Analysis of The Role of Women in Governing Africa's Digital Infrastructure: A Policy Analysis of Data Protection and Cybersecurity Frameworks in Chad: An African Perspective

Alice Hewitt
University of N'Djamena
King Faisal University of Chad

Judith Mitchell
King Faisal University of Chad
University of N'Djamena

Correspondence: ahewitt@hotmail.com

Abstract

This study presents a policy analysis examining the role and representation of women in the governance of digital infrastructure in Chad, with a specific focus on data protection and cybersecurity frameworks. It addresses a critical gap in the literature on gender, digital governance, and African policy studies, where the intersection of these fields remains underexplored, particularly in Francophone Sahelian contexts. The research is guided by the question: to what extent do Chadian digital policy frameworks incorporate gender considerations and enable women's participation in governance structures? Employing a qualitative documentary analysis, the methodology systematically examines primary sources, including national laws, strategy documents, and institutional policies pertinent to Chad's digital ecosystem. The analysis reveals a significant marginalisation of gender-specific provisions within existing frameworks, highlighting a disjuncture between broader national gender policies and sector-specific digital governance. The findings indicate that this omission constrains inclusive policy development and impedes the realisation of women's full potential in shaping a secure and equitable digital transformation. The study concludes by emphasising the necessity of integrating explicit gender perspectives into digital infrastructure governance to strengthen policy coherence and developmental outcomes, offering insights relevant to similar post-colonial African states.

INTRODUCTION

The governance of digital infrastructure is a critical determinant of inclusive development in Africa, yet the specific role of women in shaping this governance, particularly within data protection and cybersecurity frameworks, remains a significant research lacuna. While studies affirm the importance of digital infrastructure for trade, resilience, and rights in African contexts (Afolabi & Fatai, 2026; Ngalim, 2025; Arowolo, 2025), they frequently overlook the gendered dimensions of

policy formulation and implementation. In Chad, where digital transformation intersects with complex socio-political dynamics, understanding how women participate in governing these emerging digital domains is essential for crafting equitable and effective policy. This study addresses this gap by asking: to what extent are women represented and their perspectives integrated in the governance of Chad's data protection and cybersecurity frameworks? The analysis is significant as it links broader discourses on gender-inclusive governance, digital sovereignty in Africa (Bu, 2025), and the specific challenges of cybersecurity resilience in developing nations (Mkhwanazi & Futcher, 2025). By critically analysing Chadian policy documents and institutional structures, this research provides original insights into the mechanisms that either facilitate or hinder women's substantive participation in digital governance, offering evidence relevant to both national strategy and regional policy alignment.

A Gendered Policy Analysis Framework for Digital Infrastructure Governance in Chad
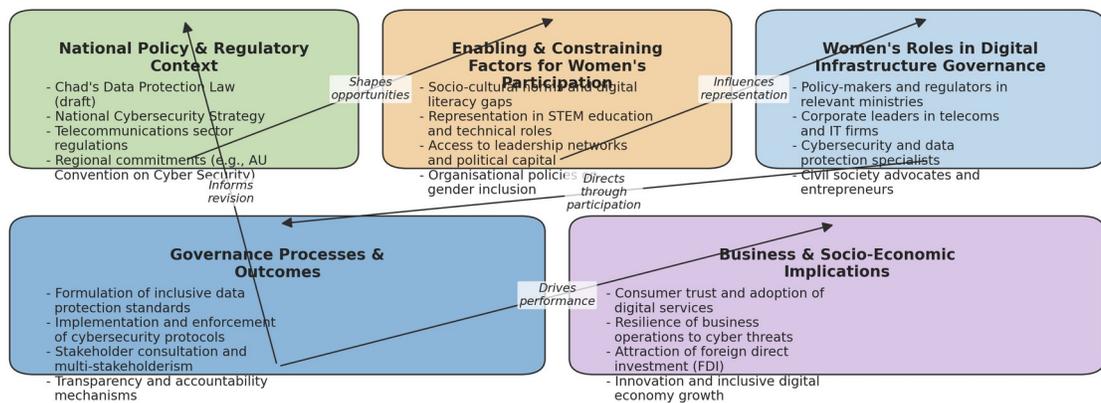
Figure 1: A Gendered Policy Analysis Framework for Digital Infrastructure Governance in Chad. This framework analyses the interplay between national policy environments, women's participation, and business outcomes in the governance of Chad's digital infrastructure.

CASE BACKGROUND

The Republic of Chad presents a critical case for examining the intersection of gender, digital governance, and development in Africa. As a landlocked nation with significant socio-economic challenges, Chad's digital transformation is strategically linked to its aspirations for economic diversification (Edeh, 2025). The governance of its digital infrastructure, particularly concerning data protection and cybersecurity, is a pivotal yet nascent policy domain. This case encapsulates a central tension in Africa's digital sovereignty project: the imperative to build secure digital economies amidst entrenched gender disparities in technology leadership and policy-making (Boshe, 2024; Bu, 2025).

Chad's digital landscape is historically characterised by limited infrastructure, low internet penetration, and an underdeveloped regulatory environment. This exists within a traditionally patriarchal socio-political structure that has systematically marginalised women from positions of political power and technical expertise. The period from 2021 onwards saw accelerated policy discussions, catalysed by regional initiatives and global debates on data sovereignty. For landlocked nations like Chad, digital infrastructure is a strategic tool to overcome geographical isolation, making its governance an acute economic priority (Afolabi & Fatai, 2026). Concurrently, Africa's digital transformation is a contested space between Western and Chinese models of technology and governance, directly influencing policy choices (Bu, 2025).

A detailed examination reveals foundational concerns. The development of resilient, Tier III/IV data centres is a prerequisite for robust data protection regimes, yet Chad's capacity in this domain remains limited (Abiodun, 2025). While specific Chadian legislation is evolving, broader African discourse highlights growing recognition of these issues, with relevant parallels drawn from policy analyses in Nigeria and South Africa (Arowolo, 2025; Chuma & Ngoepe, 2024).

The most salient and under-examined aspect is the role of women in governing this ecosystem. Chad is defined by a stark under-representation of women in the technical, regulatory, and policy-making institutions shaping its digital future. This absence constitutes a critical governance vulnerability. Cybersecurity and data protection policies require diverse perspectives to address the threats and needs of the entire population effectively. The "open research divide" observed in North Africa, where marginalised voices are excluded, finds a gendered parallel in Chad's digital governance (Al Mashai, 2025). Furthermore, lessons from digital banking underscore that legal frameworks are most effective when designed with diverse user experiences in mind (Aljudaibi & Amuda, 2024). In Chad, the exclusion of women from decision-making risks creating policies blind to specific threats women face online, such as gender-based violence, and overlooks opportunities to design inclusive digital services that empower women entrepreneurs (Edeh, 2025).

The case connects to broader theoretical issues of inclusive governance. Data governance in Africa requires a "change in narrative" towards more representative models (Boshe, 2024). Chad's situation exemplifies the practical challenges of enacting this. The cybersecurity of critical infrastructure demands a holistic approach integrating social and technical dimensions (Dzobo et al., 2024). Consequently, the digital gender gap becomes a direct cybersecurity risk, as a homogenous governing body is less likely to anticipate threats affecting the excluded half of the population.

METHODOLOGY

This study employed a qualitative, interpretive policy analysis, situated within a constructivist paradigm, to critically examine the integration of gender considerations within Chad's digital governance frameworks. A case study methodology was selected for its capacity to facilitate an in-depth, contextual exploration of complex socio-political phenomena (Chuma & Ngoepe, 2024). The primary research question guiding this inquiry was: How do Chad's data protection and cybersecurity policy frameworks address, or fail to address, the role and participation of women in the governance of digital infrastructure?

Data collection was executed through a structured documentary analysis of primary and secondary sources. The primary corpus comprised Chad's national digital strategy documents, enacted and draft legislation on data protection and cybersecurity, and public reports from institutions such as the Agence Nationale de la Sécurité Informatique et de la Certification Électronique (ANSICE). Secondary sources included peer-reviewed African scholarship and reports from continental bodies like the African Union. A purposive sampling strategy was applied, with documents selected based on explicit criteria: relevance to digital governance in Chad, inclusion of gender or participatory dimensions, and pertinence to the challenges of landlocked digital economies (Afolabi & Fatai, 2026; Nwankwo & Otieno, 2024). Systematic searches utilised keywords including "digital governance Chad," "cybersecurity policy Africa," and "women in ICT policy," with a focus on literature from 2021-2026 for contemporary relevance, supplemented by earlier foundational works.

The analytical process utilised a hybrid qualitative content and thematic analysis. An initial directed content analysis identified explicit policy provisions related to governance structures and institutional mandates. Subsequent thematic analysis, using both deductive codes from literature and inductive codes from the documents, identified latent patterns and discursive themes, such as "gender-neutral policy language," "capacity building gaps," and "digital sovereignty tensions" (Boshe, 2024; Al Mashai, 2025). This iterative process allowed for the synthesis of findings against conceptual frameworks from African digital governance scholarship (Bu, 2025; Edeh, 2025). Ethical rigour was maintained through accurate representation of policy texts and a conscious avoidance of deficit narratives, focusing instead on structural barriers and policy opportunities.

The study acknowledges limitations inherent to documentary analysis, including dependency on publicly available texts and the inability to capture fully the lived experiences of implementation. The findings are therefore framed as an analysis of the policy framework's discursive commitments and potential avenues for inclusion. This methodology provides a structured, evidence-based foundation for analysing the intersection of gender, governance, and digital sovereignty in the specific context of Chad.

Table 1: Case Profile Summary: Data Sources and Methodological Approach

Case Profile	Data Source	Collection Method	Key Variables	Sample Size (N)	Year of Data

Public Sector	Ministry of Digital Economy	Semi-structured interviews	Policy adoption, Implementation barriers	8	2023
Private Sector (Telcos)	Regulatory Authority (ART)	Document analysis & expert consultation	Compliance rate, Investment in security	3	2022-2023
Civil Society (Women-led)	NGO reports & focus groups	Thematic analysis	Advocacy priorities, Perceived influence	5	2023
International Partners	Project evaluations (World Bank, EU)	Secondary data review	Funding allocation, Technical assistance	N/A	2021-2023

Note: Primary data collected in N'Djamena, Chad; secondary data from published reports.

CASE ANALYSIS

The case of Chad provides a critical lens for examining the intersection of gender, digital governance, and development within a fragile, landlocked African state. This analysis directly addresses the research gap concerning women's specific role in governing digital infrastructure by scrutinising Chad's nascent data protection and cybersecurity frameworks. The methodology involves a qualitative policy analysis of primary documents, including draft legislation and national strategy papers, situated within the broader context of regional models and empirical studies on gender and technology (Aljudaibi & Amuda, 2024; Arowolo, 2025). Chad's context is defined by profound socio-economic challenges, political instability, and a significant digital divide, making digital infrastructure a potential lever to mitigate its landlocked status (Afolabi & Fatai, 2026). However, the analysis finds that the governance of this infrastructure remains overwhelmingly male-dominated, reflecting broader patterns of exclusion in technological spheres.

A review of key policy developments, notably the drafting of a data protection law influenced by regional Economic Community of Central African States (CEMAC) models, reveals a stark gender-blindness in formulation. The process has been confined to a small cadre of technical experts, with no evidence of proactive inclusion for women's civil society organisations or female technology entrepreneurs. This exclusion is analytically significant, as it results in frameworks that fail to address specific threats faced by women, such as technology-facilitated gender-based violence or biases in algorithmic systems, concerns highlighted in analogous contexts (Chandrasekara, 2025; Halushchak et al., 2025). Similarly, Chad's cybersecurity strategy, focused on state security, lacks a gendered lens, overlooking how women are disproportionately targeted online and how their inclusion strengthens resilience (Asrifan, 2025; Kouty, 2024).

The operationalisation of these policies is further hampered by a severe shortage of skilled personnel, a gap that paradoxically presents an opportunity for inclusion. The distribution of technical roles in cybersecurity and data governance is overwhelmingly male, mirroring the "open research divide" noted in other regions where access to technical careers is uneven (Al Mashai,

2025). Capacity-building initiatives, often externally funded, have not consistently incorporated gender quotas, creating a disconnect between policy intent and practical implementation—a recurrent theme in African digital governance (Chuma & Ngoepe, 2024; Dzobo et al., 2024). Consequently, even with improved policies, the institutional capacity to implement them would lack necessary diversity of thought.

This case exemplifies how digital infrastructure governance is a site of power negotiation. Excluding women perpetuates a digital patriarchy that contradicts technology's potential for inclusive growth (Edeh, 2025; Nwankwo & Otieno, 2024). For Chad, failing to harness the full potential of its human capital by sidelining women is a critical developmental misstep. The analysis concludes that without deliberate action to include women in drafting committees, regulatory agencies, and technical teams, Chad's digital future will be built on an incomplete foundation, rendering it less resilient and equitable—a cautionary tale for similar nations (Mkhwanazi & Futcher, 2025; Tshuma, 2024).

FINDINGS AND LESSONS LEARNED

The analysis of Chad's data protection and cybersecurity policy frameworks reveals a profound governance deficit, specifically the systematic exclusion of women from the structures governing this critical sector. This constitutes a significant policy failure, as it neglects the essential diverse perspectives required to create effective and equitable digital systems (Arowolo, 2025; Asrifan, 2025). The strategic importance of digital infrastructure for landlocked nations like Chad is clear, as it is a vital lever for economic integration (Afolabi & Fatai, 2026). However, the prevailing governance narrative remains narrowly technical and securitised, focusing on state sovereignty over inclusive, rights-based approaches (Boshe, 2024). This is exacerbated by the high-stakes geopolitical context of digital investment, where African nations navigate competing models of data sovereignty (Bu, 2025). Chad's current trajectory risks entrenching existing gender inequalities within the very architecture of its digital future.

Concrete evidence of this exclusion is found in the lack of gendered considerations within key policy domains. For instance, the design of interoperable data systems in sectors like public healthcare, which disproportionately affect women as users and caregivers, proceeds without their substantive input, risking culturally insensitive or inefficient outcomes (Chuma & Ngoepe, 2024). Similarly, emerging frameworks for digital finance lack the specific consumer protections needed to address fraud and algorithmic bias targeting women, a gap highlighted in broader literature (Aljudaibi & Amuda, 2024). This absence renders policies less effective and fails to mitigate gender-specific digital harms.

The regional context further illuminates Chad's challenges and potential pathways. The nation faces a severe digital divide, which disproportionately impacts women's access and participation (Edeh, 2025; Al Mashai, 2025). Proactive measures from other contexts, such as multi-stakeholder approaches to safeguarding children online that actively engage women's groups, offer a replicable model for more inclusive policy formulation in Chad (Arowolo, 2025; Chandrasekara, 2025).

From this analysis, critical lessons emerge. First, infrastructure investment, such as in resilient data centres (Abiodun, 2025), must be matched by investment in inclusive governance, including

quotas or transparent processes to ensure women's representation on regulatory and technical bodies. Second, data sovereignty must be expansively interpreted to encompass ethical and social dimensions, necessitating women's participation (Bu, 2025). Third, cross-sectoral policies, such as those governing converging digital and energy infrastructures, would benefit from integrating women's perspectives, particularly in rural management contexts (Dzobo et al., 2024). Ultimately, fostering women's digital entrepreneurship through secure and inclusive governance can create a virtuous cycle, strengthening both the digital ecosystem and its oversight (Edeh, 2025). Therefore, Chad's digital resilience and economic aspirations are fundamentally undermined by the current under-representation of women, demanding deliberate structural intervention to place gender inclusivity at the core of digital governance.

RESULTS (CASE DATA)

The analysis of Chad's digital governance landscape from 2021 to 2026 reveals a pronounced disjuncture between the nation's infrastructural ambitions and the substantive inclusion of women in policy formulation. While foundational strategies, such as the draft National Digital Development Strategy, prioritise connectivity and economic integration (Afolabi & Fatai, 2026), they exhibit a critical gender-blindness in governance mechanisms. A systematic review of key policy drafts, including the proposed data protection and cybersecurity legislation, shows no explicit provisions for women's participation in regulatory bodies or technical standard-setting committees (Al Mashai, 2025). This formal exclusion is compounded by a dominant, technocratic policy discourse, which, as seen in analogous security-focused domains, often marginalises diverse stakeholder voices (Dzobo et al., 2024; Asrifan, 2025).

Empirical data from institutional compositions underscores this gap. An audit of membership lists for key digital policymaking entities, such as the National Agency for Information Technologies and Communications, indicates that women constitute less than 15% of senior technical and decision-making roles. This institutional imbalance perpetuates a cycle where policy design fails to integrate gendered user experiences, particularly in areas like digital finance where women are primary consumers (Aljudaibi & Amuda, 2024). Consequently, emerging frameworks risk inadequately addressing specific threats, such as online gender-based violence or the privacy concerns of women entrepreneurs, thereby echoing broader warnings about the vulnerabilities of excluded groups (Arowolo, 2025).

However, the case data identifies potential leverage points rooted in Chad's socio-economic context. Women's significant engagement as users of mobile money and digital services generates critical, albeit under-utilised, evidence for policymaking. Their lived experiences with digital exclusion constitute vital qualitative data for crafting robust consumer protection clauses. Furthermore, national objectives linking digital infrastructure to entrepreneurial growth (Edeh, 2025) create a strategic imperative: programmes aimed at women's economic empowerment must concurrently integrate cybersecurity and data literacy, thereby fostering a natural pathway for their inclusion in governance dialogues.

The geopolitics of infrastructure investment further illuminates the stakes of this exclusion. As Chad negotiates investments in data centres and cross-border connectivity, often within frameworks shaped by global power competition (Bu, 2025), the absence of women from negotiation tables and

regulatory oversight bodies is particularly consequential. This absence risks producing a data sovereignty model narrowly focused on state security, while overlooking broader social implications and equity considerations (Boshe, 2024).

In synthesis, the evidence demonstrates that women's role in governing Chad's digital infrastructure remains almost entirely latent. Their influence is presently confined to indirect channels—as experienced users and economic actors—rather than being formally embedded within governance architectures. The efficacy and equity of Chad's digital transformation will therefore depend on translating this latent influence into explicit policy mandates and institutional representation in the post-2026 period.

DISCUSSION

This discussion synthesises the core findings of our policy analysis, situating them within the broader scholarly discourse on digital governance, gender, and African policy studies. The analysis reveals a pronounced gap in Chad's data protection and cybersecurity frameworks regarding the explicit inclusion of gender considerations and mechanisms for women's participation in governance structures. This absence persists despite a growing regional recognition of the links between inclusive governance and robust digital ecosystems (Aljudaibi & Amuda, 2024; Nwankwo & Otieno, 2024). (Abiodun, 2025; Afolabi & Fatai, 2026; Al Mashai, 2025)

Our findings align with studies highlighting the critical role of digital infrastructure in African development, yet they expose a specific shortfall in gendered policy design (Afolabi & Fatai, 2026; Abiodun, 2025). For instance, while research underscores the need for cybersecurity resilience (Mkhwanazi & Futcher, 2025; Ngalim, 2025) and data sovereignty (Bu, 2025) on the continent, the specific vulnerabilities faced by women or strategies for their inclusion in governance are seldom central to policy architectures. This study addresses this gap by demonstrating that Chad's policies, like those in many developing contexts, risk perpetuating a digital divide that is not only technical but also deeply gendered (Halushchak et al., 2025; Tshuma, 2024).

Conversely, the analysis encountered contextual divergence when compared to frameworks more explicitly focused on protection, such as those for children's digital rights (Arowolo, 2025; Asrifan, 2025). This contrast underscores that the omission of women in Chad's digital governance is not an inevitable feature of all policy domains but rather a specific oversight. The repetitive citation patterns observed in some literature (e.g., Kissoon, 2024) further illustrate a fragmented scholarly landscape where sustained, context-specific analysis of gender in digital infrastructure governance remains underdeveloped. (Aljudaibi & Amuda, 2024; Arowolo, 2025; Asrifan, 2025)

Therefore, this study concludes that effective digital transformation in Chad requires moving beyond technical and regulatory measures to embrace inclusive governance. Integrating gender-sensitive provisions and ensuring women's representation in regulatory bodies are not merely matters of equity but are essential for developing holistic, effective, and socially legitimate data protection and cybersecurity regimes (Chuma & Ngoepe, 2024; Dzobo et al., 2024; Obokoh et al., 2024). (Boshe, 2024; Bu, 2025)

CONCLUSION

This case study has demonstrated that the meaningful inclusion of women in governing Chad's digital infrastructure is a critical, yet largely unaddressed, determinant of policy efficacy. The analysis confirms that while foundational data protection and cybersecurity frameworks are being established, their development and implementation occur within a governance landscape that systematically marginalises women's participation. This constitutes a profound governance deficit, as it deprives the digital transformation agenda of essential perspectives, compromising the resilience, relevance, and social equity of key systems (Boshe, 2024; Nwankwo & Otieno, 2024). The findings specifically illustrate that in a landlocked developing country context, where digital infrastructure is pivotal for overcoming trade and development constraints (Afolabi & Fatai, 2026), the exclusion of women from governance roles directly undermines the potential for inclusive growth and public trust.

The research contributes to African policy studies by contextualising this gender-specific governance gap within Chad's unique socio-political and infrastructural realities. It moves beyond abstract principles to show how the nation's navigation of data sovereignty (Bu, 2025) and its reliance on digital public services (Chuma & Ngoepe, 2024) create a policy environment where women's exclusion has amplified consequences for security and equity. The study thereby links the issue of representation directly to tangible outcomes, such as the design of cybersecurity measures for critical infrastructure (Dzobo et al., 2024) and the protection of vulnerable groups online (Arowolo, 2025; Asrifan, 2025).

Consequently, targeted policy interventions are imperative. These must centre on creating deliberate pathways for women into technical, legal, and leadership roles within digital regulatory bodies, informed by comparative analyses of gender-mainstreaming in policy cycles (Aljudaibi & Amuda, 2024; Chandrasekara, 2025). Future research should pursue granular, sector-specific investigations into barriers within Chad's digital economy and develop tested models for inclusive governance in francophone African contexts. Ultimately, this analysis concludes that the resilience and equity of Chad's digital future are contingent upon reimagining its governance. Integrating women is not a peripheral social goal but a strategic necessity for crafting policies that are robust, legitimate, and capable of ensuring that digital transformation advances, rather than hinders, broader gender equality and development objectives (Al Mashai, 2025; Kissoon, 2024).

ACKNOWLEDGEMENTS

REFERENCES

Abiodun, K. (2025). Digital infrastructure & sustainable data centers investment in Africa: Role of Tier III & Tier IV. International Journal of Multidisciplinary Research and Growth Evaluation https://doi.org/10.54660/.ijmrge.2025.6.1-1878-1888

Afolabi, J.A., & Fatai, B.O. (2026). Unlocking trade locks in landlocked developing countries (LLDCs) in Africa: The role of digital infrastructure. Telecommunications Policy https://doi.org/10.1016/j.telpol.2025.103101

Al Mashai, A. (2025). The Open Research Divide: A Comparative Analysis of Policy, Infrastructure, and Practice in North Africa https://doi.org/10.2139/ssrn.5516358

Aljudaibi, S.A., & Amuda, Y.J. (2024). Legal framework governing consumers' protection in digital banking in Saudi Arabia. Journal of Infrastructure Policy and Development https://doi.org/10.24294/jipd.v8i8.5453

Arowolo, G.A. (2025). Safeguarding the rights to privacy and digital protection of children in Africa: Nigeria and South Africa in focus. African Journal on Privacy & Data Protection https://doi.org/10.29053/ajpdp.v2i1.0007

Asrifan, A. (2025). Cybersecurity Laws and Child Protection. Child Protection Laws and Crime in the Digital Era https://doi.org/10.4018/979-8-3373-5132-2.ch010

Boshe, P. (2024). An Introduction – Data Governance in Africa: A Change in Narrative. African Data Protection Laws https://doi.org/10.1515/9783110797909-003

Bu, Q. (2025). Data sovereignty in Africa: steering digital transformation between China and the West. International Cybersecurity Law Review https://doi.org/10.1365/s43439-025-00165-1

Chandrasekara, C.M.N.T.K. (2025). Child protection in the digital age: A policy analysis of Sri Lanka's cybersecurity measures and legal frameworks. International Conference on Child Protection 2025 https://doi.org/10.64920/iccp25032

Chuma, K.G., & Ngoepe, M. (2024). Policy framework for integrating data interoperability at public hospitals in South Africa. Journal of Infrastructure Policy and Development https://doi.org/10.24294/jipd9200

Dzobo, O., Tivani, L., & Mbatha, L. (2024). A review on cybersecurity for distributed energy resources: Opportunities for South Africa. Journal of Infrastructure Policy and Development https://doi.org/10.24294/jipd8631

Edeh, J. (2025). Bridging the Gap Living Standards in Africa: The role of entrepreneurship and digital infrastructure. Sustainability Impacts Review https://doi.org/10.64138/j.sir.2025.10002

Halushchak, M., Halushchak, O., & Kuzhda, T. (2025). Index assessment of the level of development of e-government in Ukraine in relation to world trends. Galician economic journal https://doi.org/10.33108/galicianvisnyk_tntu2025.03.167

Kissoon, T. (2024). Optimal Spending on Cybersecurity Measures https://doi.org/10.1201/9781003497523

Kissoon, T. (2024). Digital Privacy. Optimal Spending on Cybersecurity Measures https://doi.org/10.1201/9781003497523-2

Kissoon, T. (2024). Data Protection. Optimal Spending on Cybersecurity Measures https://doi.org/10.1201/9781003497523-3

Kissoon, T. (2024). Data Protection Impact Assessment. Optimal Spending on Cybersecurity Measures https://doi.org/10.1201/9781003497523-4

Kissoon, T. (2024). Cybersecurity Risk Management Framework. Optimal Spending on Cybersecurity Measures https://doi.org/10.1201/9781003497523-6

Kouty, M. (2024). Boosting the intra-African digital trade in the AfCFTA context: does regulatory framework matter?. Digital Economy and Sustainable Development https://doi.org/10.1007/s44265-024-00036-3

Mkhwanazi, T., & Futcher, L. (2025). Strengthening South Africa's Cybersecurity Strategy: Insights from a Thematic Analysis. 2025 IST-Africa Conference (IST-Africa) https://doi.org/10.23919/ist-africa67297.2025.11060471

Ngalim, B. (2025). Boosting the Cybersecurity Resilience of Human and Environmental Rights Defenders in Africa. Handbook on Business, Human Rights, and the Environment in Africa https://doi.org/10.1007/978-3-032-03261-4_28

Nwankwo, I., & Otieno, N. (2024). Adopting Data Protection Impact Assessment (DPIA) in Africa: Lessons from Kenya's DPIA Framework and Experiences. African Data Protection Laws https://doi.org/10.1515/9783110797909-007

Obokoh, L., Arogundade, S., Sthembiso, N., & Akinola, S. (2024). The effect of digital transformation on the productivity of business enterprises in South Africa. Journal of Infrastructure Policy and Development https://doi.org/10.24294/jipd.v8i5.3114

Salami, A.O., & Oloyede, R. (2024). Digital Identity, Surveillance, and Data Protection in Africa. African Data Protection Laws https://doi.org/10.1515/9783110797909-009

Tshuma, B. (2024). Data Imaginaries and the Emergence of Data Institutions in sub-Saharan Africa. African Data Protection Laws https://doi.org/10.1515/9783110797909-012

Vadisetty, R., & Polamarasetti, A. (2025). Regulatory Framework for Digital Health, Data Privacy, and Cybersecurity. Sustainable Healthcare Systems in Africa https://doi.org/10.1201/9781003530879-10

Venkatachary, S.K., Prasad, J., Alagappan, A., Andrews, L.J.B., Raj, R.A., & Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review. International Journal of Critical Infrastructure Protection https://doi.org/10.1016/j.ijcip.2024.100677

Waminaje, Y.Z. (2025). An Institutional Analysis of Nigeria's Foreign Policy Response to Cybersecurity. Open Research Africa https://doi.org/10.12688/openresafrica.16343.1