the potential of blockchain-based solutions in enhancing data protection and transparency, while highlighting concerns about regulatory compliance and interoperability in the Zambian context. Overall, the findings highlight the multifaceted nature of data protection challenges on digital platforms in Zambia. By addressing these challenges through collaborative efforts and innovative solutions, policymakers, industry stakeholders, and researchers can foster a

digital environment that prioritizes online privacy, data protection, and the relevant trust from the users.

5. Conclusion and Recommendations

In conclusion, this study sheds light on the pressing data protection challenges faced by digital platforms in Zambia, drawing insights from existing literature, reports, and regulatory frameworks. Through a desk study approach, several key findings emerged, shedding light on the regulatory landscape, privacy practices, cybersecurity incidents, user awareness, and the impact of emerging technologies on data protection. The findings underscore the critical need for concerted efforts to address these challenges and foster a digital environment that prioritizes online privacy, data protection, and user trust in Zambia. Based on the findings, the research has arrived at the following conclusions and recommendations:

5.1 Strengthen Implementation and Enforcement

The regulatory framework governing data protection in Zambia, as embodied in the Data Protection Act of 2021, provides a foundation for safeguarding individuals' personal data. However, challenges persist in implementation and enforcement, necessitating concerted efforts to address capacity constraints, enhance public awareness, and strengthen compliance mechanisms.

Policymakers and regulatory authorities should prioritize capacity building and resource allocation to enhance the implementation and enforcement of existing data protection regulations. This includes investing in training programs for regulatory personnel and establishing mechanisms for monitoring compliance among digital platform operators.

5.2 Enhance User Awareness and Empowerment

User awareness and empowerment are central to promoting a culture of data privacy and protection in Zambia's digital landscape. Digital literacy programs, educational initiatives, and awareness campaigns should be tailored to diverse audiences, including individuals, businesses, and policymakers. By empowering users to make informed decisions about their online activities and privacy preferences, Zambia can foster a more resilient and privacy-conscious digital environment.

5.3 Improve Privacy Practices on Digital Platforms

Digital platform operators play a pivotal role in fostering trust and transparency among users through robust privacy practices and ethical data handling. Our recommendation to digital service providers is that of prioritizing online privacy and data protection by implementing privacy-by-design principles, providing clear and accessible privacy policies, and offering user-friendly controls for managing personal data. Additionally, investments in cybersecurity measures and

incident response protocols are essential to mitigate the risks of data breaches and safeguard user information from unauthorized access or exploitation of citizens' personal data.

5.4 Invest in Cybersecurity Measures

Robust cybersecurity measures and incident response protocols are essential for mitigating the risks of data breaches and protecting user information from unauthorized access or exploitation. Digital platform operators should invest in cybersecurity infrastructure and collaborate with relevant stakeholders to ensure that a proactive approach to cybersecurity is adopted.

5.5 Embrace Emerging Technologies Responsibly

While emerging technologies such as blockchain offer potential solutions for enhancing data security and transparency, regulatory challenges and interoperability issues must be addressed. Policymakers, industry stakeholders, and researchers should collaborate to develop regulatory frameworks and standards that enable responsible adoption of these technologies while safeguarding online privacy rights.

5.6 Multi-Faceted Approach

Addressing data protection challenges on digital platforms in Zambia requires a multi-faceted approach involving legislative reforms, industry best practices, user empowerment initiatives, and technological innovations. By implementing these recommendations in tandem, stakeholders can navigate the complexities of the digital age while safeguarding individuals' data protection rights and fostering trust in the Zambian digital ecosystem.

REFERENCES

Acquisti, A., & Grossklags, J. (2019). Economics and Behavioral Economics of Privacy and Data Protection. In M. Hildebrandt & E. De Vries (Eds.), Handbook of Privacy Studies (pp. 297-317). Edward Elgar Publishing.

Andrejevic, M. (2018). Social Media and Surveillance: The Threat of the New. Critical Studies in Media Communication, 35(5), 447-451.

Barroso, L. A., & Hölzle, U. (2019). The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines (3rd ed.). Morgan & Claypool.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication, 67(1), 26-53.

Boyd, D. (2014). "It's Complicated: The Social Lives of Networked Teens" by Boyd Danah, Yale University Press.

CaseGuard.Com. (2021). A New Degree of Data Privacy for Zambian Citizens. [Online] Available At: https://caseguard.com/articles/a-new-degree-of-data-privacy-for-zambian-citizens. Published Date: November 10, 2021. [Accessed Date: 17th April 2024].

Castells, M. (2019). The Rise of the Network Society: The Information Age: Economy, Society, and Culture (Vol. I). John Wiley & Sons.

Cavoukian, A., & Jonas, J. (2019). Privacy by Design: A Visionary Approach to Safeguarding Data. Journal of Information Privacy, 7(3), 215-230.

Chisenga, S. & Muzumu, F. (2024). Zambia - Data Protection Overview. [Online] Available At: https://www.dataguidance.com/notes/zambia-data-protection-overview. April 2024: by Sydney Chisenga and Francis Muzimu. [Accessed Date: 24th April 2024]

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).

Crawford, K. (2016). Artificial intelligence's white guy problem. Author: Kate Crawford – The New York Times, 25.

Diggers.News, (2021). The Data Protection Act: Impact and Challenges of Zambia's first law on Protection of Personal Data. [Online] Available At: https://diggers.news/guest-diggers/2021/05/03/the-data-protection-act-impact-and-challenges-of-zambias-first-law-on-protection-of-personal-data/uest diggers. 3rd April 2021: By Diggers Correspondent. [Accessed Date: 20th March 2024]

Edwards, L., & Bayley, T. (2020). Regulatory Oversight in Data Protection: Challenges and Opportunities. Journal of Regulatory Compliance, 5(2), 45-60.

Hosseini, S. M., & Rahim, N. Z. A. (2020). The Challenges of Data Protection in Digital Platforms. Journal of Information Science and Technology.

Jalasi, A. J. (2023). Data Privacy and Protection in Workplaces in Zambia: A Brief Overview. [Online] Available At: https://www.dentons.com/en/insights. Published on 9th March 2023: Contact: Joseph Alexander Jalasi. [Accessed Date: 9th April 2024].

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2020). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocz220

Mwansa, C., & Simuyandi, C. (2019). Data Protection Laws in Emerging Economies: A Case Study of Zambia. International Journal of Cybersecurity and Digital Forensics, 8(1).

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Author: Helen Nissenbaum – Stanford University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.