Digitalization and Financial Data Governance in Africa: Challenges and Opportunities

Bitange Ndemo
and
Ben Mkalama

Working Paper DG-005

AFRICAN ECONOMIC RESEARCH CONSORTIUM
CONSORTIUM POUR LA RECHERCHE ÉCONOMIQUE EN AFRIQUE

Bringing Rigour and Evidence to Economic Policy Making in Africa

Digitalization and Financial Data Governance in Africa: Challenges and Opportunities

By

Bitange Ndemo

and

Ben Mkalama

AERC Working Paper DG-005
African Economic Research Consortium, Nairobi
February 2023

THIS RESEARCH STUDY was supported by a grant from the African Economic Research Consortium. The findings, opinions and recommendations are those of the author, however, and do not necessarily reflect the views of the Consortium, its individual members or the AERC Secretariat.

Published by: The African Economic Research Consortium
P.O. Box 62882 - City Square
Nairobi 00200, Kenya

Contents

List of tables
List of figures
Abstract

1. Introduction 1

2. The Current State of Affairs 5

3. Conclusions and Implications 17

References 18

List of tables

1. Missing clauses—digital provisions in African trade agreements 11

List of figures

1. Data production and data protection 6
2. Conceptual framework 7
3. Data protection and privacy legislation in Africa 8
4. Status of digital protection-related legislation across African countries 9

Abstract

Digitalization is quickly emerging as an avenue for future economic development. As a result of this, financial technology companies (FinTechs) have taken to digitalization both to understand their customers and to use data to design more productive and convenient products. Subsequently, they are credited with making financial resources increasingly available and affordable. In Africa, millions of people use a vast array of proliferating mobile platforms as transactional interfaces. Although these innovations have improved the ease of financial transactions, they are not without challenges. Due to the dynamic nature of these processes, ubiquitous challenges affecting collection, processing, quality and security of collected data continually emerge. These challenges create opportunities for financial data governance. In this paper, we explore digitalization and financial governance in Africa. We identify the current state of knowledge and explicate how this understanding has been applied on the continent. Finally, we specify existing knowledge gaps in areas that could form the basis of a future research agenda for practitioners and policy makers.

Keywords: *Digitalization; Data governance; Digital innovation; Fintech; Africa;*

1. Introduction

The influence of digitalization for future economic development continues to fascinate scholars and practitioners. Digitalization often initially involves sizeable costs, and its benefits become apparent after the accompanying data is transferred to an environment that minimizes operational expenses. To provide distinction, *digitization* refers to the act of converting information from an analogue to a digital format, and *digitalization* refers to the subsequent process of leveraging on the digital content to attain an enhanced user experience (Rijswijk et al., 2020). Digitalization is considered as the process of integrating digital technologies into everyday life. Among other advantages, digitalization allows users to spend less on computer hardware and software, thereby allowing team members to focus on other tasks. Additionally, digitalization aids data collection in that materials are optimized for analysis and investigation, thus allowing firms to prosper. Similarly, with digitalization, data and resources can be consolidated into a set of tools that offer a single perspective on their customer journey, operations and other business opportunities. As a result, data-driven consumer insights can facilitate a customer-centric corporate strategy, affording a better overall consumer experience in an era that rewards limitless choices, low prices and quick delivery. Businesses can, therefore, become more agile with digitalization, increasing their speed to market while embracing innovative approaches (Backbase, 2021; IFC, 2017).

Digitalization increases efficiency and raises productivity through greater automation of manual activities, integration of data across the company and empowering of team members with a collaborative digital culture that offers tools that are adapted to their context. Digitalization in the finance sphere provides convenience, efficiency and security to clients looking to access their funds; additionally, digitalization discourages corruption, financing of illicit activities and tax evasion (Jafri, 2021), while promoting greater inclusion which enables access to formal financial services for those lacking other avenues of access (Jafri, 2021; Shipalana, 2019). Put simply, a financial technology company (FinTech) innovations encourage financial inclusion and bolster economic development.

The spread of digitalization

New technologies and their attendant effects on digitalization are fuelling the emerging Fourth Industrial Revolution (4IR). Technologies such as big data analytics, Artificial Intelligence (AI), blockchain, Internet of Things (IoT) and robotics are being

used, independently and jointly, to create new data-driven business models and to generate better opportunities for enterprises to expand rapidly. Technology companies have taken to digitalization, both to understand the customer (through data) and to use this data to design new products, and to improve productivity and convenience. As part of its 2030 Agenda, the United Nations General Assembly approved the 17 Sustainable Development Goals (SDGs) as a blueprint for sustainable development in the world. Numerous experts have opined that realizing the SDGs requires the effective exploitation of data across numerous sectors (Macmillan, 2020).

Technology firms that were not previously in the financial services sector are carving out a niche for themselves (Frost et al., 2019); the number of FinTechs has, therefore, multiplied rapidly, rendering financial resources increasingly available and affordable. Increasingly active FinTechs have, however, spawned additional challenges, varying across different sectors and jurisdictions, such as e-commerce platforms registering far-reaching cross-border impacts such as tax liability for local firms across entire economies, and the emergence of regional payment platforms necessitating transnational and interdisciplinary regulatory discourses. There are also governance issues regarding cyber-resilience and data management concerns; what is more, digital currencies, especially amid economic globalization, continue to reconstitute financial and monetary policies, with potentially significant economic impact.

Mobile money platforms were built on the back of Global Systems for Mobile (GSM) connectivity and have grown phenomenally; they are now used by over one billion people around the world (Enberg, 2019). Over the past decade, mobile money services have rapidly expanded access to financial services in Africa (Kirui, 2020). The rate of growth of the FinTech industry in Africa has been influenced, too, by existing mobile network operators and their relationships with central banks (IFC, 2017). Similarly, in Africa, the payments industry leads the FinTech sector where, historically, more than 90% of the economy has been cash-based (Yermack, 2018). Indeed, across the region, some countries have become global leaders in mobile money transactions. For instance, while the rest of the world hovers at 5%, as a proportion of GDP, the average for such transactions in Sub-Saharan Africa is closer to 25% (IFC, 2017). Indeed, by 2017, mobile money transactions in Kenya—a country that pioneered the use of mobile for financial transactions—executed through the MPesa platform accounted for 44% of national GDP (Rolfe, 2019). Similarly, Zimbabwe's EcoCash platform transacted more than US$ 23 billion in 2017, or 54% of national GDP (Sengere, 2017). These profound rates of use occurred despite remittances in Sub-Saharan Africa registering just under 10% of the global value, and yet had the highest transaction costs in the world, thereby creating opportunities for exploitation (Yermack, 2018).

The growth of mobile money in Kenya and Zimbabwe was spurred by an enabling regulatory environment, whereby this innovation was led by the dynamic private sector technological communication players rather than the financial system players (Chitimira and Torerai, 2021; Muthiora, 2015). This situation was due to an appreciation that mobile money combined both a telecommunication service and a

financial service. Some of the factors that contributed to financial exclusion included "a trust deficit in banking institutions, their distance from financial institutions and their failure to satisfy documentary requirements such as a proof of identity and a proof of residence" (Chitimira and Torerai, 2021:10). As a result of mobile banking, relaxed requirements to open a mobile money account enabled the poor and unbanked persons to participate in the mainstream financial system, thereby leading to flourishing of this sector. Similarly, the mobile money agents' network and the prepaid model played a critical role in the rapid growth and assurance of security for mobile money in Kenya and Zimbabwe (Chitimira and Torerai, 2021; Muthiora, 2015). Yermack (2018) opined that mobile money flourished in markets with weak institutional structures as a result of the following characteristics: low profit margins, asset being light in nature, scalable designs, innovativeness and compliance friendly.

Digitalization has strong implications for financial access and inclusion in the Global South (Jafri, 2021), and FinTechs are poised to hasten these processes (Lewis et al., 2017). Discourses that favour the dematerialization of money as "a technological fix to broader problems of poverty and financial exclusion" have seen enhanced digitalization of the financial sector even as it is unclear whether those at the periphery of the digital money ecosystem genuinely benefit from the influence of digitalized operations (Muralidhar et al., 2019). Lack of identification documents had previously been viewed as an impediment to financial access, but this challenge has been addressed recently by providing individuals with a digital identity. Digital identities have become increasingly prominent, and a digital welfare state is developing, depicted by a gradual uptake of digital data and technologies in welfare schemes, partnerships, administrative processes and the provision of services (Jafri, 2021). Kenya, for example, now transacts social service programmes through electronic means such as mobile wallets (Republic of Kenya, 2017), notwithstanding hindrances to fulfilment and success stemming from challenges such as literacy (including IT literacy), the socio-emotional perspective of marginalized individuals and the complexity of information and service requirements that users confront (Malladi et al., 2021; Mervyn et al., 2014; Shipalana, 2019).

Innovation, prevalent poverty levels, financial sector stability, financial literacy and existing regulatory frameworks that vary between countries each affect the financial inclusion ecosystem (Ozili, 2021). Malladi et al. (2021) posited that individuals finding themselves within the financial inclusion ecosystem due to digitalization ended up being marginalized and, owing to socio-economic circumstances, incapable of sustaining themselves within the framework. Malladi et al. (2021) further observed that whereas some consumers might be savvy with technology—relishing apt gadgets—most users might not be able to afford even basic phones, meaning they would likely struggle to understand and utilize technology efficiently, thus leading to significant variance between users in terms of product and service uptake. Finally, Malladi et al. (2021) opined that a lack of financial knowledge and an understanding of financial cybercrimes led to a general mistrust among the marginalized, thereby diminishing digital penetration.

Digital financial inclusion raises key regulatory issues regarding agency, money laundering, financing of illicit activities, regulation of e-money, consumer protection, payment system regulation and competition. The increasing influence of technology firms underscores the need for global monitoring and a regulatory framework capable of accommodating the competing priorities of different countries and stakeholders while supporting inter-jurisdictional coordination and minimizing the risk of regulatory fragmentation. Global action has, however, thus far lacked coordination, emphasizing the need for urgent and concerted remedial action (Lopez, 2020). To help meet this need, this issue paper analyses the impact of digitalization and data governance in the financial sector and focusses on the challenges and emerging opportunities for private and public organizations across Africa.

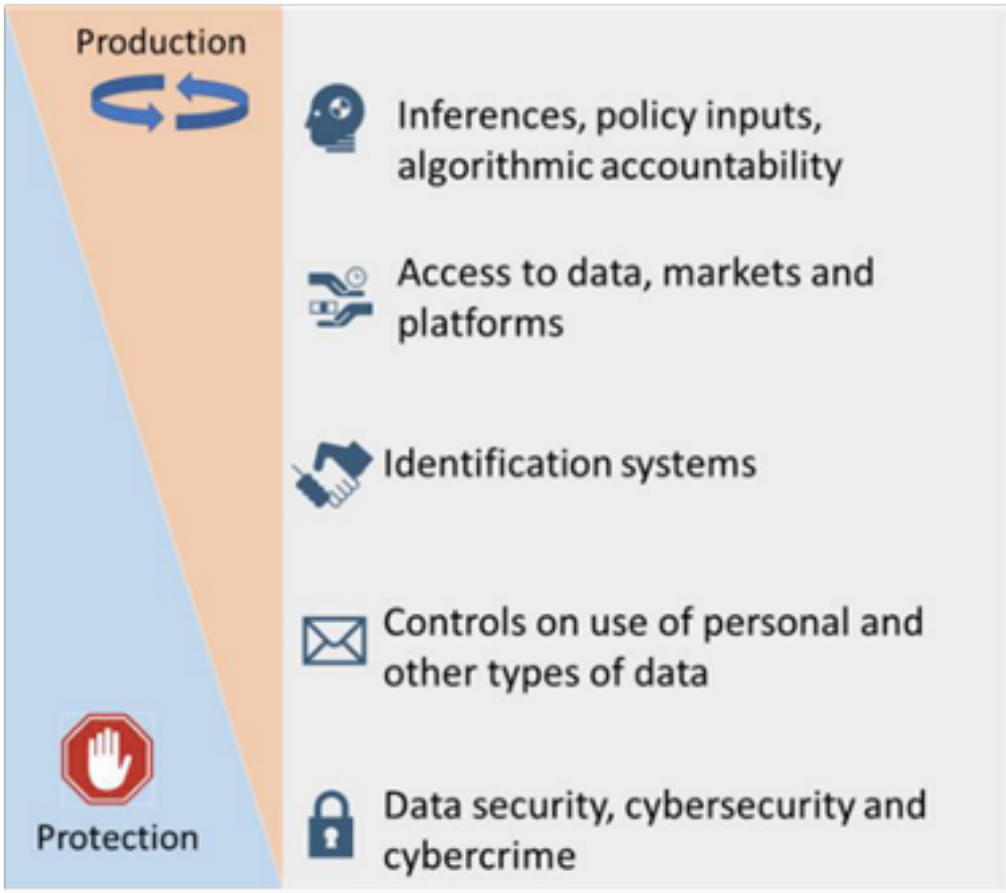
2. The current state of affairs

Emerging concerns

Digitalization has transformed global financial markets (IFC, 2017; Lehner and Simlinger, 2019), and the COVID-19 pandemic has accelerated this transition (UDESA, 2020). As finance has been democratized, credit has become at once more accessible, available and affordable. Several platforms, for example, now deploy Big data analytics and Artificial Intelligence (AI) to build customer credit scores that offer more convenient services such as digital loans. Digital transformation has also spurred fundamental changes in customer experience, affecting decisions and transactional processes across the global world of finance (Backbase, 2021; IFC, 2017).

Challenges remain, however, even with the greater inclusion delivered by emerging technology solutions. The digitalization has raised questions about data governance, as private entities have generated and deployed massive amounts of customer data without necessarily receiving consent or offering assurances of privacy (Davis, 2021). Indeed, there are numerous instances where consumers have balked at having their data used without their consent. Panian (2010) identified the goals of data governance as enabling secure data collection to complement business needs, managing data as an important competitive advantage, while optimizing costs of data storage. Macmillan (2020) argued that successful data governance means recognizing the economic and social utility of data while delivering public benefits across the economy and distribution that should be done securely and in accordance with widely observed norms of consumer protection and privacy. Figure 1 illustrates the tension between the need for data protection and production with respect to data governance issues.

Figure 1: Data production and data protection



Source: Macmillan (2020)

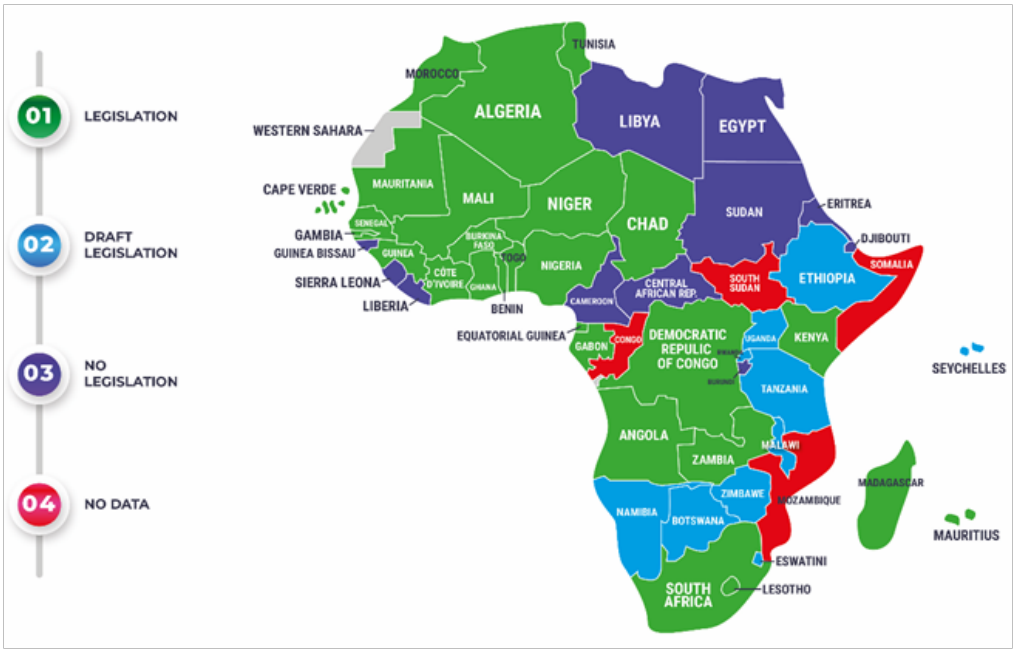
Ultimately, governance influences financial stability. We adopt the conceptual framework in Figure 2, and we argue that financial data governance requires a system of self and external regulation.

The need for regulation in FinTechs revolves around four principal pillars: compliance (such as preventing money laundering), consumer protection, tax collection and financial stability. There are interacting actions around these pillars, and scholarly work on the same is still fairly nascent.

Figure 2: Conceptual framework

It is estimated that more than 500 companies across Africa provide financial services enabled by technology (African Union Commission - AUC/Organization for Economic Cooperation and Development - OECD, 2021), and the total is even higher when accounting for firms in other sectors that also base their work in technology. Furthermore, the FinTech industry is highly dynamic and is replete with investments, acquisitions, buyouts and partnerships (Wójcik, 2021). Because massive amounts of data are now held by private corporations operating in jurisdictions other than those in which they are based, data governance has emerged a top priority especially in Sub-Saharan Africa (Devermont and Harris, 2021). In response, the European Union of the General Data Protection Regulations (GDPR) developed data-protection laws in 2016, and several African countries have produced similar legislation. Figure 3 demonstrates the status of such legislative enactments on the continent.

Figure 3: Data protection and privacy legislation in Africa



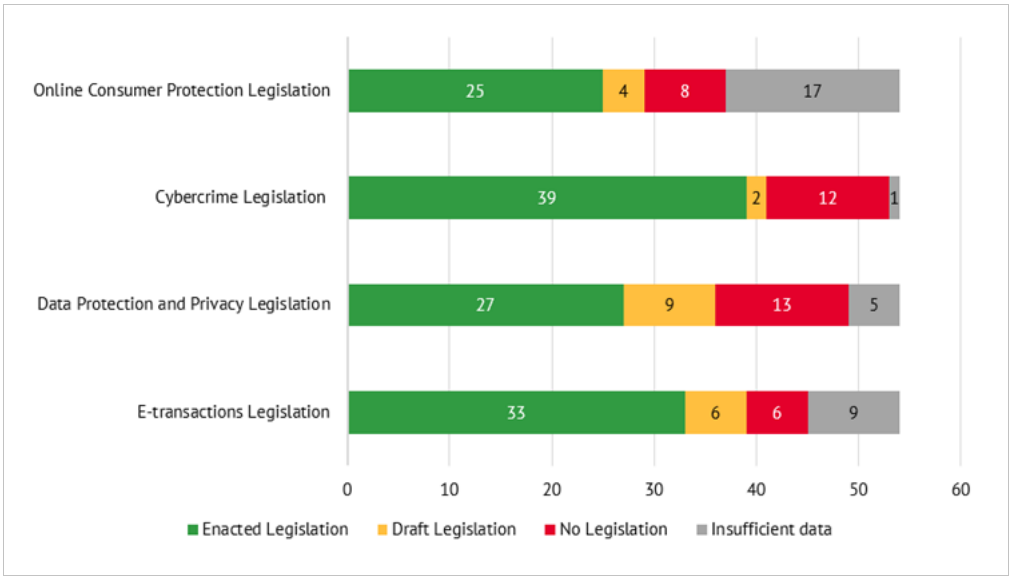
Source: Adapted from UNCTAD (2020)

Laws such as those referenced in Figure 3 address the risk of personal information leaking into the wrong hands while also attending to matters of privacy infringement, concerns about data monopoly, responsibility for data quality and service, and the limits of data governance for Big data implementation. Additionally, these laws aspire to protect personal information while safely accessing and linking open and non-sensitive data. At the same time, they offer proportionality in the use of data and autonomy for individuals and communities deploying data to achieve commercial benefits and efficiency in public services. Most countries, at present, refer to the principles of AI as developed by the OECD.

Yermack (2018) posited that regulation of FinTech companies in developing countries was undeveloped due to immature regional institutions and ever-evolving technology. Malladi et al. (2021) observed that while financial inclusion has broadened, access to credit was still a concern and has caused a spike in predatory lenders charging exorbitant rates of interest, typically due to insufficient penetration by government and credible formal schemes, thereby requiring more outreach to enhance would-be users' access to credit. Moreover, avenues for digital lending and online loans from credible financial institutions are still missing.

Despite clarity at the continent level, numerous studies have shown that not all countries have progressed towards operationalizing their data protection laws and governance mechanisms (Ademuyiwa and Adeniran, 2020; Deloitte, 2017). According to the United Nations Congress on Trade and Development - UNCTAD (2021), African countries are at different stages of legislating various aspects of safeguards on digital transactions and data use.

Figure 4: Status of digital protection-related legislation across African countries



Source: UNCTAD (2021)

As indicated by Figure 4, by 2021, only 25 of the 54 countries in Africa had fully enacted legislation on consumer protection. Similar numbers exist regarding cybercrime (39), privacy and data protection (27) and electronic transactions (33). These rates of enactment have significant implications for trade potential and subsequent financial transactions in the region.

Digitalization has heterogeneous impact across Africa

Digitalization is a multidimensional and rapidly evolving concept (IFC, 2017), one that has emerged as a practical and feasible approach to improving governance (World Bank, 2021). Information asymmetries have been reduced by increasing transparency and access to information, leading different organizations to move towards digitalization. On account of individual-level data, different organizations can offer advanced search outcomes, tailored products, service recommendations, useful ratings, timely traffic data and targeted advertisements (Devermont and Harris, 2021). Furthermore, as the World Bank (2021) has observed, digitalization can improve linkages between citizens and governments, a connection that is increasingly important as the public and private spheres have become increasing intertwined and reliant on digital technology amid the COVID-19 pandemic. Virtually every organization realizes that customer data is like gold and a major corporate asset, hence the need for careful protection and active management to preserve the integrity and realize the value of this data.

As many organizations have realized lately, notwithstanding its value, data can be a liability in the event of data breaches (Gregory, 2011; Gressin, 2018; Wang and

Johnson, 2018), especially in the financial sector where such episodes are a common occurrence. Wang and Johnson (2018) estimated that between 2005 and 2018, there were over 8,000 documented breaches affecting over 10.3 billion records. Of these cases, more than 2,300 breaches implicating 9.8 billion records affected e-commerce transactions in finance and insurance services. For example, in July 2020, a data breach was reported involving as many as 7.5 million banking users who had been exposed on a forum used by hackers to sell and swap ill-gotten data (Payments, 2020).

The African Cyber Immersion Centre - ICIC (2020) noted a marked increase in cyber-attacks transcending key sectors of the economy and found that these attacks were mostly coordinated across different countries. Cyber resilience, therefore, remains a critical component in the relationship between digitalization and economic development. The African Union (AU) Heads of States thus adopted and approved the AU Convention on Cybersecurity and Personal Data Protection at the 2014 Malabo Convention (African Union, 2014). The convention obliged member states to:

> establish in each state party, mechanisms capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage, and use; that by proposing a type of institutional basis, the convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of local communities and the interest of business; and take on board internationally recognized best practices (p.2).

Verification, vigilance and keen detection efforts are more important than ever in this rapidly changing environment. Without ratification and subsequent operationalization by the different states of the Malabo Convention, the good intentions will remain just that.

Africa is a large heterogeneous collection of countries with distinct societal objectives and institutional frameworks. There are significant intra-country disparities within the region and at the most basic levels of digitalization; higher-income countries, for example, enjoy superior connectivity (IFC, 2017). Yermack (2018) analyzed different patterns of legal systems in Africa and their influence on the adoption of technology and FinTech platforms, and deemed that common law countries (as compared to civil law countries) provided more infrastructure incentives that, in turn, encouraged robust growth for FinTech platforms. Ademuyiwa and Adeniran (2020) further established that most existing laws required substantial amendments to qualify them as appropriate to the dynamics of digitalization and highlighted emerging concerns regarding policies directed at competition and taxation in the digital space. Table 1 provides a summary of progress regarding different aspects of data governance in light of existing trade agreements and protocols.

Table 1: Missing clauses—digital provisions in African trade agreements

	Intellectual Property (IP) Protection	Data Protection	Cyber Security
	Legal rights that creators have over their works, inventions, technological developments, etc. Examples of IP protection include patents, trademarks, copyrights, and trade secrets.	The process of protecting individuals' personal information. Includes measures to secure data, data encryption, masking erasure, and backup	Protection against criminal use or manipulation of cyberspace, including breaches known as "cyberattacks"
The Cotonou Agreement (between the EU and the African, Caribbean, and Pacific Group of States) (2000)	Present but does not contain unique clauses governing IP. Relies on adherence to the Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the WTOs agreement regarding the Convention on Biological Diversity	Absent	Absent
EU–EAC Economic Partnership Agreement – EPA (2014)	Absent; contains a clause dictating that negotiations on IP are to be completed within 5 years of UK–Kenya EPA start date. However, subsequent negotiations have not resulted in an IP protection agreement	Absent	Absent
AfCFTA Agreement (2018)	Absent; to be included in Phase II of the AfCFTA Negotiations	Absent; to be included in Phase II	Absent; to be included in Phase II
UK–Kenya Economic Partnership Agreement - EPA (2020)	Present; contains brief language noting that the clause on IP is replicated from the EU-ACP EPA	Absent	Absent
US–Kenya FTA Negotiation Principles (2020)	Present; identifies IP as a key issue and calls on US to provide capacity building and technical assistance implementing IP provisions once in place	Absent	Absent
UK-Ghana Interim Trade Partnership (2021)	Absent	Absent	Absent

Source: Adapted from Devermont and Harris (2021)

What does this portend for Africa?

Africa has unique demographic advantages that include a young and increasingly literate population, a burgeoning middle class, initiative-taking mobile network operators and escalating Internet penetration (Gyori, 2018). Accordingly, digitalizing Africa today paves way for more resilient economies in the future (IFC, 2017). Innovative digital financial services, including mobile money, can increase financial opportunity in Africa and transform the landscape of financial inclusion for the unbanked or underserved (Gyori, 2018). By enhancing unconstrained access to financial services, capital, goods and services, these innovations can integrate the poor and minorities into the mainstream economy while addressing inequalities. Such innovations in economic development include development of small and micro enterprises (SME) support systems, infrastructural development, circular economic activities and increase in employment. As examples of what is possible through access to technology, some of these innovations enable remote micropayments to and from SMEs, while other proposed FinTech propositions include involving central banks in embracing blockchain technology and transitioning to sovereign virtual currencies. Transformations such as these have vast implications for macroeconomic stability, and would likely improve tax collection, compliance and other administrative functions of the government (Yermack, 2018).

At the same time, the International Monetary Fund (IMF) has noted that as countries become increasingly digitalized, they must invest in four broad policy pillars: infrastructure, policy frameworks, skill-building and appropriate risk management policies. At present, numerous African countries lack these data governance pillars (and the enforcement capacity) needed to support a well-functioning data-based economy (Adeniran and Osakwe, 2021). The discourse around the consequences of FinTechs remains controversial and should be viewed from a geographical perspective (Wójcik, 2021); in as much as MPesa was nurtured by, and successful in Kenya, very few African countries have, within their current legislative framework, taken a stand on the legitimacy of digital currency and initial coin offerings (ICO). Data governance provides invaluable support for these developments.

Formulating a research and policy agenda

Opportunities associated with financial data governance

Technology is evolving at a fast pace, and there is a constant need to both evaluate these developments and engage in research to nurture the capacity for the management and governance of data. Financial data governance should be viewed from the perspective that it can create value, if appropriately managed. Data governance enables organizations to be competitive and agile, managing costs to

address the needs of their customers (Panian, 2010) more effectively. The desirable attributes that facilitate value creation include the availability of superior, relevant and consistent data, and compatible technology, combined with clear audibility and easy accessibility (Panian, 2010; Petzold et al., 2020).

What is the expected level of data quality and service attendant to new financial innovations? Inadequate data quality and poor availability yields poor productivity, with significant amounts of time wasted on non-value-added activities, including data sourcing, data aggregation, data reconciliation, data cleansing and manual reporting (Petzold et al., 2020). Therefore, effective data governance may require rethinking organizational design to accommodate a balance between the setting of standards, strategic direction and execution—a balance necessarily affected by data complexity (which increases with the scope of business operations), the speed with which core data evolves and the maturity of the underlying and predominant technology.

What are some of the emerging models of organizational design that would best utilize available opportunities? With its focus on systems that appreciate autonomy for individuals and communities, and its emphasis on using open data to achieve commercial benefit and efficiency in public services, digitalization balances public and private interests. In its Policy Brief No. 89, the United Nations Department of Economic and Social Affairs (UDESA) outlined some areas in which the use of open data and Big data analytics could be considered useful (UDESA, 2020), such as in attaining real-time reactions to changes in economic phenomena, facilitating coordination and collaboration across different stakeholders in the financial system and enhancing public trust and countering misinformation when explaining complicated economic cycles. The COVID-19 pandemic propelled digitalization to the forefront of discourse on the nature of the world economy of the future (Wójcik, 2021), but digitalization can also identify and address vulnerable groups to provide effective resource management. Such value-added actions, however, necessitate enhanced data governance to complement their efforts. The question that follows then is: What have been the linkages between different levels of data governance and resource management?

Challenges and risks associated with big data in the financial sector

As FinTechs expand the geographical limits of the financial sphere, initiating new products and offerings based on copious financial data, they complicate the predicament of regulators (Wójcik, 2021). Firms that have under-invested in governance make their organizations vulnerable to real and often expensive breaches. The concerns around the handling of personal information, and privacy infringement by FinTechs, have not been fully assessed but certainly include issues of customer privacy and protection. Data handling risks arise at three nodes: data collection,

processing and even archiving. These risks crystallize when data is inadequately handled at the three nodes and in a manner that compromises the firm. In a January 2020 Consultative Group to Assist the Poor – CGAP, 2020: 1) report, Medine and Murthy noted that:

> As the commercial use of personal data grows exponentially, so do concerns over whether that data will be used in consumers' best interests. This is particularly true for financial services in emerging economies, where data expand the potential for reaching poor and underserved communities with suitable products but where customer protection risks are great. In many markets ranging from Indonesia to India and Kenya, it is unfair to impose the burden of consent on individuals to protect their data when such a large proportion of the population are opening accounts or coming online for the first time, literacy rates are low, and individuals face potential language and technological barrier.

To address these concerns, Janssen et al. (2020) argued that data governance principles should include evaluation of data quality and bias (before data is used), post-processing validity checks and data minimization/need-to-know protocols (e.g., only necessary information should be shared as opposed to complete data sets). Other policies advocated by Janssen et al. (2020) include bug bounty schemes (i.e., rewarding those who detect errors and issues), informing when sharing, data separation (e.g., sensitive versus insensitive data) and citizens' control of data (i.e., citizens and organizations should be sufficiently empowered to validate the accuracy of their data). Finally, Janssen et al. (2020) stressed the importance of collecting data at the source, and authorization to access data (including separation of concerns so no single person could misuse or abuse data), distributed storage of data (because distributed systems are less vulnerable and circumvent easy data combining) and the appointment of data stewards for accountability.

In short, the data risks posed by FinTechs can be better managed by an improved regime of data management, adoption of advanced analytic techniques and reliance on cognitive technologies. The overriding concern is the extent to which these principles, policies and procedures have been implemented, and the degree to which they have influenced data governance. Malladi et al. (2021) observed that stakeholders exercised disjointed efforts to achieve sustainable last-mile delivery models. Furthermore, open access to information such as healthcare-schemes data, social-inclusion data, COVID-19 data and vaccination data had not been fully leveraged, demonstrating incidences of incoherence. In a dynamic environment, last-mile technological systems and artefacts are especially vulnerable to exposure and exploitation.

Cybersecurity remains the biggest threat facing digitalization, with few available experts to mitigate attacks in Africa (International Development Research Centre - IDRC, 2019). Evidence indicates that risks increase as organizations digitalize and automate their operations (Kaplan et al., 2019). Owing to an emergent worldwide commitment

to diminish cybersecurity threats, the International Telecommunication Union (ITU, 2021) developed an index, the Global Cybersecurity Agenda (GCA), to assess countries according to five strategic pillars (Legal Measures, Technical Measures, Organizational Measures, Capacity Building and International Cooperation) and to then aggregate an overall score. Based on these calculations, the top 10 African countries most committed to cyber stability are (with their overall scores in parentheses) as follows: Mauritius (96.89), Tanzania (90.58), Ghana (86.69), Nigeria (84.76), Kenya (81.70), Benin (80.06), Rwanda (79.95), South Africa (78.46), Uganda (69.98) and Zambia (68.88) (ITU, 2018). Each of these countries has, subsequently, addressed challenges in a collaborative manner and, because of this collaboration, 18 African countries currently have an institutional framework for reporting cybersecurity incidents.

Social and ethical issues affecting digitalization of financial data

Beyond the technological challenges of digitalization are the social and ethical issues it presents. The predominant view of regulatory structures is that they stifle innovation; data privacy continues to be a major concern as vast amounts of captured data is easily available to unauthorized stakeholders because personal-information and privacy norms are not honoured (Malladi et al., 2021). There are also technology concerns around some of the technologies such as AI, whose algorithms may be discriminatory. Zook and Grote (2020) imagined digitalization as a decentralized techno-utopian vision of society that would enshrine individual liberty and resist the centralized and surveillance nature of regulations. Royakkers et al. (2018) identified privacy, autonomy, security, human dignity, justice and the balance of power as impacted by digitalization and, consequently, in need of protection; moreover, they opined that, whereas regulation had been developed around privacy and security, official scrutiny was not as well-articulated in the other four areas (which are inherently fundamental in many modern-day constitutional architectures). The question then becomes: What policies and systems can hold governments and private citizens accountable for the use of financial digital data in a manner that does not run afoul of their basic rights?

Enhancing institutional frameworks

Institutional frameworks must be addressed because they affect data collection, transmission, processing, storage, access and interoperability. The preferred approach has, thus far, been regulatory sandboxes that offer co-development of regulation by stakeholders and private self-regulation (Yermack, 2018). However, as policy makers chart their way forward and consider various factors, they must question what structures exist to incentivize FinTechs to adopt and adapt data governance. Davis (2021) proposed a series of actions that could strengthen transparency, accountability and participation in data protection; one such recommendation would require proactive verification of the compliance activities by each of the players in this space.

The impact of FinTechs on the fragility and profitability of financial institutions is still uncertain (Fung et al., 2020). The impact of digitalization through the coordination of decentralized data systems across institutions must still be assessed. What, for example, are the risks to financial data associated with data monopoly? What is the scope for antitrust regulation in so far as data concentration is concerned? Davis (2021) opined that applicable regulatory sanctions and monetary fines should deter breaches of existing governance requirements, but others are not so sure.

From a regulatory perspective, the limits of data governance for Big data implementation are unclear, as are the regional and in-country impacts of recently enacted frameworks and legislation. Davis (2021) recommended that regulatory authorities enjoy multiple mandates, affording them multi-stakeholder engagements and, where possible, regional collaborations. Is there scope for regulatory sandboxes that would allow experiments with direct feedback between citizens and the government? In Africa, this terrain is uncharted; more areas call for in-depth analysis regarding the possible challenges and opportunities of digitalization and financial governance.

3. Conclusions and Implications

The literature on digitalization reveals several emerging themes. Scholars should consider how the abovementioned issues will guide any future discourse on digitalization and financial governance in Africa. In this issue paper, we have outlined the state of financial-data governance and practices in Africa and have discussed areas that necessitate more investigation to narrow existing gaps in knowledge and policy. Finally, we have identified questions and dilemmas facing scholars, practitioners and policy makers and proceed on this journey into a digitalized future. Policy makers should be aware of emerging trends and concerns brought about by digitalization, and they must appreciate that this process will elicit myriad impacts across the continent, ranging from financial to socio-ethical concerns. Such an appreciation calls for continuous reviews and enhancement of existing institutional frameworks.

A dialogue on financial data policy and governance in Africa is essential. The AERC must take this opportunity to create a forum that unites practitioners, scholars, policy makers and institutions to lay the groundwork for the governance of financial data. Such a forum would be well equipped to conduct research and disseminate high-impact findings and recommendations for application across the continent.

References

Abdychev, A., Cangul, M., Diouf, M.A., Esham, N., Gupta, P.K. and Li, Y. Woldemi. 2020. Digitalizing Sub-Saharan Africa: Hopes and hurdles. In *IMF, Regional Economic Outlook: Sub-Saharan Africa.* Washington DC: International Monetary Fund.

ACIC. 2020. *Africa cyber security report −2019/2020*. Africa Cyber Immersion Centre.

Ademuyiwa, I. and Adeniran, A. 2020. *Assessing digitalization and data governance issues in Africa*. Centre for International Governance Innovation.

Adeniran, A. and Osakwe, S. 2021. *Why digitalization and digital governance are key to regional Integration in Africa.* Centre for Global Development. https://www.cgdev.org/blog/why-digitalization-and-digital-governance-are-key-regional-integration-africa.

African Union. 2014. African Union Convention on CyberSecurity and Personal Data Protection. https://au.int/sites/default/fles/treaties/29560-treaty-0048-_african_union_convention_on_cyber_security_and_personal_data_protections_e.pdf.

AUC/OECD. 2021. *Africa's development dynamics 2021: Digital transformation for quality jobs.* African Union Commission/ Organization for Economic Cooperation Development. https://doi.org/10.1787/0a5c9314-en.

Backbase. 2021. *Banking 2025: Four pillars of the digital First Bank.* Backbase. https://go.backbase.com.

BIS. 2019. *BigTech and the changing structure of financial intermediation.* Bank for International Settlements, BIS.

Chitimira, H. and Torerai, E. 2021. "The nexus between mobile money regulation, innovative technology and the promotion of financial inclusion in Zimbabwe". *Potchefstroom Electronic Law Journal, 24*: 1-33. https://doi.org/10.17159/1727-3781/2021/v24i0a10739.

Davis, T. 2021. *Data protection in Africa: A look at OGP member progress*. Open Government Partnership.

Deloitte. 2017. *Privacy is paramount: Personal data protection in Africa.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Provacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf.

Deloitte. 2020. *Acceleration of digitization as a result of COVID-19.* Deloitte. https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/acceleration-of-digitization-as a result-of-covid-19.html.

Derrick, W., Lee, W.Y. J. and Yeh, F. 2020. "Friend or foe: The divergent effects of FinTech on financial stability". *Emerging Markets Review, 45*(100727).

Devermont, J. and Harris, M. 2021. *Digital Africa: Levelling up through governance and trade.* Centre for Strategic and International Studies. https://www.csis.org/analysis/digital-africa-leveling-through-governance-and-trade.

Enberg, Jasmine (2019). *emarketer*. Global Mobile Payment Users. https://www.emarketer.com/content/global-mobile-payment-users-2019, 2019

Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). BigTech and the changing structure of financial intermediation. *Economic Policy*, 34(100), 761–799.

Global Mobile Payment Users. 2019. *Emarketer*. Global mobile payment users. https://www.emarketer.com/content/global-mobile-payment-users-2019, 2019.

Gregory, A. 2011. "Data governance—Protecting and unleashing the value of your customer data assets". *Journal of Direct, Data and Digital Marketing Practice, 12*(3): 230–248. https://doi.org/10.1057/dddmp.2010.41.

Gressin, S. 2018. *Federal Trade Commission*. The Marriott data breach. https://www.consumer.ftc.gov/bog/2018/12/marriot-data-breach.

Guest, G., Namey, E. and McKenna, K. 2017. "How many focus groups are enough? Building an evidence base for non-probability sample sizes". *Field Methods*, 29(1): 3–22. https://doi.org/10.1177/1525822X16639015.

Gyori, D. 2018. *Africa's ten key advantages in digital transition.* The Asian banker. http://www.theasianbanker.com/updates-and-articles/africas-ten-key-advantages-in-digital-transition.

IDRC. 2019. Shaping an Internet for women's empowerment. International Development Research Centre. https://www.idrc.ca/en/research-in-action/internet5-shaping-internet-womens-empowerment. International Telecommunications Union (2021). Global Cybersecurity Industry.

IFC. 2017. *How Fintech is reaching the poor in Africa and Asia: A start-up perspective.* International Finance Corporation.

International Telecommunications Union - ITU. 2018. *IG_workshop_August2018.* https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session5_SergeZongorev.pdf.

International Telecommunications Union - ITU. 2021. *Global cybersecurity index* (GCI). https://www.itu.int/pub/D-STR-GCI.01.

Janssen, M., Brous, P., Estevez, E., Barbosa, L.S. and Janowski, T. 2020. "Data governance: Organizing data for trustworthy artificial intelligence". *Government Information Quarterly,* 37(3): 1-8. https://doi.org/10.1016/j.giq.2020.101493.

Jafri, J. 2021. Fintech, philanthropy and development: Emerging issues with digital inclusion. Financial Geography Working Paper Series: ISSN 2515–0111, 2.

Kaplan, J., Richter, W. and Ware, D. 2019. *Cybersecurity: Linchpin of the digital enterprise.* McKinsey and Company. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20Linchpin%20of%20the%20digital%20enterpri.

Kirui, B. 2020. The role of mobile money in international remittances: Evidence from Sub-Saharan Africa. Nairobi: AERC Working Paper.

Lehner, O.M. and Simlinger, R. 2019. "When function meets emotion, change can happen: Societal value propositions and disruptive potential in fintechs". *International Journal of Entrepreneurship and Innovation, 20*(4): 277–288. https://doi.org/10.1177/1465750319857974.

Lewis, R., Villasenor, J. and West, D. 2017. Building a secure and inclusive global financial ecosystem. Brookings Financial and Digital Inclusion Project report.

Lopez, C. 2020. Principals of financial regulation for Big Tech. Observer Research Foundation. Digital frontiers. https://www.orfonline.org/expert-speak/principles-financial-regulation-big-tech/.

Macmillan, R. 2020. "Data governance: Towards a policy framework". *Industrial Development Think Tank (IDTT).*

Malladi, C., Soni, R. and Srinivasan, S. 2021. "Digital financial inclusion: Next frontiers—Challenges and opportunities". *CSIT*, 127–134.

Medine, D. and Gayatri, M. 2020. *Making data work for the poor: New approaches to data protection and privacy.* CGAP.

Mervyn, K., Simon, A. and Allen, D.K. 2014. "Digital inclusion and social inclusion: A tale of two cities". *Information, Communication and Society,* 17(9): 1086–1104. https://doi.org/10.1080/1369118X.2013.877952.

Muralidhar, S.H., Bossen, C. and O'Neill, J. 2019. "Rethinking financial inclusion: From access to autonomy". *Computer Supported Cooperative Work,* 28(3–4), 511–547. https://doi.org/10.1007/s10606-019-09356-x.

Muthiora, B. 2015. "Enabling mobile money policies in Kenya: Fostering a digital financial revolution". *GDMA Mobile Money for the Unbanked.*

Ozili, P.K. 2021. "Financial inclusion research around the world: A review". *Forum for Social Economics,* 50(4): 457–479. https://doi.org/10.1080/07360932.2020.1715238.

Panian, Z. 2010. "Some practical experiences in data governance". *World Academy of Science, Engineering and Technology, 62:* 939–946.

Petzold, B., Roggendorf, M., Rowshankish, K. and Sporleder, C. 2020. *Designing data governance that delivers value*. McKinsey Technology.

Rolfe, K. 2019. Payments industry intelligence. Mobile money transactions equivalent of half of Kenya's GDP.

Royakkers, L., Timmer, J., Kool, L. and Est, R. 2018. "Societal and ethical issues in digitization". *Ethics and Information Technology, 20:* 127–142.

Payments. 2020. Security and risk. FinTech Dave Reports Data Breach Involving 7.5M Users. https://www/pymnts.com/news/security-and-risk/2020/fintech-dave-data-breach-hackers/.

Republic of Kenya. 2017. *Kenya Social Protection Sector Review Report 2017*. Nairobi: Ministry of Labour and Social Protection.

Rijswijk, K., Bulten, W., Klerkx, L., den Dulk, L., Dessein, J., Debruyne, L. and en Nematoden, O. 2020. *Digital transformation: Ongoing digitization and digitalization processes.* Desira.

Sengere, L. 2017. EcoCash has processed over $23 billion since launch and that's not the only impressive figure. TechZim.

Shipalana, P. 2019. Digitising financial services: A tool for financial inclusion in South Africa? South African Institute of International Affairs.

UNCTAD. 2020. Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

UNCTAD. 2021. Summary of adoption of e-commerce legislation worldwide. United Nations Conference on Trade and Development. https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

UDESA. 2020. Strengthening data governance for effective use of open data and big data analytics for combating COVID-19. United Nations Policy. Department of Economic and Social Affairs, United Nations.

Wang, P. and Johnson, C. 2018. "Cybersecurity incident handling: A case study of the Equifax data breach". *Issues in Information Systems, 19*(3).

Wójcik, D. 2021. "Financial geography II: The impacts of Fintech—Financial sector and centres, regulation and stability, inclusion and governance". *Progress in Human Geography,* 45(4): 878–889. https://doi.org/10.1177/0309132520959825.

World Bank. 2021. *Data, digitalization and governance*. Washington DC: World Bank.

Yermack, D. 2018. Fin Tech in Sub Saharan: What has worked well and what hasn't p. 25007. National Bureau of Economic Research Working Paper.

Zook, M. and Grote, M.H. 2020. "Initial coin offerings: Linking technology and financialization". *Environment and Planning Annuls*, 52(8): 1560–1582. https://doi.org/10.1177/0308518X20954440.

Mission

To strengthen local capacity for conducting independent, rigorous inquiry into the problems facing the management of economies in sub-Saharan Africa.

The mission rests on two basic premises: that development is more likely to occur where there is sustained sound management of the economy, and that such management is more likely to happen where there is an active, well-informed group of locally based professional economists to conduct policy-relevant research.

www.aercafrica.org

Learn More

www.facebook.com/aercafrica

www.instagram.com/aercafrica_official/

twitter.com/aercafrica

www.linkedin.com/school/aercafrica/

Contact Us
African Economic Research Consortium
Consortium pour la Recherche Economique en Afrique
Middle East Bank Towers,
3rd Floor, Jakaya Kikwete Road
Nairobi 00200, Kenya
Tel: +254 (0) 20 273 4150
communications@aercafrica.org