Padmashree Gehl Sampath & Fiona Tregenna (Editors)

Digital Sovereignty: African Perspectives

Digital Sovereignty: African Perspectives

Padmashree Gehl Sampath and Fiona Tregenna (Editors)

With Contributions From:

Ayça Atabey; Benjamin Akinmoyeje; Michael Asiedu; Odilile Ayodele; Ngwinui Belinda Azenui; Bridget Boakye; Adio-Adet Dinika; Oarabile Mudongo; Sylvia Ndanu Mutua; Jacquelene Mwangi; Faith Obafemi & Emma Ruiters

An output of the Virtual Research Sprint: Toward an African Narrative on Digital Sovereignty, which ran from 7 June to 30 July 2021, a collaboration between the Alexander von Humboldt Institute for Internet and Society and the University of Johannesburg.

CITE AS:

P. Gehl Sampath & F. Tregenna (Eds.) (2022). Digital Sovereignty: African Perspectives. Johannesburg: DSI/NRF South African Research Chair in Industrial Development. DOI: 10.5281/zenodo.5851685.

ISBN: 978-1-77630-398-4

UNIVERSITY OF JOHANNESBURG

ALEXANDER VON HUMBOLDT INSTITUT FÜR INTERNET UND GESELLSCHAFT

Contents

Contributor Bios

Adio-Adet Dinika a doctoral researcher in Digitisation, digital labour rights and the digital economy based at the Center for Labour and Politics (ZAP) at the University of Bremen and a PhD Adjunct fellow at the Bremen International Graduate School of Social Sciences (BIGSSS).

Ayça Atabey is a lawyer and a researcher, currently enrolled as a PhD student at Edinburgh University. Her PhD research focuses on the role that the notion of 'fairness' plays in the protection of vulnerable data subjects. She is also a research assistant for the Digital Futures Commission at 5Rights Foundation.

Ngwinui Belinda Azenui is an assistant professor of Economics at Denison University, with a PhD in Economics from the University of Utah. Her primary research interests center around growth and structural change in Sub-Saharan Africa, using macroeconomic modeling and evidence-based analysis. She is enthusiastic about issues related to the sustainable transformation of Africa's economies.

Benjamin Akinmoyeje is a PhD candidate at the Namibia University of Science and Technology. His research focuses on persuasive technology and mHealth apps for stress management among university students in Namibia. Among his key interests is the use of internet access and technologies to improve healthcare in low resource environments.

Bridget Boakye is Policy Lead: Internet Policy Unit at the Tony Blair Institute for Global Change. Her work focuses on internet policy, start-ups and innovation in Africa, AI ethics and resetting the global narrative of Africa through tech. Her previous work includes data science and analytics, and business development and strategy.

Emma Ruiters is an associate consultant at Genesis Analytics in the digital economy practice. She has assisted in the development of South Africa's ICT and Digital Economy Masterplan, Malawi's Digital Economy Strategy. She has an MSc in Development Economics from SOAS, University of London.

Faith Obafemi is a tech lawyer with a focus on blockchain, cryptocurrency, emerging technologies and Space technologies. Faith helps projects navigate the compliance maze for novel technologies through Future-Proof Intelligence (FINT) where she serves as Head of Strategy.

Jacquelene Mwangi is a doctoral candidate at Harvard Law School. Her doctoral work centers on the historical and current trends of technological change in Sub-Saharan African societies, and its evolving relationship with rules and institutions, the state, and society.

Michael Asiedu is a doctoral researcher at the University of St. Gallen Institute of Political Sciences (IPW-HSG), Switzerland. His research focuses on digital censorships such as internet shutdowns in Africa and the attendant challenges regarding roles of the courts and civil societies.

Oarabile Mudongo is a Research Fellow at Research ICT Africa and a Technology Exchange Fellow with Ford Foundation and Media Democracy Fund. He is currently researching data driven technologies, particularly AI surveillance, automated facial recognition and algorithm-assisted decision-making tools in the AI in Africa Policy (AI4D) project. He is also as an MA candidate in Interdisciplinary Digital Knowledge Economic Studies at University of the Witwatersrand.

Odilile Ayodele is a Senior Research Associate in the BRICS at the University of Johannesburg. She holds a PhD in Politics from the University of Johannesburg. Her current research interests include: the International Relations of Technology, and the International Politics of Digital Transformation in Africa. She is particularly curious about Africa's evolving subnational diplomacy in the context of the digital age.

Sylvia Ndanu Mutua is a communication expert and broadcast media professional with extensive experience in Kenyan media. She holds a PhD in Communication Studies from the Communication University of China. Her research interests focus on; Content governance, New Media, and Digital Literacy.

About the Editors

Professor Padmashree Gehl Sampath is currently a Director of the Global Access in Action Project, Harvard University, and a Fellow at the Berkman Klein Center, Harvard University. Her thought leadership is at the intersection of Development Economics, Economic History and Political Economy. In particular, she is interested in issues related to capabilities, technology governance, inequality and global governance. She is the recipient of many prestigious international research grants and awards on these topics, including from the Rockefeller Foundation and the German Chancellor, and currently advises a number of agencies on related topics, including the UNDP, ILO, WHO, and the African Development Bank.

Professor Fiona Tregenna heads the DSI/NRF South African Research Chair in Industrial Development, and is a Professor of Economics at the University of Johannesburg. She holds a Ph.D. in Economics from the University of Cambridge. Her primary research focus is on structural change, deindustrialisation, industrial development, innovation and technological change. Fiona is an elected member of the Academy of Science of South Africa (ASSAf), and has received various awards and major research grants. She serves on a number of high-level boards, advisory panels and councils, and has acted as a consultant or advisor to organisations such as UNIDO, UNCTAD and the ILO.

Acknowledgements

This publication is an outcome of the Virtual Research Sprint, titled *Toward an African Narrative on Digital Sovereignty*, which ran from 7 June to 30 July 2021.

The sprint was conceptualised in discussions between the Berkman Klein Center and the Humbolt Institute for Internet and Society, facilitated in particular by Prof. Urs Gasser (Former Executive Director of the Centre, now Dean of the School of Social Science and Technology of the Technical University of Munich), Prof. Wolfgang Schultz (Director of the Humbolt Institute for Internet and Society) and Prof. Padmashree Gehl Sampath (Senior Advisor, Global Access in Action, Berkman Klein Center for Internet and Society, Harvard University). It is based on reflections from Prof. Gehl Sampath's three-year project at the Berkman Klein Center, titled *Development in the Digital Economy*. The Sprint was then situated as part of the *Ethics of Digitalisation* project run by the Humboldt Institute for Internet and Society, the Leibniz Institute for Media Research, the Hans-Bredow-Institut, the Berkman Klein Center for Internet and Society, and the Global Network of Internet and Society Research Centers (NoC), under the auspices of the Federal President of Germany, with funding from the Mercator Foundation.

The Sprint was run from the DSI/NRF South African Research Chair for Industrial Development (SARChI Industrial Development) at the University of Johannesburg. The editors are grateful for the engagement of colleagues from SARChI Industrial Development, particularly Dr Phumzile Ncube (the Sprint Coordinator), Prof. Alexis Habiyaremye (Senior Researcher, SARChI Industrial Development) and Mrs Koketso Manyane-Dlangamandla (Administrator, SARChI Industrial Development). A special thanks to Dr. Phumzile Ncube for her invaluable contributions to the sprint and this publication. The editors also acknowledge Dr Matthias Ketterman and Ms Nadine Birner of the Humbolt Institute for Internet and Society, for their support during the programme, and for the organisation of a high-level seminar with the Federal President, Mr Frank Walter Steinmeier, who personally engaged with the Fellows of the Sprint. Discussions with and support from colleagues from the Berkman Klein Center for Internet and Society, particularly Prof. Urs Gasser and Mr Reuben Langevin helped situate the Sprint better in the wider milieu of the Sprints organised by the Network of Centers respectively.

The Sprint, and this collection, have benefited from the rich and diverse contributions of each of the experts who interacted with the fellows on a weekly basis. We are thankful to Mr Bright Simons (mPedigree and the IMANI Centre for Policy and Education), Prof Wim Naudé (Cork University), Ms Khadija Abdulla Ali (drone pilot, Zanzibar Drone Mapping Initiative), Mr Manish Raghavan

(Cornell University), Mr Leonard Cortana (Tisch School, New York University), Prof James S. Wahutu (New York University), Prof Thomas Streinz (New York University), Mr Amadou Diop (MNS Consulting Group), Prof Olufunmilayo Arewa (Temple University), and Prof Irene Lo (Stanford University), for their time and contributions. The Sprint could not have succeeded without the commitment and engagement of our outstanding Fellows, as reflected in two sets of peer-reviewed outcomes of the Sprint: the papers in this volume, and a series of blog posts. We thank them for their engagement and look forward to continuing and building on the discussions in other forums in the future.

Chapter 1

Digital Sovereignty in Africa: An Introduction

Padmashree Gehl Sampath and Fiona Tregenna

Introduction

Digital technologies can promote productivity, dynamic growth returns, structural change and the implementation of sustainable development goals, but they also present new challenges. Some of these challenges – such as data extraction and commodification, rising costs of innovation, an influx of predatory firms and the loss of privacy – have received much attention in policy and academic debates in recent years (O'Neil, 2016; Abebe, 2019). Many commentators have suggested a wider framing of national policy to assert digital sovereignty in this new age, with stronger state regulation of the way the internet works to help realise the national and individual interests of citizens (Pohle & Thiel, 2020).

Put simply, such calls for digital sovereignty require governments to articulate a national vision of economic independence, development and personal freedom in the interest of their citizens. Yet this can be complex in practice. As countries around the world, both developed and developing, embark on policy-making exercises to exercise digital sovereignty, many important questions arise. What does economic independence and development look like in the digital economy? How can we define and balance freedom, at the national, economic and personal levels, within countries? Are states best positioned to define the interests of their citizens and, if so, what forms of participatory engagement are required? What are the implications of the 'digital divide', both within and between countries, for digital sovereignty? Is 'digital sovereignty' the best way to articulate and frame policy in the digital economy?

These questions assume particular importance in developing countries, for a number of reasons. First, the challenges associated with the digital economy – including data extraction, rise of predatory firms and increasing costs of innovation – have specific effects on developing countries. They manifest as growing knowledge divides, loss of comparative advantages in business, and technology-led unemployment. Second, weak institutions and, commonly, a low policy capacity to anticipate the influence of new digital technologies, undermine the ability of countries to effectively steer the process. Third, data inequality materialises in different ways in practice. Consequently, considering how the data economy interacts with different social and cultural norms to shape (or influence) linguistic and cultural exclusion, community identity is highly relevant to asserting digital sovereignty. In this process, important questions of data use and

accountability by actors – notably foreign firms, local firms and governments – arise, with important substantive and distributive implications at the country level (Fisher & Strienz, 2019).

Articulating a vision of wider development and personal freedom in such a context is crucial, but, at the same time, might require a bigger push and greater ambition on the part of countries. This is particularly because it will need a nuanced and differentiated approach that requires:

(a) identifying the core aspects of digital sovereignty that can promote national development objectives in policy and practice, while at the same time,
(b) striking the right balance between the economic value and personal value of data.

Digital Sovereignty: Issue Identification

The notion of digital sovereignty is by no means a new one, but one that has gained prominence in digital economy debates due to the emergence of new geopolitical alliances and actors, and the growing accumulation of power in large platform companies (Couture & Toupin, 2019). The ideological underpinnings of dominant narratives in this debate can be traced back, on the one hand, to normative principles of the rule of law, and the protection and preservation of human and constitutional rights of citizens (see, for example, Bria, 2015) and, on the other, to the need to re-establish the primacy of institutions, processes and guarantees, including the economic freedom for local companies to operate in the digital economy (Floridi, 2020; Polatin-Reuben & Wright, 2014). In July 2020, for example, the German government announced its intention "to establish digital sovereignty as a Leitmotiv of European digital policy" in its official programme for its presidency of the European Council.[1] In this context, digital sovereignty could be identified as a route to preserve and protect the constitutional rights and guarantees of European citizens and to control the platform economy to enable European companies to have sufficient freedom to operate.

But elsewhere, and particularly in the global South, there is little clarity on the term and its application. Arguably, reasons for this this could include the fact that the notion of sovereignty itself remains relatively problematic in several ways in the global South (Kukutai & Taylor, 2016), but it could also stem from the fact that countries have viewed digital policy as a sub-set of their technology policies (see Budnitsky & Jia, 2018). This publication is one of the outcomes of the *Virtual Research Sprint: "Toward an African Narrative on Digital Sovereignty"*, which ran from June to July 2021. This Research Sprint, the first of its kind in Africa, was designed to focus on what

[1] European Sources Online, Thea German Presidency of the EU Council (2020). Available from: <https://www.europeansources.info/record/german-presidency-of-the-council-of-the-european-union-july-to-december-2020/> (accessed 24 March 2021).

digital sovereignty could mean in the context of Africa, with the intent of extracting the key elements of a pan-African narrative on digital sovereignty. Key issues considered in the Sprint include:

- In the digital economy, how can citizens and states reassert control, to what end, and how? To this end, is digital sovereignty a useful concept and, if so, what could be the meaning and import of digital sovereignty in the global South, and specifically in Africa?
- Can there be economic autonomy and a break away from technological dependence without political autonomy on the one hand, and without data infrastructure and data control on the other?
- Can a collective capacity for states, individuals and communities to engage in technological development be created (Couture & Toupin, 2019) and, if so, how?
- Do current developments in Africa reflect, or build towards, a sovereign, pan-African vision for development and economic independence in the digital age?
- In such a vision, how can data extraction, data use and data re-use foster the creation of competitive advantage, innovation and technological learning, thereby enabling local businesses, creating jobs and promoting structural change in Africa?
- Building on that, what sort of relationships between citizens and states could enable such a developmental model?
- How can we frame a new discourse that factors in development as a central component of the data economy, taking into account the different starting points of countries as they enter and as they engage with data?

In grappling with these broader framing questions, the Sprint addressed questions related to linguistic and cultural heterogeneity in the internet world, and the need for a homegrown narrative on privacy, informed consent and data protection in the African context.

The Research Sprint

The Virtual Research Sprint was conceptualised and run from the University of Johannesburg, within the framework of the *Ethics of Digitalisation* project run by the Humboldt Institute for Internet and Society, the Leibniz Institute for Media Research, the Hans-Bredow-Institut, the Berkman Klein Center for Internet and Society, and the Global Network of Internet and Society Research Centers (NoC), under the auspices of the Federal President of Germany and with funding from the Mercator Foundation. The programme ran for eight weeks, with each week covering a substantive, thematic module. The modules were conceptualised to generate discussions on four key components of digital sovereignty in a 'latecomer' context:

- Economic autonomy and technology access
- Developmental autonomy
- A tailored discourse on privacy and data governance
- Equal data and digital access.

Following a call for applications, fellows were selected through a rigorous and competitive process. The cohort of fellows was drawn from 14 different countries, and from a diverse range of disciplinary backgrounds, including law, social sciences, engineering, innovation studies, international relations and data science. Fellows were also drawn from different institutional backgrounds, such as universities, NGOs, the media, and both the public and private sectors. This mix of backgrounds and experience made for a diverse and dynamic group, transdisciplinary discussions and out-of-the-box thinking.

To facilitate productive engagements amongst the fellows, four working groups were created on the following issues, corresponding with the key components of the Sprint:

- Digital transformations for and in Africa (economic autonomy, technological change)
- Digital technologies for development in Africa
- Privacy and data governance models for Africa
- Data access and data equality for Africa.

This enabled the cross-fertilisation of ideas and the sharing of country-specific experiences, and also enabled the fellows to interact more closely in smaller groups. The discussions from the working groups fed back into the weekly deliberations in the main sessions, thereby creating dynamic feedback loops between academic research topics, policy and practice.

This Volume

This volume includes twelve pieces written by fellows in the Research Sprint.[2] The first piece, by Adio-Adet Dinika in Chapter 2, focuses on digital infrastructure, including the contentious issue of who funds connectivity and the implications for digital sovereignty. Next, in Chapter 3, Ayça Atabey analyses the issue of data protection through a legal lens, evaluating legal frameworks governing cross-border data flows. In Chapter 4, Ngwinui Belinda Azenui considers digital technologies in the context of structural constraints on Africa's development, and discusses how these technologies can form part of a structural change agenda. Benjamin Akinmoyeje's contribution in Chapter 5 turns to the links between digital development and digital sovereignty and health, with a specific focus on digital health in the context of Nigeria. Chapter 6, by Bridget

[2] Additional contributions by fellows are published as blogs, available at: https://digitalsovereigntyafrica.wordpress.com.

Boakye, explores the key issue of AI governance in Africa through a case study of Mauritius's national AI strategy. In Chapter 7, Emma Ruiters discusses the relationship between entrepreneurship and the digital economy, drawing particular attention to policy measures needed to support tech entrepreneurship. Chapter 8, authored by Faith Obafemi, connects the issues of digital inclusion, digital sovereignty and 'smart cities', putting forward a range of policy recommendations for smart cities stakeholders. In Chapter 9, Jacquelene Mwangi critiques received notions of digital colonialism and argues for a shift to a 'people-centred' narrative of digital sovereignty. Data privacy is the focus of Chapter 10, in which Michael Asiedu advocates for data access principles as a key priority for African countries. In Chapter 11, Oarabile Mudongo discusses the implications of digital ID as a digital sovereignty measure, especially in the post-Covid world. In the penultimate chapter, Chapter 12, Odilile Ayodele explores the global connectivity politics of Big Tech in Africa, reflecting on divergent perspectives and also considering the implications of the African Continental Free Trade Agreement (AfCFTA) for digital sovereignty. Finally, Chapter 13, authored by Sylvia Ndanu Mutua, grapples with the contentious issue of the role of AI in content governance and draws out the potential implications for African digital sovereignty.

These chapters thus engage with a range of topics on digital sovereignty in Africa, and offer a rich set of perspectives. They have a high degree of policy relevance and provide fresh insights into key issues relating to digital economies, digital transformation and data access in governance in Africa. The diversity of topics and standpoints, united around the common theme of digital sovereignty, reflects the range of the authors' experiences and disciplinary backgrounds. While focused on Africa, the chapters are also relevant to developing countries more broadly. We hope that these contributions will stimulate further research in this field, while also having value for policymakers and other stakeholders. Ultimately, the volume seeks to contribute to developing a distinctly African narrative on the topic of digital sovereignty, a topic that is likely to become increasingly important in years to come.

References

Abebe, R. T. (2019). Designing algorithms for social good. Dissertation, Cornell University. Available from: https://doi.org/10.7298/n8w3-8629 (accessed 19 November 2021.

Bria, F. (2015). Public policies for digital sovereignty. Available from: http://platformcoop.net/participants/francesca-bria (accessed 07 November 2021).

Budnitsky, S. & Jia, L. (2018). Branding internet sovereignty: Digital media and the Chinese-Russian cyberalliance. *European Journal of Culture Studies,* (21)5: 594-613.

Couture, S. & Toupin S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media and Society*, 21(10): 2305-2322.

Fisher, A. & Strienz, T. (2021). Confronting data inequality. International Law and Justice Working Papers 1, Institute for International Law and Justice, New York, NY. Available from: https://ssrn.com/abstract=3825724

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33:369-378.

Kukutai, T. & Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda*. Canberra, Australia: Australian National University Press.

O'Neil, C. (2016). *Weapons of math destruction*. New York, NY: Crown Books.

Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532.

Polatin-Reuben, D. & Wright, J. (2014, July 7) An Internet with BRICS characteristics: Data sovereignty and the Balkanisation of the Internet. *Usenix*. Available from: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (accessed 22 November 2021).

Chapter 2

Rethinking Digital Infrastructure Development in Africa

Adio-Adet Dinika

Introduction

That digitalisation holds massive potential for Africa is beyond question (Reiter, 2020). The McKinsey Global Institute's (MGI) "Lions go digital" report highlights that "[i]f governments and the private sector continue to build the right foundations, the Internet could transform sectors as diverse as agriculture, retail, and healthcare – and contribute as much as US$300 billion a year to Africa's GDP by 2025" (McKinsey Global Institute, 2013, p.7). In the wake of the COVID-19 pandemic, McKinsey and Company recommend that Africa accelerate its digital transformation by speeding up investments in digital infrastructure, improving access and creating an enabling environment.

The COVID-19 pandemic has not only exponentially pushed forward digitalisation but has also revealed the digital infrastructure disparities across the continent, thus making the need for massive investment in digital infrastructure even more critical. Digital infrastructure, in its broad sense, comprises the physical and non-physical resources essential for the use of data, computerised devices, systems and processes (Atkinson, Castro, Ezell, McQuinn & New, 2016). The components of digital infrastructure include, but are not limited to, the Internet, end-user devices (computers, phones), data centres, the internet of things (IoT), the cloud and software applications (Designing Buildings Wiki, 2021). This article focuses specifically on Internet connectivity (broadband).

Digital investment does not come cheap; the UN Broadband Commission for Sustainable Development estimates that Africa requires an additional US$109 billion in investment to achieve universal, affordable and high-speed internet access by 2030. Africa relies mainly on private funding for digital infrastructure. Vodafone, one of the most prominent investors in African telecoms infrastructure, spends around US$1 billion per year in upgrading its facilities across the region (Reiter, 2021). That is a significant amount just for maintenance, and means that the cost for construction and set-up is significantly higher. In the light of this, the most burning question then is, who is funding Africa's digital infrastructure, and at what cost?

Who is Funding Connectivity?

Several non-African organisations have been rushing to provide Internet connectivity to the unconnected people in Africa. Most of this rush has been led by Google, Apple, Facebook, Amazon

and Microsoft, generally referred to as GAFAM (Benyera, 2021; Velluet, 2021). Facebook's Free Basics is already present in at least 65 African countries (Nothias, 2020). Facebook is also leading a private consortium with seven telecom operators (China Mobile International, MTN Global Connect, Orange, Saudi Telecom Company, Telecom Egypt, Vodafone and WIOCC) to finance a 37,000 kilometre fibre-optic cable, called 2Africa, which will circle the continent and connect 16 African countries to the rest of the world. With an estimated cost of between US$500 million and US$1 billion, this project will become operational in 2023 (Dludla, 2021). Google has also launched Project Link, constructing a private cable connecting Portugal to South Africa, with a branch landing in Nigeria. The first phase of this project is set for completion in 2021 (Denis, 2021). In addition, Google has also announced Project Loon, which aims to employ high-altitude balloons to provide Internet connectivity (Sawers, 2017). Just like Facebook's project, this project also makes Africa its priority.

Microsoft has launched its TV White Spaces project as part of its Microsoft Airband Initiative, which it claims will ensure that more people in Africa can have affordable Internet. Bluetown, another Microsoft Airband Initiative partner, provides affordable internet access to 440 000 people in Eastern Ghana (Abdella, 2020). The European Investment Bank has also provided funding to the tune of US$12.3 billion for digital projects in Africa between 2015 and 2020 (Denis, 2021).

Over the last two decades, the Chinese have emerged as a dominant force in the telecom infrastructure landscape in Africa. Approximately 50% of Africa's 3G networks and 70% of the 4G networks were built by Huawei (Hruby, 2021). According to the China Global Investment Tracker, Chinese tech investments and contracts in sub-Saharan Africa between the years 2005 and 2009 were worth US$7.19 billion, with Huawei and ZTE dominating. China's investment in Africa should be viewed in the context of its Digital Silk Road programme, which was launched in 2015 to invest in international digital infrastructure (Govender, 2021). The Digital Silk Road is itself a component of Beijing's Belt and Road Initiative (BRI), a Chinese government white paper from 2013 (Szczepański, 2020; Triolo & Greene, 2021). The activities of private companies such as Huawei and ZTE, which initially were driven by profit maximisation, have also become enveloped in the Digital Silk Road (Triolo & Greene, 2021).

Thus far, Angola, Ethiopia, Nigeria, Zambia and Zimbabwe are beneficiaries of the Digital Silk Road project, with an estimated investment value of USD8.43 billion (Govender, 2021). In 2018, a study by the Infrastructure Consortium for Africa revealed that China had contributed about USD25.7 billion in infrastructure financing to African countries (Govender, 2021). It is important to note that this figure combines digital infrastructure and other infrastructure projects that go beyond the digital. In addition to prior investments in digital infrastructure, China's Digital Silk Road project is

building an information superhighway meant to connect China, Europe and Africa, with the 15 000 km Pakistan and East Africa Connecting Europe (PEACE) expected to be completed by the end of 2021 (Nyabiage, 2021).

It is estimated that Africa needs at least 250,000 new 4G base stations and at least 250,000 kilometres of new fibre to achieve universal internet access (Fukui, Arderne & Kelly, 2019). The African Union, through AUDA-NEPAD, initiated the 10,000-kilometre Eastern Africa Submarine System cable and the Africa Coast to Europe cable connecting Gibraltar to South Africa and landing in countries in the Gulf of Guinea (Denis, 2021). While not comprehensive, this paints a picture of Africa's digital infrastructure needs and the percentage of African funding compared to external financing. Further to this, it is also understood that at least 45% of Africa's population is at least 10 kilometres from fibre network infrastructure, which paints a need for other types of internet connectivity (Fukui et al., 2019).

Implications for Digital Sovereignty

With the high number of investments being made to improve connectivity in Africa, it is clear beyond reasonable doubt that what is being obtained is a repeat of the scramble and partition of Africa, albeit this time led by private corporates, not countries. The most important question to ask is, why? Why are these private companies scrambling to provide "free" internet connectivity to Africa? Could this be a new form of colonialism? Scholars such as Rikap (2021) have argued that this is the rise of intellectual monopolies. Intellectual monopolies rely on their capacity to significantly and systematically monopolise knowledge, leading to them growing exponentially and swallowing any competitor. Facebook is a typical intellectual monopoly, growing exponentially and acquiring most of its competitors, such as Instagram and WhatsApp. To date, Facebook owns four of the most downloaded apps: Instagram, WhatsApp, Facebook, and Facebook Messenger (Shead, 2019). This has severe implications for African start-ups, who cannot reasonably compete with Facebook due to its sheer size and budget.

The fact that a few superstar firms are leading Internet connectivity in Africa is an indication of a rise in intellectual monopoly and digital colonialism (Rikap, 2021). Colonialism relied on predation, which was itself a direct relation of spoliation. Predation is being witnessed at a massive scale at the hands of a few superstar firms – the GAFAM, and Chinese firms such as Huawei and ZTE. At no other time in history has a small sector wielded so much power over the whole world; the power to monitor present behaviour and locations, and the power to predict the future behaviour and locations of individuals in all countries around the globe. According to Facebook IQ (2021), Facebook has 2.74 billion active users, meaning that Facebook literally knows where 35% of the world's population is located and in what they are engaged.

What is more alarming is that, moving beyond questions of privacy and security, there are issues about freedom and control. Facebook can decide what can or cannot be posted and what topics will be allowed to go viral or not. Facebook's free basics project fallout in India and its subsequent focus on Africa is evidence of its use of what Madianou (2019, p.9) calls the "use of disadvantaged communities and less regulated territories as testing grounds for data extraction and technological experiments". It is vital to the view infrastructure financing by these external players in the context of the "new oil" obtained from this digitalisation, that is, data (The Economist, 2021). Data is the most valuable product of digitalisation. It is essential to consider the implications of external financing for digital infrastructure in the light of the data generated, and to not merely end at construction or setup. The lackadaisical approach of African leaders, where they leave these superstar tech firms to provide Internet connectivity and do as they please with the data collected from African users, is akin to blessing digital colonialism. Once Google pays for the Internet connectivity on the African continent, without clear agreements on where the data collected will be hosted, the adage "he who pays the piper calls the tune" becomes evident. The case for having African data stored on the African continent has far-reaching positive benefits, such as developing African data-storage innovations, employment creation and more control and oversight of data security and usage.

Way Forward?

Moving forward, there is a need for Africa to have a consolidated regulatory and investment framework. A lot of political messaging and talk has taken place. Despite the presence of the African Union, Africa remains fragmented, which is to the disadvantage of all African countries. The creation of the African Continental Free Agreement is a good starting point; however, further to this there is a need for Africa to come up with consolidated ways to negotiate with external investors so that negotiations take place with Africa presenting itself as a single block, with a population of 1.3 billion and a budget of US$2.6. Negotiating as one will ensure that Africa has a more significant bargaining position on the table, in contrast to the situation where a country like Zimbabwe negotiates with a company with an annual revenue several times larger than its GDP. One of the resultant effects of this is that the deals often put the African country at a disadvantage and lend themselves to abuse and a situation in which company executives can influence national decisions, thus undermining national sovereignty.

Pursuant to the point above, a united Africa, with a combined total of more than one billion people, can look inwards for its digitalisation agenda. A good example is how China has created digital applications such as Weibo and WeChat, ensuring its digital sovereignty, as all the data is stored in China. The applications operate on the basis of Chinese rules and regulations. Continued

use of externally created applications by Africans poses a severe threat to digital sovereignty, especially in the wake of the Facebook privacy leaks (Holmes, 2021). In addition, it also means large tech companies continue to operate on the continent without oversight, compared with other places where they operate. For example, following the Facebook data leaks, the United States Senate summoned Facebook CEO Mark Zuckerberg for a hearing (Perticone, 2018). The British and Canadian parliaments have done the same (Griffin, 2021). African leaders were conspicuous in their silence on this; after all, Facebook invested millions in improving digital infrastructure in Africa. In a separate case, the US Senate also voted to subpoena the heads of Facebook, Twitter and Google over issues to do with misinformation, bias and privacy (BBC News, 2020).

Strategic public-private partnerships (PPP) may be a viable solution to Africa's digital infrastructure deficit. Instead of Africa relying on external players such as Google and Facebook to come in with their investments, there is a need for more scrutiny of the projects being brought in and the creation of PPP that are strategic and place the interests of Africa first. Critical to this are questions of data security, the use of that data, and the storage of the data. Strategic PPP may entail developing and manufacturing infrastructure on the African continent, with African personnel, and storing the data on the continent and not in the organisations' countries of origin.

Conclusions

African leaders need to rethink the models for financing digital infrastructure. The current model, which sees large corporations come up with a "philanthropic" effort to provide Internet connectivity to unconnected Africans, needs more scrutiny. There is a need for more consolidated regulatory frameworks for African countries, fronted by the African Union and presenting Africa as a single entity, even though Africa is made up of 54 heterogeneous countries. Still, the fact is that, while the Internet needs of the countries may differ in depth, they are by and large the same. Africa will also stand to gain by acting as one united block than as a loose collection of small countries against giant corporations from outside the continent who answer to no one and have revenues bigger than some African nations.

References

Abdella, A. (2020). *How investing in digital infrastructure can make the difference to Africa's economic recovery*. Microsoft News Center Middle East & Africa. Available from: https://news.microsoft.com/en-xm/2020/09/02/how-investing-in-digital-infrastructure-can-make-the-difference-to-africas-economic-recovery/.

Atkinson, R. D., Castro, D., Ezell, S., McQuinn, A. & New, J. 2016. *A policymaker's guide to digital infrastructure*. Information Technology and Innovation Foundation. Available from: https://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf.

BBC News. (2020). *US Senate subpoenas heads of Google, Facebook and Twitter*. Available from: https://www.bbc.com/news/technology-54376327.

BBC News. (2021). Facebook faces mass legal action over data leak. Available from: https://www.bbc.com/news/technology-56772772.

Benyera, E. (2021). *The fourth industrial revolution and the recolonisation of Africa*. Oxon: Routledge.

Denis, B. (2021). *The rise of Africa's digital economy – The European Investment Bank's activities to support Africa's transition to a digital economy*. Luxembourg: European Investment Bank.

Designing Buildings Wiki. (2021). *Digital infrastructure*. Available from: https://www.designingbuildings.co.uk/wiki/Digital_infrastructure.

Dludla, N. (2021). Facebook, telcos to extend subsea cable to four countries. *Reuters*, 16 August. Available from: https://www.reuters.com/world/africa/facebook-telcos-extend-subsea-cable-four-countries-2021-08-16/.

Facebook IQ. (2021). *Insights to go from Facebook IQ*. Available from: https://www.facebook.com/iq/insights-to-go/2740m-facebook-monthly-active-users-were-2740m-as-of-september-30.

Fukui, R., Arderne, C. & Kelly, T. (2019). Africa's connectivity gap: Can a map tell the story? World Bank Blogs. Available from: https://blogs.worldbank.org/digital-development/africas-connectivity-gap-can-map-tell-story.

Govender, M. (2021, July 18). The West looks on as Africa opts for China's Digital Silk Road programme. *BusinessDay*. Available from: https://www.businesslive.co.za/bd/opinion/2021-07-18-the-west-looks-on-as-africa-opts-for-chinas-digital-silk-road-programme/.

Griffin, A. (2021, October 31). Facebook's Mark Zuckerberg summoned to appear before UK and Canadian parliaments. *The Independent*. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/mark-zuckerberg-parliament-uk-canada-westminster-dcms-select-committee-a8609996.html.

Holmes, A. (2021, April 3). 533 million Facebook users' phone numbers and personal data have been leaked online. *Business Insider*. Available from: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

Hruby, A. (2021). The digital infrastructure imperative in African markets. *Atlantic Council*. Available from: https://www.atlanticcouncil.org/blogs/africasource/the-digital-infrastructure-imperative-in-african-markets/.

Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society*, 5(3):1-13. https://doi.org/10.1177/2056305119863146.

McKinsey Global Institute (MGI). (2013, November 1). *Lions go digital: The internet's transformative potential in Africa*. Available from: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa.

Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, 42(3):329-348.

Nyabiage, J. (2021, March 21). Can China's 'digital silk road' secure dominant role in communications? *South China Morning Post*. Available from: https://www.scmp.com/news/china/diplomacy/article/3126280/can-chinas-digital-silk-road-ensure-dominant-role-information.

Perticone, J. (2018, March 23). Another congressional panel just summoned Mark Zuckerberg – and it could be the tip of the iceberg. *Business Insider*. Available from:

https://www.businessinsider.com/facebook-mark-zuckerberg-testimony-in-cambridge-analytica-2018-3.

Reiter, J. (2020). 4 ways digitisation can unlock Africa's recovery. *World Economic Forum*. Available from: www.weforum.org/agenda/2020/06/4-ways-digitisation-can-unlock-recovery-in-africa/.

Rikap, C. (2021). *Capitalism, power and innovation*. New York: Routledge.

Sawers, P. (2017, May 16). Google and partners commit $100 million to African broadband project CSquared. *VentureBeat*. Available from: https://venturebeat.com/2017/05/16/google-and-partners-commit-100-million-to-african-broadband-project-csquared/.

Shead, S. (2019, December 18). Facebook owns the four most downloaded apps of the decade. *BBC News*. Available from: https://www.bbc.com/news/technology-50838013.

Szczepański, M. (2020). *Is data the new oil? Competition issues in the digital economy*. European Parliamentary Research Service. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf.

The Economist. (2021). *The world's most valuable resource is no longer oil, but data*. Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Triolo, P. & Greene, R. (2021, May 8). Will China control the global internet via its Digital Silk Road? *Carnegie Endowment for International Peace*. Available from: https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857.

Velluet, Q. (2021, April 16). Can Africa salvage its digital sovereignty? *The Africa Report*. Available from: https://www.theafricareport.com/80606/can-africa-salvage-its-digital-sovereignty/.

Chapter 3

The Potential Economic Empowering Role of Cross-Border Data Flows in Legal Frameworks for Data Protection in Africa

Ayça Atabey

Introduction

Having an adequate legal framework for data protection is a necessity in today's data-driven world. Such a framework needs to be used effectively as a foundation for the execution of the daily commercial activities of businesses, and to ensure that the data processed is freely transferred on a global scale (World Economic Forum, 2020). In Africa, transferring data abroad as a requirement of daily commercial activities and using technological infrastructures located abroad are not harmonised. Barriers to cross-border data transfers can have significant economic consequences in today's data-driven world.

Debates

Although there are obvious benefits to cross-border data flows (World Economic Forum, 2020), there is a growing tendency to achieve data localisation practices (Ferracane, 2017). There are significant gaps among African countries' legal frameworks for data protection (Gwagwa & Wilton, 2014; Makulilo, 2015). The lack of harmonisation in data protection laws among African countries and a reluctance to work with cross-border data transfers by enforcing regulatory restrictions on data flows can have economic consequences, since data has become the new oil of today's world and is important for the digital trade/economy and international business (Casalini & López González, 2019; Manyika et al., 2016; OECD, 2019). The main debates around cross-border data transfers concern the lack of robust legal frameworks, perceptions of data localisation and sovereignty matters, and the realities of today's data-driven globalised economies, such as tech industries that render cross-border data flows a necessity.

Perspective

The EU General Data Protection Regulation ([GDPR] Legislation.gov.uk, 2016; see also European Data Protection Board, 2020) was adopted to serve a dual purpose: to facilitate the free flow of personal data within the European Union, while preserving the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data. The role of the Council of Europe's (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in international data transfers in countries outside of the EU can set a good example for African countries that want to enhance cross-border data flow regimes and help the digital economy ecosystem prosper in Africa. By looking at the examples in the EU and beyond in the context of Convention No. 108, and its amended version – Convention No. 108+ –

this paper aims to underscore that the economy can be severely affected by a lack of data protection laws or a lack of their effective enforcement.

A landscape of cross-border data flows is a must in a globalised world. Not having adequate legal frameworks that protect personal data might not only bear the risk of hampering the digital economy in any country, but it would also undermine individuals' rights to privacy and data protection, which are recognised under many legal instruments. Having a robust data protection legal framework could open the doors for opportunities in today's data-driven world. However, it may also hold potential risks that may exist to understand why countries lacking robust data protection legal frameworks (like the GDPR in the EU) tend to go towards requiring high standards, such as obtaining consent, or the potential reasons why they are inclined to favour data localisation practices and what legal and economic implications these can create.

If data protection rules are introduced or applied without having a true understanding of what lies at their essence, and without having taken other rights and freedoms that are recognised under international law into account, it could give rise to a situation in which we see data protection laws being used largely as a tool to impose fines, causing cumbersome procedures for data controllers.[3] This could also make regulatory compliance unreasonably difficult in practice and cause the benefits of digital trade and opportunities that a data-driven economy creates not to be materialised (Ferracane, 2017; World Economic Forum, 2020).

Such undesired consequences could also have serious legal and practical implications for users' rights and freedoms, not only in terms of data protection law, but also in other fields such as consumer protection law.[4] The reason for this is that, when data protection laws are merely applied according to the letter of the law but not its spirit, data subjects/users may be deprived of a free online ecosystem in which many options and benefits can be offered to them. Overall, it is crucial to remember that cross-border data flows are not only about data protection rules, but they also have implications for human rights, consumer protection, and international and constitutional law. This is why a lack of a sufficient understanding of the realities, necessities and dynamics of the data-driven economy in a globalised world might have significant legal implications outside of the economic sphere.

[3] The current Turkish DPA's decisions can be an example to such a restrictive approach.
[4] For the intersection between consumer protection laws and cross-border data transfer laws and policies, see, for example, Casalini et al. (2021).

The Current Data Protection Legal Framework in Africa

The 2018 DHL Global Connectedness Index (DHL, 2018) indicates that African countries lag behind, with considerably lower averages of connectedness. Not much seems to have changed, as the 2020 index demonstrates that a majority of African countries are ranked at the bottom of the list (DHL, 2020). Africa could benefit from opportunities by investing in taking steps towards digital development (including, but not limited to, the introduction and effective implementation of legal frameworks) that would foster the digital economy and protect individuals' rights and freedoms. Data-driven technologies present a chance to open new doors for fast economic growth, innovation, job creation and access to services that would have been unthinkable only a few years ago (World Bank, 2020). However, despite these opportunities, there is also "a growing 'digital divide', and increased cyber risks, which need urgent and coordinated action to mitigate" (World Bank, 2020). There are some recent developments in Africa in the context of data protection laws, yet they do not seem to be sufficient to have a robust application of the frameworks that is similar to the European context, which has the GDPR and Convention 108+.

The African Union (2020a) Convention on Cybersecurity and Personal Data Protection (Malabo Convention) aims to establish a harmonised continental data protection legal framework. The Digital Transformation Strategy for Africa aims to utilise digital technologies and foster innovation to transform African societies and economies to promote Africa's integration, generate inclusive economic growth, stimulate job creation, break the digital divide, and eradicate poverty for the continent's socio-economic development and to ensure Africa's ownership of modern tools of digital management (African Union, 2020b). The Digital Transformation Strategy mirrors the support of the ratification of the Malabo Convention and the Council of Europe Budapest Convention on Cybercrime (Council of Europe, 2004; see also Abraha, 2020) during the 2020 session of the African Union (Kayihura, 2020). Continental Free Trade Agreement demonstrates important steps towards collaboration between African countries and raises hopes for the potential to open the doors of the region's economic potential (Kayihura, 2020).

Yet, there are uncertainties as to the effectiveness of a harmonised framework as there are significant differences among the countries' legislations in Africa. Also, the current practices seem to have a favour towards data localisation practices. In 2014, Nigeria enacted the "Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)," that set out some restrictions on cross-border data transfers and required that all subscriber, government, and consumer data be stored locally (Cory, 2017). In 2016, Kenya published its National Information and Communications Technology Policy draft, aiming to update the government's efforts to modernize ICT-relevant economic policy (Cory, 2017).

Despite the many mentioned benefits of data localization, it also has significant costs (Bauer et al., 2014). Accordingly, experts argue that broad data localization requirements would pose a threat for Africa's global competitiveness and economic development (Kayihura, 2020). Africa's future in a data-driven world might depend on harmonisation of the modernised laws that provide adequate protection of personal data while allowing cross-border data flows (Kayihura, 2020).
An example can be given from the Internet of Things (IoT) ecosystem, which is believed to have positive effects for both advanced industrialised economies and emerging economies. Data localisation practices, on the other hand, are expected to have a significant negative effect and to undermine GDP growth, employment, trade and investment in the context of IoT (GSMA, 2021). Data localisation is also argued to have a considerable negative effect on employment, causing job losses, for example around 182 000 in South Africa (GSMA, 2021:3).

A study by the European Centre for International Political Economy (ECIPE) on the economy-wide effect of data localisation and data protection laws in the European Union points out diminished innovation and productivity and finds that restrictions on the movement of data can result in "a major misallocation of resources and threaten the continent's productivity and competitiveness" (Bauer et al., 2016). In the African context, data localisation practices could have even more serious effects if they proceed in a manner "unlike [that of] the European Union, [as] the African continent lacks a common and enforceable data protection regime" (Kayihura, 2020). Today, many African countries lack a unified data protection legal framework and, where relevant, rely on civil, criminal, and constitutional laws and individual rights of privacy (Kayihura, 2020). As mentioned before, African countries currently have different pieces of legislation that are not aligned with each other. Fifty-four percent of African countries have specific data protection laws, whereas 17% are in the drafting process, and 30% of them do not have any specific data protection law (World Economic Forum, 2020). The fragmented legal landscape of data protection in Africa is likely to make regional or international cooperation difficult. Therefore, it might be beneficial for African countries to enact robust national data protection laws and then become part of a harmonised framework (continental, regional or international) (World Economic Forum, 2020). Moreover, having a robust data protection legal framework in place is aligned with the concept of digital sovereignty, as it would allow individuals to have control over their data (Vahisalu, 2019). In addition to the economic and data protection (individuals having control over their data) aspect, laws on cross-border data transfers are also important for the fight against cybercrime. Data sharing enables secure data sharing and helps stakeholders in the fight against online crimes, with a focus on legislation and law enforcement relating to abuses such as cybercrime, fraud and harmful discrimination (World Economic Forum, 2020).

Implications

Legal frameworks for data protection and the use of data are driving or shaping many aspects of our economies and societies. In an increasingly data-driven and globalised world, businesses have become reliant on the seamless flow of cross-border data transfers. Transatlantic data flows play an important role in the world's economy, and African countries are no exception to this. Innovation, data-driven economies, and transatlantic trade are facilitated by cross-border transfers of data. This is because global commerce and digital trade are enabled by the free flow of personal data (Casalini et al., 2021; US Congressional Research Service, 2020). Restrictions on the cross-border transfer of personal data could put commercial life and the overall economic state in Africa to a significant test. In the global digital age, where significant amounts of trade and commerce take place online and across multiple jurisdictions, cross-border data transfers are necessary for a dynamic economy (Singh, 2017).

In its report, the UNDP (2021) highlights the role geopolitics and other challenges play in the fragility of the international system. The report underscores protectionism and nationalism, and there were several different aspects that had negative impacts around the world. It further argues that there is a need for "data to flow across borders to drive industries, opportunities, and sectors" (UNDP, 2021). Establishing an adequate level of data protection through robust legal and policy frameworks is crucial. African countries should have adequate national legal frameworks in place to allow data subjects to enjoy their right to data protection and privacy. Cross-border data transfers should generally be allowed, although with potential exceptions including for sensitive personal data (e.g., personal data about one's sexual orientation, political views, health, etc.). Transferring such data should be subject to an additional legal basis, such as the explicit consent of the data subject.

There are different reasons for countries' efforts to regulate data flows. On the one hand, it could be to protect the privacy of individuals and their personal data. On the other hand, countries could restrict the cross-border data flows or require that this data "be stored on local (domestic) servers, in order to meet other regulatory objectives, such as access to information for auditing purposes" (López González, 2018). Governments could also adopt a restrictive approach towards data flows when it comes to sensitive personal data or sensitive information when looked at from a national security perspective. Yet several countries have also been observed to be increasingly regulating data flows with the aim of "helping develop domestic capacity in digitally-intensive sectors, as a form of digital industrial policy" (Gonzalez, 2018).

Once countries take steps in their own national legal frameworks to ensure data protection, establishing effective cooperation among African countries on a supranational level might be triggered. It is also important to note that the introduction of robust laws is not enough. There is a need to strengthen enforcement authorities to be able to implement these laws in the best possible way and to encourage inactive or non-operational authorities to be proactive (Ademuyiwa & Adeniran, 2020). Cooperation on issues relating to cross border data flows does not have to be limited to a regional context, it can also be strengthened by considering being a party to the other frameworks such as the Convention 108+ in the EU. Different options should be considered to explore the best option and an impact assessment should be carried. Such cooperation would ensure more certainty and trust for data protection, which could have a positive effect on the digital economy in Africa. African countries could explore the possibility of reaching an agreement on the adequacy of other countries' data protection frameworks where the respective legal frameworks provide adequate protection for the protection of data. Although having a harmonised and robust data protection legal framework could be a difficult task for African countries, when realities and opportunities are taken into account in today's data-driven world, we could say that it is worth it.

References

Abraha, H. H. (2020, July 6). How African countries can benefit from the emerging reform initiatives of cross-border access to electronic evidence. *Cross-border Data Platform*. Available from: https://www.crossborderdataforum.org/how-african-countries-can-benefit-from-the-emerging-reform-initiatives-of-cross-border-access-to-electronic-evidence/?cn-reloaded=1.

Ademuyiwa, I. & Adeniran, A. (2020). *Assessing digitalization and data governance issues in Africa*. CIGI Papers No. 244. Waterloo, Canada: Centre for International Governance Innovation. Available from: https://www.cigionline.org/static/documents/documents/no244_0.pdf.

African Union. (2020a). *Convention on cyber security and personal data protection*. Available from: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

African Union. (2020b). *The digital transformation strategy for Africa (2020-2030)*. Available from: https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

Bauer, M., Ferracane, M. F., Lee-Makiyama, H. & Van der Marel, E. (2016). *Unleashing internal data flows in the EU: An economic assessment of data localisation measures in the EU member states*. ECIPE Policy Brief, No 03/2016. Belgium, European Centre for International Policy Economy. Available from: https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

Bauer, M., Lee-Makiyama, H., Van der Marel, E. & Verschelde B. (2014). *The costs of data localisation: A friendly fire on economic recovery*. ECIPE Occasional Paper, No. 3/2014. Belgium: European Centre for International Political Economy. Available from: https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf.

Casalini, F. & López González, J. (2019). *Trade and cross-border data flows*. OECD Trade Policy Papers 220, OECD Publishing.

Casalini, F., López-González, J. & Nemoto, T. (2021). *Mapping commonalities in regulatory approaches to cross-border data transfers*. OECD Trade Policy Papers, No. 248. Paris: OECD Working Party of the Trade Committee. Available from: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)15/FINAL&docLanguage=En.

Cory, N. (2017, May 1). Cross-border data flows: Where are the barriers, and what do they cost? *Information Technology & Innovation Foundation*. Available from: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data*. European Treaty Series, No. 108. Available from: https://rm.coe.int/1680078b37.

Council of Europe. (2004), *Budapest Convention and related standards*. Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

DHL. (2018). *Global Connectedness Index*. Available from: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-gci-2018-ten-key-take-aways-en.pdf.

DHL. (2020). *Global Connectedness Index*. Available from: https://www.dhl.com/content/dam/dhl/global/dhl-spotlight/documents/pdf/spotlight-g04-gci-2020-highlights.pdf.

European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Available from: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en.

Ferracane, M. F. (2017). *Restrictions to cross-border data flows: A taxonomy*. European Centre for International Political Economy (ECIPE). Available from: https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/.

GSMA. (2021). *Cross-border data flows: The impact of data localisation on IoT*. Available from: https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf.

Gwagwa, A. & Wilton, A (2014). *Protecting the right to privacy in Africa in the digital age*. IDRC/CRDI. Available from: https://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf.

Kayihura, R. (2020). Cross-border data flows: The key to Africa's success in a data-driven world. *LinkedIn*. Available from: https://www.linkedin.com/pulse/cross-border-data-flowsthe-key-africas-success-world-robert-kayihura/.

Legislation.gov.uk. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available from: https://www.legislation.gov.uk/eur/2016/679/contents#.

López González, J. (2019). Hitchhiker's guide to cross-border data flows. *OECD*. Available from: https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/.

Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*, 31(1):78-89.

Manyika, J., Lund, S. Bughin, J., Woetzel, J. Stamenov, K. & Dhingra, D. (2016). Digital globalization: The new era of global flows. *McKinsey Global Institute*. Available from: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

OECD. (2019). Trade in the digital era. *OECD Going Digital Policy Note*. Paris: OECD. Available from: https://www.oecd.org/going-digital/trade-in-the-digital-era.pdf.

Singh, A. (2017). *Data without borders: How to manage cross-border data transfers in South Africa*. Available from: https://altadvisory.africa/2017/11/07/data-without-borders-manage-cross-border-data-transfers-south-africa/.

UNDP. (2021). *Enabling cross-border data flow: ASEAN and beyond*. Available from: https://www.undp.org/publications/enabling-cross-border-data-flow-asean-and-beyond.

US Congressional Research Service. (2020). *Data flows, online privacy, and trade policy*. CRS Report No. R45584. Available from: https://fas.org/sgp/crs/misc/R45584.pdf.

Vahisalu, R. (2019, May 15). Digital sovereignty: The key to safeguarding Africa's booming digital economy. *Global Voice Group*. Available from: https://www.globalvoicegroup.com/digital-sovereignty-the-key-to-safeguarding-africas-booming-digital-economy/.

World Bank (2020). *The Digital Economy for Africa Initiative (DE4A)*. Available from: https://www.worldbank.org/en/programs/all-africa-digital-transformation.

World Economic Forum. (2020). *A roadmap for cross-border data flows: Future-proofing readiness and cooperation in the new data economy*. White Paper. Available from: http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

Chapter 4

Leveraging Digital and New Technologies for Development in Africa's Emerging Economies with Significant Structural Constraints

Ngwinui Belinda Azenui

Introduction

The use of digital technologies and internet connectivity, commonly referred to as the fourth industrial revolution, has grown very rapidly in Africa in recent decades. The fourth industrial revolution has two components: progress in the integration of physical capital, and digital production and consumption. In essence, the recent revolution is about digitalisation and the integration of digitisation with physical production tools, such as sensors, artificial intelligence (AI), big data analytics, robotics, and the internet (Naudé, 2018).

When information is converted into digital formats that can be processed by a computer, this opens multiple opportunities, especially in e-government, finance, access to knowledge, and global connectivity in general. However, if not adequately regulated, the real risks – including inequality of voice and income, invasion of privacy, monopolisation, limited data control, less secure employment due to robotisation, and tax evasion and avoidance – would greatly outweigh the benefits (Stiglitz, 2019). For example, Twitter set out to democratise publishing, but those with money can dominate through bots. Therefore, it is worth paying attention to the relevance of these changes in growth and development, and in the protection of digital data and the rights of citizens in Africa.

Africa has the potential to tap into the opportunities and benefit substantially from the digital age but needs to pay attention to sovereignty over its own digital data. This would enable Africa to protect its citizens from manipulated media and ensure democratic participation. In addition, to achieve sustainable growth in the digital age and overcome the difficult problems posed by new technologies, African countries need to overcome structural constraints, build reliable institutions, and build capacity and capabilities that would enable its economies to absorb and utilise the opportunities that new technologies create.

Debates

Summary of Main Debates

Many scholars believe that digital transformation and connectivity are a sure-shot route through which African economies can emerge and leapfrog during the fourth industrial revolution (amongst others McAfee & Brynjolfsson, 2017; Newfarmer et al., 2018). There is evidence that

digitalisation has positive implications for education, finance and ICT applications in agricultural development (Angus et al., 2004; Friederici et al., 2017; Lokeswari, 2016). Specifically, there are many success stories in Kenya and other African countries in the area of digital payment systems. However, other scholars are not so optimistic due to the structural constraints that are still a main concern in many African countries (among them Naudé, 2018; Rodrik, 2015; Stiglitz, 2014, 2019). Their major concern is the means through which African countries will utilise new technologies and evolve their economies without transitioning from an agrarian economy to manufacturing and other industries. Scholars see digital inequality that stems from unequal control over data as a major problem for economic development (Fisher & Streinz, 2021).

Structural Change and the Role of Manufacturing

Sustained development requires the transformation of the structure of an economy as a concomitant process of growth, as asserted by the old structuralists and recent development economists, including Maddison (2001), Ocampo (2005), Rodrik (2015), Stiglitz (2014), among others. In other words, changes in the structure of the economy are necessary for economic growth and development, and structural change is not just a by-product of economic growth. Evidently, today's developed countries and developing countries experiencing growth miracles in Asia have historically moved away from traditional societies towards modernisation: a transformation of their economies first from agriculture to manufacturing or other industries, and then to services.

Basically, a reallocation of labour from a lower-than-average productivity sector (such as agriculture) to high-productivity activities (such as manufacturing) leads to higher average productivity levels, called the static effect of structural change, and raises average productivity growth over time, known as the dynamic structural change bonus (Kaldor, 1957; Verdoorn, 1949). Successful structural change has been associated with manufacturing and other industries because manufacturing and labour-intensive industries have the capacity to absorb excess labour and have positive externalities (Rodrik, 2016; Szirmai & Verspagen, 2015). Other mechanisms through which manufacturing serves as an engine of growth have been established around dynamic economies of scale, learning by doing, as well as direct and indirect backward and forward linkages between manufacturing and other sectors (Azenui & Rada, 2021). Therefore, how are African countries planning to emerge in the digital age without manufacturing and basing such emergence on commodity trade and new technologies that are not sourced in Africa? What structural constraints impede this emergence?

Structural Constraints in Africa

The main structural impediments limiting Africa's ability to actively and democratically participate in the digital economy include poor infrastructure, weak and unreliable institutions, limited financing, and limited data. According to Stiglitz (2019), what separates developing countries from developed countries is not just a disparity in resources, but a disparity in knowledge and institutions. Good infrastructure and dependable working institutions – that enforce laws governing the proper treatment of data and digital assets and that facilitate growth – are the foundation for investment and business growth, and the backbone of digital sovereignty. This would enable African countries to absorb the benefits of digitalisation. For instance, if internet or connectivity reaches the poor and underprivileged in villages without electricity or food, how would such indigenes charge their phones or feel the need to manipulate the internet if they are hungry or have no lights? Evidently, despite rapid growth in internet connectivity in Africa in recent decades, the growth miracle and leapfrogging are farfetched ideals.

Small and medium-sized businesses are the foundations and drivers of growth, and most entrepreneurial start-ups need capital. Without financing, business ideas cannot be realised, and so limited financing poses a great challenge. Finally, data in most African countries are collected and managed by international organisations and multilateral industries, which do not own or have data centres locally. For example, some African government officials still use Gmail and Yahoo accounts, and the servers of such accounts are managed by the United States and other Western countries. African researchers get most secondary data about African countries from the United Nations, the World Bank World Development Indicators or from the International Labour Organization (ILO). How then can we talk about protection and digital sovereignty when we do not own or have control over our information?

Perspective

It is puzzling to see the widespread ideology or ambition among young Africans who believe that digitalisation and connectivity would serve as an instrument to achieve a wide range of social and economic development goals in Africa. African countries are going to miraculously transition from an agrarian to services economy, with high productivity and high value-added, regardless of invasive economic and structural constraints. I think energies rather should be geared towards the following: the application of new technologies in agriculture to improve agricultural productivity and reduce the reliance on land; the use of artificial intelligence and robots to supplement workers in industries; the structural transformation of African economies to labour-intensive industries and services; the ownership and protection of African data and digital assets in the internet age that translates to digital sovereignty; and active participation in the discussion and development of new technologies by African countries.

There are many questions that linger when digital transformation, digital sovereignty, and its application in African countries are discussed and implemented by researchers and policymakers. How does digital transformation translate into the structural change and growth of African economies? What is the role of the manufacturing sector, and can African economies emerge in the digital age without developing a solid manufacturing sector, given that manufacturing is the engine of growth – as postulated by the Kaldor and Verdoorn law, and as shown by the development pathways of developed countries in the West and Asia? If manufacturing has a role, what types of manufacturing industries are best suited for Africa? How about skilled and high value-added services? Many scholars on Africa generally agree that African countries need better policies and institutions to reap the benefits of globalisation and digitisation. Exactly what policies and institutions are needed, and how do we ensure that all that talk turns into real action? How do we design policies for Africa by Africans, taking into consideration evidence from African countries? Where are priorities such as electrification and poverty reduction? How do African citizens, especially marginalised communities, control their freedom against manipulated media in the digital age? How does the entrepreneurial start-up scene participate in the digital age by using new technologies for their growth, and how does that translate into development? The list of these questions continues when digital sovereignty and the use of new technologies for development in the African context are considered in the midst of structural constraints, colonial history and power dynamics with the West.

Implications

Well-defined rules and policies, as well as institutions to enforce the rules and protect the rights of citizens, are necessary for Africa to reap the benefits of digitisation and innovation. It is important for policymakers to bear in mind that new technologies expand possibilities, but often lead to a new equilibrium with more inequality. Therefore, Africa has to revise its strategies and focus on basic important targets, such as collecting and protecting its own data, drafting practical regulations for digital technologies, or finding practical ways to tax the digital economy, alleviate poverty, and change the structures of its economies, especially resource-based economies.

The starting point of regulation for Africa is data ownership. Currently, most of Africa's data is collected and owned by international organisations and foreign multilateral firms. The privacy issues related to such foreign ownership of local data are enormous. Africa should strive to achieve data sovereignty through data localisation and the creation of data centres in Africa. Put differently, African governments need to establish laws and governance structures within Africa, and pass data sovereignty laws around the storage and control of Africa's data. Therefore, if Africa wants to participate actively in the digital age, it must have sovereignty over its own digital data

and discuss its colonial histories and power dynamics that are being maintained with Western countries in the global North. Bonilla (2017) asserts that sovereignty should be questioned because it is rooted in the Western history of colonialism and imperialism and still deeply encoded in the structures and discourses of international law. This colonial history has been one of the main setbacks for structural change and economic growth in Africa.

It is obvious that more organisations are aiming to help Africa design its policies without taking into consideration evidence from Africa, which leads to inadequacy in foreign support. For instance, the Washington consensus and/or the structural adjustment programme designed by the IMF for African countries failed due to inadequacies in design and implementation. Particularly, Cameroon suffered from its effect for about two decades. However, the IMF and the West alone cannot be blamed for the failure of these programmes; dictatorship, tribalism and weak institutions are strong forces against any such programmes for Africa. Africa's solutions to African problems will be ideal, but I think the sponsors always worry that their money would be embezzled. So, sponsors try to advise and direct projects using their methods, which have not been tested in the African context.

The education of indigenes and citizens during the digital age helped the underprivileged find a voice and speak up. This enabled citizens to control their freedoms against manipulated media and to participate democratically. For example, in a remote village in Zimbabwe, villagers used toilet holes (latrines) dug by an NGO to store grains. Such situations could be avoided if local communities are taught the purpose and functions of the amenity. Teaching locals about their privacy and rights is therefore essential in helping them have a voice.

Last but not the least, government intervention through sectoral, industrial and regulatory policies is necessary to direct innovation and digitalisation. States should set rules that govern the use of digital technologies and enforce them. Rules should aim to protect the rights and privacy of citizens and ensure transparency. Intervention must target aspects of the digital age that facilitate the development of productive capabilities and capacities, ease macroeconomic and structural constraints, as well as shape and direct structural transformation (Azenui & Rada, 2021). To reiterate, digital and structural transformation should go hand in hand with regulations to avoid destructive effects.

New technologies and innovation offer enormous opportunities in education, finance and increasing productivity in agriculture, but Africa has to be wary of the threats these technologies pose in terms of digital sovereignty, cybercrimes, increased inequality and labour-replacing robots, and thus increased unemployment and vulnerability to global shocks. Africa needs to lead

and direct its own economic, structural and digital transformation process, paying particular attention to and understanding how technology interacts with the institutions, socio-economic structures and informality that exist in African countries.

References

Angus, L., Snyder, I. & Sutherland-Smith, W. (2004). ICT and educational (dis)advantage: Families, computers and contemporary social and educational inequalities. *British Journal of Sociology of Education*, 25(1):3-18.

Azenui, N.B. & Rada, C. (2021). Labor productivity growth in sub-Saharan African LDCs: Sectoral contributions and macroeconomic factors. *Structural Change and Economic Dynamics*, 56:10-26.

Bonilla, Y. (2017). Unsettling sovereignty. *Cultural Anthropology*, 32(3):330-339. https://doi.org/10.14506/ca32.3.02

Fisher, A. & Streinz, T. (2021). Confronting data inequality. International Law and Justice Working Paper No. 2021/1. New York, NY: Institute for International Law and Justice, New York University School of Law. Available from: https://www.iilj.org/wp-content/uploads/2021/04/Fisher-Streinz-Confronting-Data-Inequality-IILJ-Working-Paper-2021_1.pdf.

Friederici, N., Ojanpera, S. & Graham, M. (2017). The impact of connectivity in Africa: Grand visions and the mirage of inclusive digital development. *The Electronic Journal of Information Systems in Developing Countries*, 79(2):1-20.

Kaldor, N. (1957). A model of economic growth. The Economic Journal, 67(268):591-624.

Kaldor, N. (1966). *Causes of the slow rate of growth of the United Kingdom*. London, UK: Cambridge University Press.

Lokeswari, K. (2016). A study of the use of ICT among rural farmers.*International Journal of Communication Research*, 6(3):232-238. Available from: http://www.ijcr.eu/articole/325_03%20K%20LOKESWARI.pdf

Maddison, A. (2001). *The world economy: A millennial perspective*. Paris: Development Centre of the Organisation for Economic Cooperation and Development.

McAfee, A. & Brynjolfsson, E. (2017). *Machine, platform, crowd: Harnessing our digital future*. New York, NY: W.W. Norton & Company.

Naudé, W. (2018). Brilliant technologies and brave entrepreneurs: A new narrative for African manufacturing. *Journal of International Affairs*, 72(1):143-158.

Ocampo, J.A. (2005). The quest for dynamic efficiency: Structural dynamics and economic growth in developing countries. In *Beyond reforms, structural dynamics and macroeconomic vulnerability* (pp. 3-44). Edited by Ocampo, J.A. Stanford, CA: Stanford University Press.

Newfarmer, R., Page, J. & Tarp, F. (2018). Industries without smokestacks: Industrialization in Africa reconsidered. WIDER Policy Brief 2018/2. Helsinki: UNU-WIDER.

Rodrik, D. (2015). Premature deindustrialization. NBER Working Paper No. 20935. Cambridge, MA: National Bureau of Economic Research.

Rodrik, D. (2016). An African growth miracle? *Journal of African Economy*, 27(1):10-27.

Stiglitz, J.E. (2014). Why learning matters in an innovation economy. *The Guardian*. Available from: https://www.theguardian.com/business/2014/jun/09/why-learning-matters-innovation-joseph-stiglitz.

Stiglitz, J.E. (2019). *Globalization, development, changing technology: Achieving sustainable and equitable growth*. PowerPoint presentation, Tokyo, 27 August.

Szirmai, A. & Verspagen, B. (2015). Manufacturing and economic growth in developing countries, 1950–2005. *Structural Change and Economic Dynamics*, 34:46-59.

Verdoorn, P. (1949). Fattori che regolano lo sviluppo della produttiva del lavoro. *L'industria* 1:3-10.

Chapter 5

If Health is Wealth, Where is Africa's Health Data?

Benjamin Akinmoyeje

Introduction

About 80% of health data platforms in Nigeria are hosted in the cloud, which is based outside the territory of Nigeria. This is according to observational data derived from discussions with digital health experts in Nigeria (Report Linker, 2021). The proverbial saying, "health is wealth", dictates that having good health is as important as acquiring riches, and development is strongly tied to the wealth of a nation or an individual. In recent times, data also has become the new oil, according to a publication by *The Economist* (2017): this is synonymous with the new wealth. The important point here is that our health and data are valuable, and more valuable when you combine the two. This article asks the question, where is the health data of many African countries (e.g., Nigeria) located, and what are the implications of that location for the sustainable digital development of the region?

The term digital development has been defined succinctly as the digital information technologies to improve community interventions towards social and economic development (ICTWorks, 2021), and the World Bank envisages digital technologies as a tool with a unique potential to drive economic growth by creating more services and jobs for the large numbers of Africa youths (World Bank, 2021).

Recently, digital health has been the buzzword (International Telecommunication Union, 2020) for a tool that can help accelerate most of the desired outcomes of these organizations' investment in many of their sponsored interventions in Nigeria and other African countries. The World Health Organization defines digital health as "the use of information and communication technology to support health and health-related fields" (World Health Organization [WHO], 2019), whereby citizens can access healthcare over the Internet or via mobile phones. Hence, there is increased investment in ICT infrastructure to help developing economies leapfrog in areas with limited healthcare infrastructure, deliver quality healthcare, provide healthcare access to marginalised communities, and provide the needed data for decision making (DIAL, 2020; Ehimuan, 2021; Iacopino & Meloan, 2017; ITU Publications, 2021; World Bank, 2017).

Nevertheless, beyond investment and the adoption of ICT, the systems approach to the adoption of digital development should stimulate the overall strengthening of the entire healthcare system of Nigeria, as it aligns with the overall goals of the development organisation. However, with the

routine programme implementations approach being the mainstream method of implementing healthcare intervention, it is difficult to actualise sustained development in the region, especially in local digital development. One such is the local hosting of digital health data in Nigeria.

Main Debate on Digital Health

Limited Capacity: Nigeria's information technology sector has experienced a drastic boom in the past ten years, starting with the Lagos start-up ecosystem led by the Co-Creation Lab (Ramachandran et al., 2019). The spread of the start-up fever has been viral. This growth has affected almost every sector in Nigeria. Entertainment, banking, agriculture and healthcare have benefited from the Nigerian start-up ecosystem, but the Nigerian health system can benefit from a more enabling environment (Ehimuan, 2021). However, most of the digital health interventions implemented in Nigeria have been by international organisations and, even when locally inspired, are still foreign-led. The foreign-led approaches have been a serious concern for local digital development advocates (Erondu et al., 2021). Interest in data science has gained popularity, and the creation of organisations such as Data Science Nigeria (2020) has helped accelerate the building of local skills, especially among unemployed Nigerian graduates. A new crop of talent can add value and bring quality insights from existing Nigerian health data.

In the immediate future, hosting on GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) cloud centres may be cheaper due to the economies of scale for subscribers in Nigeria. But many years of investment by these big-technology companies in Nigeria to increase their capacity to harvest data from Nigeria have only increased the companies' profits margins, and not Nigeria's capacity to host her health data. In contrast, despite all the local challenges, local providers are still rendering quality services and building local workforce and capacities to support and innovate to meet the current data and future eHealth data needs (Onwuegbuchi, 2020). The common narrative is that Nigeria has limited infrastructure to support its critical health data (Cory & Stevens, 2020). It is challenging to develop the digital health capabilities in the country when the existing ICT infrastructure and skills developed in recent years are left without patronage and investment (Onwuegbuchi, 2020). International development organisations and NGOs with a mandate to support development efforts work in multiple countries, so it is economically viable to host in the international cloud. However, if they want to be true to their mandate they must invest in local efforts, such as local cloud service providers.

Sensitive nature of health data: The sensitive nature of health data requires adequate attention is paid to ensuring the integrity, protection, and security of the data, which is paramount. A breach of Nigerian health data can significantly affect the lives of many Nigerians, as there have been similar cases of data breaches. It was reported that there was a case in Singapore, in which HIV

patients' details were exposed to the public (Leyl, 2019), and there have been unethical applications of AI algorithms to population health data. Finally, to encourage local cloud capacity to handle health data, government agencies and businesses collecting health data must make use of local cloud services to help develop their ability to manage health data, such as biometric data. The availability of data provides the needed information for improved health care for the population.

The patronage of cloud services in Nigeria will enhance digital development as these companies expand, especially for the underserved communities across Nigeria. Localisation provides the needed high-speed access to health data, irrespective of the region in Nigeria where it is required. Location is inconsequential: Ordinarily, customer agreements stipulate that host companies do not access data on their servers. However, health data is different from other types of business data; it requires special considerations, and a country should have proper control of its citizens' health data. The new Nigerian "National Cloud Computing Policy" stipulates a second-level data classification for health data hosting in the cloud, but no details are provided on the handling of such data. The policy document only provides incentives to motivate the local hosting of health data, but no regulation to enforce this hosting (National Information Technology Development Agency [NITDA], 2019).

Perspective

Issues arise regarding the systems thinking approach in African digital development (digital health), as many of the interventions by donor agencies and development partners are focused on programme or project implementations, and this approach ignores other stakeholders or supporting systems necessary for the sustainability of the projects (Van Velthoven & Cordon, 2019). Jonathan Whiteside (2020), in his article titled "A Systems Thinking Approach to Digital Transformation", defines the systems thinking approach as the holistic idea of "the whole being more than the sum of its parts". Digital health interventions that require health data should consider direct functions and stakeholders, as well as indirect ones; the development organisations' digital development interventions must be seen as part of a holistic process of development, and hence must be willing to support all the pillars that will enhance the sustainability of their programmes or projects in Nigeria. A typical example is the implementation of an electronic medical record (EMR) system in a health facility; it is not enough to just deploy the hardware, train the staff and leave. It will be wise to ensure that IT maintenance workers in the community are carried along, so that when there is a need for minor repairs, local IT professionals such as data analysts, software engineers and technicians can support the health facility. This collaboration can be extended to Internet service providers, power backup providers, and many other stakeholders necessary for successful digital development. The typical project

implementation only deploys technology solutions and expects local ownership by direct beneficiaries. These projects often become redundant once the support from the implementer stops. The engagement of a broader stakeholder group at every phase of the project implementation gives a sense of ownership that breeds sustainability and ownership by the community.

Also, localisation and sovereignty have largely been ignored. The localisation of health data allows for the development of local content and innovation. Easy access to data for research for local circumstances and sources in the case of disease outbreaks; thereby making national authority capable to manage healthcare crisis (Hansen, J. et al., 2021). Localization provides the opportunity for local values are given top priority in the creation of templates to collect health data, which ordinarily may not always be at the forefront of health data and digital development.

Data localisation provides requirements for the cross-border transmission of data. In law, it is also an issue of jurisdiction over data and where it is currently hosted. There are risks to having the country's health data in foreign jurisdictions. One of such risks relates to legal implications, as in which laws will supersede when there is a contention – Nigerian law, or the host country law? Of the many digital health interventions currently making headlines in Nigeria, emphasis has been on the effect of the digital tools without some consideration for the implications of these interventions in data ownership, location and access. The proper clinical data ownership model is paramount in this season of scrambling for digital information or data occurring in Africa by big techs. The value of health data is being ignored, but health data will play a significant role in the future. Hence, it should not be harvested without the necessary controls or licensing agreements on its ownership. In most cases, data harvested from Nigeria or other part of Africa will help build models and algorithms in health systems that will be useful for the fourth industrial revolution. If proper ownership models or principles are not adopted, it may result in the digital colonisation of our health data (Coleman, 2019).

Most of the interventions follow guidelines such as digital development principles (*Principles for Digital Development*, 2017), which are copied or inspired by design principles from the UK (GOV.UK, 2012) and the digital investment principles launched in Berlin on 16 October 2018 (Digital Investment Principles, n.d.). Though the *Principles for Digital Development* well intended and good, it is important to pay significant attention to encoding African values such as Ubuntu, which share the principle of African humanism described as 'I am because of who we all are' (Mugumbate & Nyanguru, 2013), into the information communication technologies used for development tools to collect our health data. The inherent values will ensure that, when

innovations such as artificial intelligence are implemented, we are able to derive maximum benefits from such interventions without unintended consequences from existing biases.

Implications for Policy or Future Research

The current trend of hosting Nigerian health data on platforms hosted outside of Nigeria does not give adequate incentives for local digital development; it only makes Nigeria's health sector a super user or consumer of western solutions. None of these outcomes align with the goals of many international development agencies working in Nigeria, nor with the digital economy transformation agenda of the present Nigerian government. Although the government's policy documents support local cloud hosting services, these are yet to be enforced or operationalised. The policy implications of these ongoing trends will make digital development unachievable, especially in the health system, and there thus is a need in Nigeria for an urgent review of the templates used to approach digital development investments.

The governments of developing countries such as Nigeria that receive aid need to renegotiate the implementation of digital health interventions with the entire healthcare system in perspective. International aid agencies should be motivated to engage with local companies that can support the implementation of interventions. In this way, sustainable digital health development can be achieved.

The increasing profile of data as a vital component of future economic growth also demands that a nation desirous of growth must be in control of her own data, in line with data sovereignty and data localisation. Therefore, the necessary incentives or subsidies must be given to local companies to develop the capacity required to host country-generated content. Investments in data centres and other digital development infrastructure by international development agencies should be encouraged. Currently there are lots of initiatives, such as the Lagos cloud computing hackathon (Lagos State Science Research & Innovation Council [LASRIC], 2021), to encourage local cloud companies. The government of Nigeria must patronise local service providers, especially those who incorporate the principles of data localisation and sovereignty. Suggestions about a new business model for big tech companies in Nigeria are that they should encourage the establishment of their data centres either regionally or locally in Nigeria, and that they should help keep local data local, despite being foreign companies. In the future, useful research to conduct would be on the effect of foreign-developed digital platforms on African digital development.

References

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race and Law*, 24(2):417. Available at: https://repository.law.umich.edu/mjrl/vol24/iss2/6.

Cory, N. & Stevens, P. (2020). *Building a global framework for digital health services in the era of COVID-19*. Information Technology & Innovation Foundation. Available from: https://itif.org/publications/2020/05/26/building-global-framework-digital-health-services-era-covid-19.

Data Science Nigeria. (2020). Available from: https://www.datasciencenigeria.org/.

DIAL (Digital Impact Alliance). (2020). *Unlocking the digital economy in Africa: Benchmarking the Digital Transformation Journey* Available from: https://digitalimpactalliance.org/wp-content/uploads/2020/10/SmartAfrica-DIAL_DigitalEconomyInAfrica2020-v7_ENG.pdf.

Digital Investment Principles. (n.d.). *The principles of donor alignment for digital health*. Available from: https://digitalinvestmentprinciples.org/.

Ehimuan, J. (2021). *What my decade at Google taught me about Africa's tech future*. The Africa Report. Available from: https://www.theafricareport.com/90339/what-my-decade-at-google-taught-me-about-africas-tech-future/.

Erondu, N.A., Aniebo, I. Kyobutungi, C., Midega, J,. Okiro, E. & Okumu, F. (2021). Open letter to international funders of science and development in Africa. *Nature Medicine*, 27:742-744. doi:10.1038/s41591-021-01307-8.

GOV.UK. (2012). *Government design principles*. Available from: https://www.gov.uk/guidance/government-design-principles.

Hansen, J. et al., (2021). Assessment of the EU Member States' rules on health data in the light of GDPR. *DG Health and Food Safety* Available from:https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.

ICTWorks (2021). *Practical insights on digital development*. Available from: https://www.ictworks.org/tag/digital-development/#.YP0SFI4zbIV.

International Telecommunication Union. (2020). *Handbook: Digital health platform: Building a digital information infrastructure (infostructure) for health*. Geneva, Switzerland. Available from: https://ehna.acfee.org/c67802a7d4b3dc8914700842bf6776402b8d343c.pdf.

ITU Publications. (2021). *Digital trends in Africa 2021: Information and communication technology trends and developments in the Africa region 2017-2020*. Available from: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf.

Iacopino, P. & Meloan, M. (2017). *Analysis. Scaling digital health in developing markets: Opportunities and recommendations for mobile operators and other stakeholders*. GSMA Intelligence. Available from: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/07/Scaling_digital_health_in_developing_markets.pdf.

Lagos State Science Research & Innovation Council (LASRIC). (2021). Driving a culture of innovation, science & technology research in Lagos and beyond. We invest and enable tomorrow's industries. Available from: https://lasric.lagosstate.gov.ng/callup.

Leyl, S. (2019, February 22). Singapore HIV data leak shakes a vulnerable community. *BBC News*. Available from: https://www.bbc.com/news/world-asia-47288219.

Loufield, E. &Vashisht, S. (2020). *Data globalization vs. data localization* Available from: https://www.centerforfinancialinclusion.org/data-globalization-vs-data-localization.

Mugumbate, J. & Nyanguru, A. (2013). Exploring African philosophy: The value of ubuntu in social work. *African Journal of Social Work*, 3(1):80-100.

National Information Technology Development Agency (NITDA). (2019). *Nigeria cloud computing policy*. Available from: https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf.

Onwuegbuchi, C. (2020, May 15). Nigeria loses N60bn annually to foreign data hosting firms. *The Guardian*. Available from: https://guardian.ng/technology/nigeria-loses-n60bn-annually-to-foreign-data-hosting-firms/.

Ramachandran, V., Obado-Joel, J., Fatai, R., Masood, J.S. & Omakwu, B. (2019). *The new economy of Africa: Opportunities for Nigeria's emerging technology sector*. Centre for Global Development. Available from: https://www.cgdev.org/reader/new-economy-africa-opportunities-nigerias-emerging-technology-sector?page=0.

Report Linker. (2021). *Nigeria Data Center Market – Investment Analysis & Growth Opportunities 2021-2026*. Available from: https://www.reportlinker.com/p06129724/Nigeria-Data-Center-Market-Investment-Analysis-Growth-Opportunities.html?utm_source=GNW.

The Principles of Digital Development. (2020) *Principles for Digital Development*. Available from: https://digitalprinciples.org/. [Accessed October 12, 2021].

The Economist. (2017). The world's most valuable resource is no longer oil, but data. Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Van Velthoven, M.H. & Cordon, C. (2019). Sustainable adoption of digital health innovations. *Journal of Medical Internet Research*, 21(3): 311922. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6452285/.

Whiteside, J. (2020). *A systems thinking approach to digital transformation*. Digitalisation World. Available from: https://m.digitalisationworld.com/blogs/56217/a-systems-thinking-approach-to-digital-transformation.

World Bank. (2017). Leapfrogging: The key to Africa's development? From constraints to investment opportunities Available from: https://openknowledge.worldbank.org/bitstream/handle/10986/28440/119849-WP-PUBLIC-Africa-Leapfrogging-text-with-dividers-9-20-17-web.pdf?sequence=1&isAllowed=y.

World Bank. (2021). *World Development Report 2021: Data for better lives*. Available from: https://doi.org/10.1596/978-1-4648-1600-0.

World Health Organization (WHO). (2019). *WHO guideline: Recommendations on digital interventions for health system strengthening*. Available from: https://www.who.int/publications/i/item/9789241550505.

Munshi, N., 2020. Africa's cloud computing boom creates data centre gold rush. Financial Times. Available at: https://www.ft.com/content/402a18c8-5a32-11ea-abe5-8e03987b7b20 [Accessed July 23, 2021].

Nigeria Federal Ministry of Communications,2018, *FEDERAL REPUBLIC OF NIGERIA AT THE A4AI-NIGERIA BROADBAND INFRASTRUCTURE FORUM 2018* Available from: https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2018/11/Speech-Minister-of-ICT-Nigeria-Broadband-Forum-Oct-30.pdf.

Rack Centre, 2021. Carrier neutral Tier iii data centre in Nigeria. *Rack Centre*. Available at: https://rack-centre.com/ [Accessed July 27, 2021].

Chapter 6

AI Governance in Africa: The Case of Mauritius and Lessons for Africa

Bridget Boakye

Introduction

Policymakers around the world now widely accept that artificial intelligence (AI) is not merely an abstract computer domain, but the most transformational technology of our time. Notably, Russian president Vladimir Putin said on the implications of AI that "AI is the future, not only for Russia but for all humankind …Whoever becomes the leader in this sphere will become the ruler of the world." This illuminates the high-stakes nature of the global AI arms race (Allen, 2017: para. 1).

The Covid-19 pandemic has further underscored the strategic importance of AI for governments. From assisting in contact tracing through mobile phone and geolocation data, to the development of new drugs and treatments, pandemic management, and economic recovery, AI has proven invaluable in the fight against the novel coronavirus and its variants (Oxford Insights, 2020). In fact, the pandemic has only accelerated the 'AI revolution'. In 2016, PricewaterhouseCoopers predicted a 14% increase in global GDP in 2030 due to AI adoption. But early data from 2020 shows a more pronounced effect of the technology on the global economy, with jobs lost during the pandemic being rapidly replaced by AI (Semuels, 2020).

In Africa, accelerated digitisation due to the Covid-19 pandemic is supporting an ongoing expansion of AI in the private and public spheres (Gehl Sampath, 2021). Emerging evidence points to innovative AI-use cases across the continent, from agriculture, transportation, fintech, natural language processing and computing in Kenya, Nigeria, Somalia, Ghana and South Africa, to beneficial AI use in wildlife conservation, point-of-care diagnostics, government services, crop monitoring, water management and enterprise development in Uganda and Ethiopia (Gwagwa et al., 2020). Moreover, despite persistent challenges, new research points to a transformative "feminisation" of technology entrepreneurship in Africa, strengthening the case of a burgeoning gender, application and location-inclusive AI ecosystem on the continent (Gwagwa et al, 2020).

Questions on AI governance and ethics have also exploded in the public and private domains, fuelling debates among scholars and policy practitioners on data commodification, responsibility and morality, among others. These debates arise from four universal challenges for AI systems: bias and fairness, privacy, robustness, and explainability. To address these concerns, big tech companies and other private sector actors have released guidelines and frameworks in an attempt

to self-regulate. However, with the increasing prominence of AI systems, constant media buzz on harmful outcomes, growing disillusionment with Big Tech's self-regulatory mechanisms in what scholar Ben Wagner calls "ethics washing" (Wagner, 2018:3), and glaring public discontent, governments around the world are taking a more active role in AI regulation, designing and publishing various policy instruments to govern its use. In one telling example, the OECD's live AI policy observatory boasts more than 600 national AI policies and strategies from over 60 countries, territories and the EU (Oecd.ai Policy Observations, 2021).

These policy initiatives include landmark frameworks such as the OECD AI Principles, the G20 AI Guidelines, the Universal Guidelines for AI, UNESCO's AI Ethics Recommendations, and the draft European Union (EU) AI Act of the European Commission. Like the EU's General Data Protection Regulation (GDPR), the EU's AI Act is a first-of-its-kind rule for AI and a major effort to provide a risk-based regulatory framework for AI that could have outsized global impact (European Commission, 2021).

In Africa, CNN's report uncovering Russian troll farms in Nigeria and Ghana in 2020 and the exposés revealing the involvement of data-mining firm, Cambridge Analytica, in Nigeria and Kenya's elections in 2007 and 2013/2017 respectively, have intensified the local debate on data protection and privacy and have catapulted Africa's AI debate onto the international stage (Boakye, 2021b). Beyond privacy, scholars have identified Africa-specific ethics concerns within the broader ethical AI movement. Situated within the historical and socio-political context of Africa's relationship with the West, concerns around "algorithmic colonialism" and "data colonialism" suggest that the import of Western-developed and/or controlled AI tools to solve social problems are often unfit for the African context and come at the expense of local solutions, reproducing and reinforcing colonial and neo-colonial power structures (Birhane, 2020; Couldry & Meijas, 2018). According to Birhane (2020:389), the "… West's algorithmic invasion simultaneously impoverishes development of local products while also leaving the continent dependent on Western software and infrastructure".

In one effort, an increasing number of African governments are developing data governance laws (28 countries as of 2020), a basis for AI governance and ethics, given the data protection elements in the AI governance and ethics debate (Gwagwa et al., 2020), However, very few AI-specific frameworks and regulations exist. As of 2021, Kenya, South Africa and Morocco had AI-related policy initiatives, but only two African countries – Mauritius and Egypt – had national AI strategies: an essential AI governance instrument (Oecd.ai, 2021). National AI strategies bolster national security, aid economic growth, ensure ethics and safety, and promote public wellbeing with

policies to steer the development and adoption of the technology to mitigate its risks and expand its rewards (Allerin, 2021; World Bank, 2021).

At the regional level, the African Union has also established a working group on AI with the mandate to craft a pan-African strategy and a unified African position on AI (Egypt Minister of Communications and Information, 2019). But beyond this scope, little exists that is defining, soliciting or engaging with African voices and perspectives on AI governance and ethics, especially in multinational fora. Scholars point to an entrenched tendency, an old age mistake of limiting technology regulation to languages, ideas, theories and challenges of the few, primarily the global North, at the expense of those in the global South (Gupta and Heath, 2020).

Debates on Africa's AI policy gap are also intimately tied to increasing calls for African digital and data sovereignty. Cognisant of harmful AI-use cases and cautious of Western dependence and the side-lining of Africa's voice in the global tech governance debate, some scholars and activists propose that African governments control their digital infrastructure and assets independently through data location, digital taxes, and national civil registers (Velluet, 2021). But, without proper recourse and checks on government authority, digital sovereignty – as loosely interpreted by some – threatens to stifle Africa's nascent but burgeoning creative economy, fragment the internet into ideological camps, and disrupt global processes, norms and institutions that are intended to protect the economic, governance and social freedoms afforded by the open and free internet (Bennett et al., 2021; Boakye, 2021a).

But the trajectory of Africa's AI governance narrative need not be either/or – purely externally controlled or internally restrictive. Mauritius's AI governance approach provides a good counter-narrative to the prevailing notion of African dependence and lack of initiative and ownership in technology governance, specifically AI. The case study below examines Mauritius's national AI strategy as a progressive, forward-looking Africa-led AI governance instrument that embodies global best practices while responding to the local needs and demands of its citizens. Moreover, Mauritius's AI strategy demonstrates a new way of thinking about digital sovereignty: sovereignty based less on control, borders and closed systems, but rather based on unique national priorities, investment and socio-economic strategy. Ultimately, such a vision addresses existing structural inequalities that adversely affect Africa in the technology policy debate, without crippling its growing digital economies.

Case Study: Mauritius's National AI Strategy

Mauritius, a small island country of about 1.3 million people, has long been a model of democratic governance and economic transformation in Africa. The country has the second highest GDP per

capita in Africa and, as of July 2020, had achieved high-income status classification by the World Bank. This was achieved through an export-oriented development strategy centred on the manufacturing of textiles and clothes in the 1980s, and on the offshore/global business development sector in the 1990s (Working Group on Artificial Intelligence, 2018).

The country has taken a similar frontrunner approach to digital transformation. In a recent interview, Deepak Balgobin, the country's Minister of Information, Technology, Communication, and Innovation, shared that the country has "150% mobile penetration … and more than 90% of the country has high broadband internet connection" (Prisma Reports, 2020). On digital policy, Mauritius is one of only six African countries that has ratified the African Union (AU) Convention on Cyber Security and Personal Data Protection since it was adopted in 2014. The country was also the first African country to release a national AI strategy, just a year after Canada released the first-ever national AI strategy in 2017.

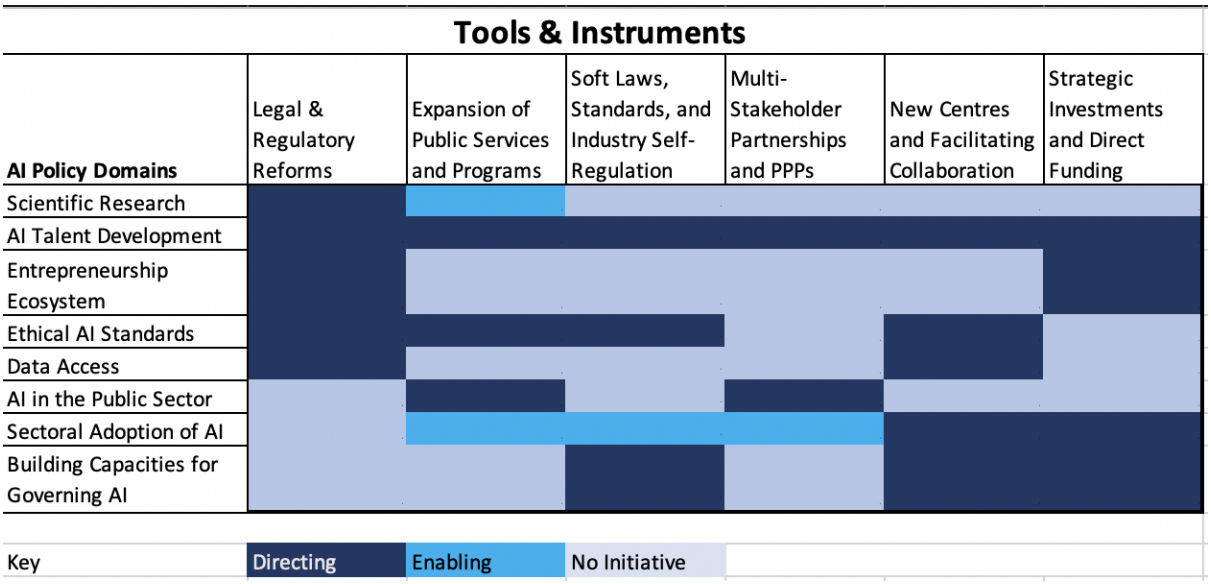
Developed by senior ministers and advisors on its working group (WG) on AI, the country seeks to "create the first-mover advantage in AI development in [Africa]" through technology, innovation and skill development (Working Group on Artificial Intelligence, 2018). With a specific focus on AI adoption rather than development, the 70-page document explores three areas of AI governance:

1. Defining AI, benchmarking of AI strategies around the world, and a discussion of challenges with implementing AI in Mauritius.
2. Exploring potential applications of AI in strategic sectors (manufacturing, healthcare and biotechnology, fintech, agriculture, ocean economy, transport, and citizen services/government) to address existing challenges and create new solutions with Mauritius's unique selling point in these areas.
3. Recommendations on the implementation of the strategy, including financial incentives for start-ups, bolstering regulatory frameworks on ethics and data protection, and establishing the Mauritius Artificial Intelligence Council (MAIC), the coordinating and project implementation and monitoring body for the country's AI strategy.

While national AI strategies share common features, none are the same. For example, Finland's strategy takes a bottom-up facilitative approach to build digital platforms and networks to drive AI development, while Canada's take a government-led and funded research-centred approach in an effort to become the AI research and talent capital of the world (World Bank, 2021). Inspired by the World Bank's recently developed Role of Government in AI heatmap (World Bank, 2021), the analysis (Figure 1) of Mauritius's national AI strategy confirms a top-down, skills-first approach

to AI governance. Noting the reluctance of public-sector adoption of AI, Mauritius's strategy centres on government-directed initiatives in sectoral projects and AI talent development, funding incentives for start-ups, and developing an enabling environment for private sector implementation of selected projects through "adequate support, implementation capacity and clear and impactful deliverables" (Working Group on Artificial Intelligence, 2018:64). Other tools and instruments within areas such as scientific research and the entrepreneurial ecosystem are considered but, given their minimal relevance for (small AI talent for scientific research) and influence on the country's AI and digital transformation vision at this time (the strategy acknowledges a plethora of existing initiatives to foster entrepreneurship not related to AI), have no dedicated policy initiatives.

Figure 1: Mauritius: Role of Government in AI Heat Map



The figure above is a tool from the World Bank's Role of Government in AI report (World Bank, 2021). The scores defining the heatmap for Mauritius's government in AI are not produced by the World Bank, however, but defined independently through an analysis of Mauritius's AI strategy.

Mauritius has received high praise for its national AI strategy. While noting that rigorous analysis of and evidence for the strategy's effectiveness are not yet available, the media point to speedy implementation of the WG's recommendations, especially in skills development. The government has operationalised a Skills Development Programme for AI to accelerate AI training (allAfrica.com, 2019), is fully funding a new MSc programme in artificial intelligence at the University of Mauritius (Business Mauritius, 2020), and has made a budget allocation for its MAIC

(Le Defi Media Group, 2019). For its efforts, the country is now the highest-ranked African country on the 2020 Government AI Index released by Oxford Insights and the International Research Development Centre (Oxford Insights, 2020). According to Richard Stirling, CEO of Oxford Insights, Mauritius' approach to AI is fantastic … They have a clear strategy as to what they want to achieve. They are also bringing the private sector and academia with them. They have a council with all these sectors on them. They are investing in the skills, and they are thinking about how that can be transferred back into the industry. That's amazing and that's the perfect playbook (Retief, 2020).

Beyond vision and strategy, Mauritius ranks highly on the report's newly developed 'Responsible Use Sub-index', a metric of nine indicators across four ethics pillars advanced by the International Development Research Centre and the Canadian government to ensure that governments not only develop and implement AI, but use it in a responsible manner. Of 34 countries covered on the 'Responsible Use Sub-index', Mauritius ranks 13th and relatively high across all responsible-use metrics: privacy (66.22), inclusivity (63.20), transparency (65.77), and accountability (65.20), suggesting an effective and ethical implementation of its AI vision, although little evidence exists.

Lessons and Implications for African Policymakers

Although the economic and socio-political context of Mauritius as an advanced digital economy and welfare state differs from the less-mature digital ecosystem and mixed economic model of many African states, its historical and geopolitical position, and current socio-economic challenges, are like that of many other African countries. As such, its national AI strategy approach and vision provide better guidance than those of other countries, e.g. Finland or Canada. Three lessons emerge for African policymakers:

1. The nascent stage of Africa's digital economies and AI ecosystems should not preclude African governments from developing AI strategies and policy instruments for AI governance. Mauritius's bold decision to publish a simple and clear AI strategy that is not merely aspirational but emblematic of where it is now, its challenges, and where it seeks to go is a behavioural approach that can help expand African technology governance perspectives and catapult its frameworks to the global stage. Although difficult to commit fully and implement a grand vision such as a national AI strategy, Mauritius's early success in relation to key priorities is improving its AI readiness and catalysing adoption, moving from being ranked 3rd in Africa and 60th in the world in 2019 to 1st in Africa and 45th in the world in 2020 (Oxford Insights, 2020).
2. In manufacturing, ocean economy and transport (Kanife, 2020), many Sub-Saharan African countries face similar challenges – decreasing productivity in manufacturing, congestion and climate change – as those outlined by Mauritius in its AI strategy. African governments should

therefore seek to share strategy, projects and technologies through open policy discussions and clinics, and thereby foster intuitive cohesion among AI policies and positions developed across the continent. Supported by the AU Working Group on AI, such idea-sharing and discussion could be facilitated through a secure digital knowledge-sharing platform that is transparent and allows for public input.

3. Mauritius's national AI strategy is guided by the experiences of other nations, but not defined by them. While encouraging partnerships with global actors, including seeking foreign expertise on its MAIC, partnerships at the World AI Show and the Blockchain Summit, and MOUs with international networks, Mauritius's national AI strategy is unique in its sectorial and socio-economic priorities. While maintaining many of the common features of national AI strategies, and adhering to international best practices such as aligning with the EU's GDPR, Mauritius's AI strategy defines a path that is best for its people.

Conclusions

While AI has brought tremendous benefits to the world, it has also introduced profound challenges and questions, requiring government steering and regulation. In Africa, only two countries have national AI strategies, with that of Mauritius being the first. With increasing caution about Western-developed models of digital policy and the desire and need for homegrown and socially responsive digital policy initiatives in Africa, Mauritius's embrace of AI to address its unique challenges, balanced against global best practices and collaboration, can be a good model for African leaders and policy practitioners looking to define Africa's tech policy trajectory and narrative in this new era.

References

allAfrica.com. (2019). *Mauritius: HRDC organises talk on implementation of Ai in businesses* [online]. Available from https://allafrica.com/stories/201912130930.html [Accessed 27 July 2021].

Allen, G.C. (2017). Putin and Musk are right: Whoever masters AI will run the world [online]. *CNN*. Available from https://edition.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html [Accessed 26 July 2021].

Allerin (2021). *Why countries need a national AI strategy* [online]. Available from https://www.allerin.com/blog/why-countries-need-a-national-ai-strategy [Accessed 26 July 2021].

Bennett, A., Beverton-Palmer, M. & Stapp, A. (2021). *Defending the free and open internet in an age of authoritarianism* [online]. Available from https://institute.global/policy/defending-free-and-open-internet-age-authoritarianism-0 [Accessed 27 July 2021].

Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPT-ed*, 17(2):389-409.

Boakye, B. (2021a). *Social media futures: Changing the African narrative* [online]. Available from https://institute.global/policy/social-media-futures-changing-african-narrative [Accessed 27 July 2021].

Boakye, B. (2021b). *Tech policy in Africa: Emerging trends in internet law and policy* [online]. Available from https://institute.global/policy/tech-policy-africa-emerging-trends-internet-law-and-policy [Accessed 26 July 2021].

Business Mauritius. (2020). *Fully funded MSC artificial intelligence offered by University of Mauritius co-funded by the HRDC* [online]. Available from https://www.businessmauritius.org/latest-news/fully-funded-msc-artificial-intelligence-offered-by-university-of-mauritius-co-funded-by-the-hrdc/ [Accessed 27 July 2021].

Couldry, N. & Mejias, U.A. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4):336-349.

Egypt Minister of Communications and Information. (2019). *Egypt hosts AU working group on AI first session* [online]. Available from https://mcit.gov.eg/en/Media_Center/Press_Room/Press_Releases/40507 [Accessed 26 July 2021].

European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* [online]. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 [Accessed 26 July 2021].

Gehl Sampath, P. (2021). Governing artificial intelligence in an age of inequality. *Global Policy*, 12(56):21-31.

Gupta, A. & Heath, V. (2020). AI ethics groups are repeating one of society's classic mistakes [online]. *MIT Technology Review*. Available from https://www.technologyreview.com/2020/09/14/1008323/ai-ethics-representation-artificial-intelligence-opinion/ [Accessed 26 July 2021].

Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I. & De Beer, J. (2020). Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. *The African Journal of Information and Communication*, 26:1-28. Available from http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132020000200002 [Accessed 21 June 2021].

Kanife, E. (2021). The many struggles of the AI space in Nigeria and the lessons from Mauritius [online]. *Technext*. Available from https://technext.ng/2021/04/21/the-many-struggles-of-the-ai-space-in-nigeria-and-the-lessons-from-mauritius/ [Accessed 26 July 2021].

Le Defi Media Group. (2019). *Artificial intelligence: Steps towards a smart Mauritius* [online]. Available from https://defimedia.info/artificial-intelligence-steps-towards-smart-mauritius [Accessed 26 July 2021].

OECD.ai Policy Observatory. (2020). OECD National AI Policies and Strategies [online]. Available from https://oecd.ai/dashboards [Accessed 25 July 2021].

Oxford Insights. (2020). *Government AI Readiness Index 2020* [online]. Available from https://www.oxfordinsights.com/government-ai-readiness-index-2020 [Accessed 26 July 2021].

PricewaterhouseCoopers. (2016). *Sizing the prize. PwC's global artificial intelligence study: Exploiting the AI revolution* [online]. Available from https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html [Accessed 26 July 2021].

Prisma Reports. (2020). Interview with Deepak Balgobin, Minister of Information Technology, Communication and Innovation [online]. Available from: https://prisma-reports.com/interview-with-deepak-balgobin-minister-of-information-technology-communication-and-innovation/ [Accessed 26 July 2021].

Retief, C. (2020). Mauritius, South Africa & Seychelles are in the driver's seat of AI readiness in Africa [online]. *Forbes Africa*. Available from https://www.forbesafrica.com/technology/2020/10/01/mauritius-south-africa-seychelles-are-in-the-drivers-seat-of-ai-readiness-in-africa/ [Accessed 27 July 2021].

Semuels, A. (2020). Millions of Americans have lost jobs in the pandemic – And robots and AI are replacing them faster than ever [online]. *Time*, 6 August. Available from https://time.com/5876604/machines-jobs-coronavirus/ [Accessed 25 July 2021].

Velluet, Q. (2021). Can Africa salvage its digital sovereignty? [online]. *The Africa Report*, 16 April. Available from https://www.theafricareport.com/80606/can-africa-salvage-its-digital-sovereignty/ [Accessed 27 July 2021].

Wagner, B. (2018). Ethics as an escape from regulation: From "ethics-washing" to ethics-shopping? In *Being profiled: Cogitas ergo sum: 10 years of profiling the European citizen* (pp. 84-89). Edited by Bayamlioğu, E., Baraliuc, I., Janssens, L & Hildebrandt, M. Amsterdam University Press. Available from https://www.jstor.org/stable/j.ctvhrd092.18?seq=1#metadata_info_tab_contents [Accessed 26 July 2021].

Working Group on Artificial Intelligence. (2018). *Mauritius Artificial Intelligence Strategy* [online]. Available from https://cib.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy%20(7).pdf [Accessed 25 July 2021].

World Bank. (2021). *Harnessing artificial intelligence for development in the post-Covid-19 era: A review of national AI strategies and policies* [online]. Available from https://thedocs.worldbank.org/en/doc/2e658ef2144a05f30e254221ccaf7a42-0200022021/original/DD-Analytical-Insights-Note-4.pdf [Accessed 26 July 2021].

Chapter 7

African Entrepreneurship and the Promise of the Digital Economy

Emma Ruiters

Introduction

Entrepreneurship is often touted as a panacea for economic development in African countries, particularly by those who perceive the potential in the youthful population and rapid growth of African economies (such as the World Bank, OECD, UNCTAD, UNIDO, etc.). The rate of total early-stage entrepreneurial activity in Africa is 13.7%, but this varies significantly by country (Global Entrepreneurship Monitor (GEM) Report, 2019).

With increased interest in technology start-ups due to the influence of Silicon Valley and the growth of big technology companies, most contemporary digital economy strategies include an innovation and entrepreneurship thematic area. In 2020, 359 African tech start-ups received funding, while African tech start-ups received financial backing six times faster than the global average from 2015 to 2020 (World Economic Forum [WEF], 2021). However, only a few African tech start-ups transition successfully into mature companies. Moreover, venture capital (VC) investment in Africa suffers from relatively low average returns compared to other regions (Boston Consulting Group [BCG], 2021). For governments, discretion is required to assess whether these businesses are value-creating or value extracting, as this avenue of growth can be beholden to shareholder or market interests, which may be at cross-purposes to the long-term economic development of the country (O'Reilly, 2019).

On balance, improved entrepreneurial activity across African economies lends itself to greater sovereignty through localised innovation and its contribution to growth and development. Within economic theory, entrepreneurship has been intrinsically linked to innovation and growth by Joseph Schumpeter (1942), who identified the entrepreneur as a critical element of creative destruction and thus economic change. The entrepreneur carries this out through new combinations of existing technology or innovations. Thus, African tech entrepreneurship is promising as a source of innovation, growth and development.

Definition of Entrepreneurship

Entrepreneurship, the activity of setting up a business or businesses, taking on financial risks in the hope of profit, need not be focused just on start-ups; it can also be activities undertaken within a public sector agency or large company by an employee expanding into a new business area (Oxford Languages Dictionary, 2021). Entrepreneurship and innovation in African countries has

been driven by significant growth in internet penetration and mobile device access, with falling data costs. As Figure 1 shows, there are still significant gaps to an enabling business environment for African countries.

The Current Debate and Context

Wim Naudé (2019) asserts that African countries face a unique opportunity to grow manufacturing because of the convergence of 4IR technologies due to start-up entrepreneurship. However, there is a tension between innovation, capital accumulation and power. This is embodied in the argument of Andreoni and Roberts. They posit that there are power dynamics inherent in data management[5] as a critical input to the modern innovation process, particularly for 4IR technologies (Andreoni & Roberts, 2020; WEF, 2017). In this space, developing countries are often unprepared to navigate the complex and dynamic environment that is the domain of multinational companies worth trillions of USD and other players who eye lucrative data flows (UNCTAD, 2019). If developing countries can harness these massive flows of data in the digital economy, but are unable to navigate the complex global environment, they may become mired in a "middle-income technology trap". This term is described by Andreoni and Tregenna (2020:2) as "a specific structural and institutional configuration of their economies preventing innovation and domestic industrial development" due to exercises of power higher up the data value chain.

These debates are situated within the broader canon of innovation economics. Schumpeter argued that big business creates capitalist surplus, but entrepreneurs drive innovation (Schumpeter, 1942). This evolutionary character is not due to increases in population or capital, but rather through new consumer goods, new methods of production, improved quality of goods, new transportation methods, networks, materials, markets and new forms of industrial organisation (Schumpeter, 1942). Baumol (1996) added two more innovation drivers: technology transfer from countries with high adoption to new markets, and innovation in rent-seeking procedures. Here, contemporary authors have discussed digital platforms as new avenues of creative destruction: different types of platforms shape the processes of value creation, market power and value capture, and thus the process of industrial development (Kenney & Zysman, 2016) (Evans, 2016).

Outstanding Issues within the Academic Discourse

BCG's (2021) report on "Overcoming Africa's Tech Startup Obstacles" suggests that the relative success of tech entrepreneurs in Africa is due to the continent's fertile environment of a growing, youthful population and the aforementioned growth in digital access, and the application of

[5] This extends to data storage, aggregation, localisation in data centres, and data use by businesses and governments.

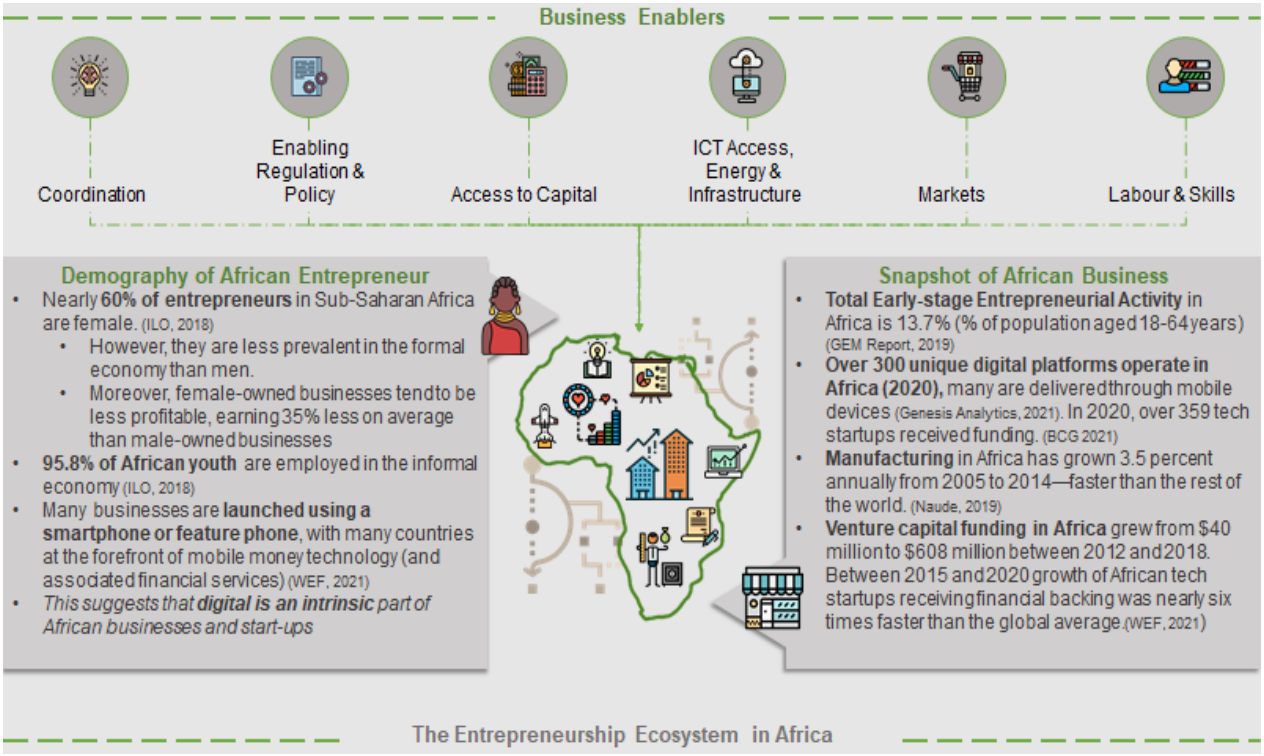
emerging technologies across both the private, i.e. financial services and energy, and public sector, in particular health and education. However, the business environment for start-ups prevents maturation into larger firms. These barriers include: low consumer purchasing power; complex and inconsistent regulations; inadequate data communications infrastructure; a fragmented marketplace of 54 countries; and scarce capital and digital talent (WEF, 2021). An additional risk factor is competition for African countries and businesses with large multinationals and domestic state monopolies. This crowds out domestic opportunities for local entrepreneurs to develop innovative technologies, products and business models (BCG, 2021). It is thus a matter of critical importance for broader African economic development and growth that entrepreneurship and innovative activity do not falter at the start-up stage, but include maturation, so that larger firms can contribute to domestic capital accumulation and compete in the highly complex international environment dominated by multinationals.

Implications for African Entrepreneurship

That said, key business enablers should be prioritised to ensure entrepreneurship is supported, but this must be done through a careful balance of both foreign and domestic power dynamics to ensure that development outcomes are attained sustainably. While start-ups can be innovative, the dynamics of commercialisation, finding new markets and scale-up mean that larger enterprises, like venture capital funds or development banks, are critical components of the process. This is often framed as a solely private sector-driven operation, but the example of the Brazilian Development Bank (BNDES), which is larger than the World Bank and structured as a federal public company associated with the Ministry of the Economy of Brazil, could be a potential model that is public sector driven (Pessoa, Samuel, Roitman, Fabrio, Ribeiro, Eduardo, Barboza & Ricardo, 2020). BNDES loans have been found to increase investment, employment and exports for small and medium enterprises. The Bank also appears to have positive effects on the economic activity and revenue of supported firms. The presence of government 'counterweights' or alternatives to funding from international MNCs or venture capital can be critical for ensuring that economic development is aligned with national objectives.

Ultimately, enablers for the digital economy and entrepreneurship extend beyond just investment. Figure 1 describes key business enablers for entrepreneurship ecosystems in the African context. This occurs along the six themes of Energy and Infrastructure, Enabling Regulation and Policy, ICT access, Markets, Labour and Skills, and Access to Capital.

Figure 1: The entrepreneurship ecosystem in Africa



Source: Author.

Coordination

Governments can facilitate development through industrial policy such as subsidies, infant industry protection and constructing a well-functioning national innovation system. An example is Finland's national innovation system, which was critical to the development of Nokia through a mix of public sector players such as parliament, SITRA (the Finnish National Fund for Research and Development (R&D)), the Ministries of Education and of Trade and Industry, universities and, of course, the private sector. Incredibly, Nokia was subsidised for 17 years before it became profitable (Lin & Chang 2009). Thus, through patient and sustained investment, policy, subsidies and extensive public-private sector coordination, the development of domestic market conditions can foster sustainable capacity building in targeted sectors.

Government strategic procurement of products and services from local businesses can be a supportive mechanism to ensure that emerging businesses have sources of demand. This could be through a digital application or platform, as digital platforms are key infrastructures for intermediating and shaping market transactions and ecosystem relationships (Mazzucato,

Entsminger & Kattel, 2020). Local markets can become testing grounds for global competition, as practised by both Finnish and East Asian industrialisers. Once this has been achieved, governments can also support the sourcing of and access to new markets through investment-promotion agencies and other export development and promotion programmes.

Enabling Regulation and Policy

Policies that enable e-commerce growth, privacy and personal data protection, cybersecurity, competition policy, intellectual property protection, telecommunications and financial sector regulation are critical to supporting entrepreneurship, particularly in the digital economy. Government has a significant regulatory role, which it currently is not fully fulfilling in many African countries.

Access to Capital

While access to VC funding has grown rapidly, this often comes with shareholders and obligations. Due to the inequality of capital between developed and developing countries, this often means that local start-ups and businesses are beholden to the interests of foreign capital. These interests often are far more short term. At present, R&D as an expenditure of GDP is significantly below global averages in Sub-Saharan Africa (SSA). It was hovering between 0.25% and 0.5% in 2018, while the global average was near 1.75% of GDP (UNESCO Institute for Statistics, 2021). Expenditure on R&D can be recouped by the government through tax revenue when firms mature, which gives governments an incentive for businesses to do well.

ICT Access, Energy and Infrastructure

Mobile network and fixed broadband, access to devices and affordable data, amongst other considerations, are critical to accelerating participation in the digital economy. This expands the economies of scale for businesses, as more domestic consumers can access products and services. Energy and other infrastructure play a key role here, also as enablers and critical constraints to the growth of the digital economy, if they are not in place.[6]

Markets

Businesses require markets to expand production and growth. Due to the smaller population, density and greater distances between markets, African countries have often been at a disadvantage from a cost perspective, thereby inhibiting expansion of market share and, broadly, capital accumulation. The introduction of the African Continental Free Trade Area (AfCFTA) in 2021 has been touted as a means to connect 1.3 billion consumers across 55 countries and deliver real

[6] The energy sector is rapidly changing due to new technologies like solar, which is accelerating decentralised, private energy generation rather than traditional utility models with national grids.

income gains of nearly $450 billion by 2035 (World Bank, 2020). However this cannot happen without advances in trade infrastructure and technologies. That said, there is a strong correlation between increased ICT adoption and increasing levels of trade. Studies show that improved access to ICT and the adoption of e-commerce applications stimulate bilateral trade flows on a number of levels (Xing, 2018). It has also been found that a 10% increase in internet use leads to a 2% increase in bilateral trade (Xing, 2018).

Labour and Skills

Citizens and consumers require high levels of literacy, skills and entrepreneurial acumen, which can only be imparted through a high-quality and well-functioning education system. This channels through to the government, which must be well-capacitated in administrative skills, investment and business analysis skills and regulatory capacity in order to play the role of coordinator and strategist in the digital economy. Government capacity should be scaled to be able to perform this task adequately, at a local and national level, while maintaining high standards – lest investment be wasted and the efficiency of spend decline.

Concluding Remarks

The digital economy provide opportunities for entrepreneurship, but the performance of African start-ups must be supported by local governments through procurement, subsidies and a well-defined industrial strategy, along with other forms of support, lest business becomes captured by foreign influences. This requires significant capacity development for governments and an aggressive, cohesive industrial strategy in order to reap the economic benefit of African tech entrepreneurship as a promising source of innovation, growth and development. This suggests that existing issues that faced industrial policy and development before the Fourth Industrial Revolution have not changed.

References

Andreoni, A. & Roberts, S. (2020). *Governing data and digital platforms in middle income countries: Regulations, competition and industrial policies, with sectoral case studies from South Africa*. Digital Pathways at Oxford Paper Series No. 5, Oxford, United Kingdom.

Baumol, W.J. (1996). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Business Venturing*, 11(1):3-22.

Boston Consulting Group (BCG). (2021). *Overcoming Africa's tech startup obstacles: How established enterprises can help the region's innovators scale up*. Available from: https://www.bcg.com/publications/2021/new-strategies-needed-to-help-tech-startups-in-africa.

Evans, P and Gawer, A. (2016) The Rise of the Platform Enterprise. A Global Survey. The Emerging Platform Economy Series, No.1, 1-30.

Genesis Analytics (2021). How social media is powering small business in Africa. Available from: https://genesis.imgix.net/uploads/files/GENESIS_Unlocking-Africas-Potential-2021_Report-FINAL.pdf.

Global Entrepreneurship Monitor (GEM) Report (2019). Available from: https://www.gemconsortium.org/report.

ILO (2018). Women and men in the informal economy: *A statistical picture. Third edition.*

Kenney, M. & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3):61-69.

Lin, J. & Chang, H.-J. (2009). Should industrial policy in developing countries conform to comparative advantage or defy it? A Debate Between Justin Lin and Ha-Joon Chang. *Development Policy Review*, 27(5):483-502.

Mazzucato, M., Entsminger, J. & Kattel, R. (2020). Public value and platform governance. Working Paper Series IIPP WP 2020-11, UCL Institute for Innovation and Public Purpose, University College London, London. Available from: https://www.ucl.ac.uk/bartlett/public-purpose/wp2020-11.

Naudé, W. (2019). Brilliant technologies and brave entrepreneurs: A new narrative for African manufacturing. *Journal of International Affairs*, 72(1):143-158.

O'Reilly, T. (2019, July 17). Antitrust regulators are using the wrong tools to break up Big Tech. *Quartz*. Available from: https://qz.com/1666863/why-big-tech-keeps-outsmarting-antitrust-regulators/.

Oxford Languages Dictionary (2021). Oxford: Oxford University Press.

Pessoa, Samuel & Roitman, Fabrio & Ribeiro, Eduardo & Barboza, Ricardo. (2020). What Have We Learned About the Brazilian Development Bank? Available online at: https://www.researchgate.net/publication/345508833_What_Have_We_Learned_About_the_Brazilian_Development_Bank.

Schumpeter, J. (1942). *Capitalism, socialism and democracy*. New York: Harper & Brothers.
UNESCO Institute for Statistics. (2021). *Research and development expenditure as a proportion of GDP (% of GDP)*. Available from: https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS.

World Bank. (2020). *The African Continental Free Trade Area: Economic and distributional effects*. Washington, DC: World Bank.

World Economic Forum (WEF). (2021). The rise of African tech startups in 3 charts. Available from: https://www.weforum.org/agenda/2021/06/africa-tech-startups-technology-economics/.

Xing, Z. (2018). The impacts of information and communications technology (ICT) and e-commerce on bilateral trade flows. *International Economics and Economic Policy*, 15:565-586.
UNCTAD. (2019). Digital Economy Report. Available Online At: Https://Unctad.Org/System/Files/Official-document/Der2019_overview_en.Pdf.

Chapter 8

Advancing Digital Inclusion Through Distributed, People-Centric African Smart Cities That Promote Digital Sovereignty

Faith Obafemi

Introduction

Smart cities aim to provide their inhabitants with advancements in urban planning that are enabled by technology and that improve their daily lives, community, health, business activities and transportation. Cities are made up of inhabitants with different backgrounds, languages, education, occupation and so on, making it difficult to have a unifying definition of a city. Consequently, smart cities also lack a unifying definition and have to be defined in different contexts. Some definitions focus on contexts such as sustainability, level of industry, and people-centredness.

A smart sustainable city is an innovative city that uses ICTs and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects. His Excellency Paul Kagame, President of the Republic of Rwanda, defines smart cities in a people-centred context and says "[s]mart cities are about people not computers. The mission is not to invest in technology for its own sake, but to do so strategically, to make life measurably better for the people who live in our cities". (Smart City Expo, 2019)
The common denominator in the different definitions of smart cities is that technology is used to transform a certain location. This manifests in use cases such as e-governance, as seen in Singapore and Estonia, and in smart transportation, as seen in China.

Debate

The promise of smart cities, whether created from blank slates (Akon City) or upgrades of existing cities (Barcelona), is an exciting one. But would the average person be able to afford to live in such a city if everything is expensive? For existing cities that are transformed into smart cities, where would those who cannot afford living there go? What happens to the underutilised so-called rural areas? At least 40% of Africans currently live in cities, with this figure expected to double by 2050 (Muggah & Hill, 2018). Low-income earners within this percentage live in slums that lack the barest of basic utilities such as clean water, stable power, efficient waste disposal and more.

Drawing on the above background, defining African smart cities in the African context would mean smart ways to manage resources, human and natural, to make life easier, faster and cheaper. This

definition emphasises that cities are not smart just because of technology, as technology is an enabler, not a driver; *cities are smart because technology is used to make lives better* (Smart Cities Council, 2015). Aligning with Sénamé Koffi Agbodjinou's neo-vernacular (Agbodjinou, 2020) idea of smart cities for Africa, this article proposes distributed African smart cities that leverage our culture of collaboration and community sustenance. African smart cities should not be focused on skyscrapers, which mean nothing to the people at the grassroots. Rather, they should be conceived as distributed and sustainable smart cities that are built for their unique needs, crowdsource capacity building and produce their own power and technology.

Perspective

With most smart city initiatives in Africa focusing just on the technology or adopting a copy-and-paste approach, there are certain blind spots. Most smart cities in Africa (African Smart Cities, 2021) have been in construction for years, yet have made only little or cosmetic progress. Nigeria's Eko Atlantic, for instance, has been in construction since 2003; the last update on its official website (Eko Atlantic, 2021) was in 2019, while that of Ghana has been stagnant since 2016. It is likely that the large scale of the projects and funding issues are the reasons for the delay. Rather than building on a grand scale and trying to do everything at once, it would be more practical to focus on just one aspect of the different pieces that make up a smart city. Better still, the focus should be on meeting priority needs like water, housing and education in a smart way, and then scaling up. For instance, focusing on water issues, Cape Town leveraged technology, to solve the still-existing water crisis (Edmond, 2019).

For funding issues, current attention appears to be focused on the two approaches of government to business and business to consumer. But there could be opportunities for incorporating consumer-to-consumer business models into smart cities. For instance, in a small town in Togo, locals focused on waste management and built an e-waste management app to aid efficiency. Those who use the app earn tokens that they can use to purchase services from others on a dedicated marketplace (Agbodjinou, 2020). Another reason for the delay could be the pushback from the fear of displacing people and jobs. When a bus conductor realises he is to be replaced with a card and smart meter, opposition can be expected. This is where communication is vital. As this article has been proposing, the focus should be on the people and not on the technology. Thus, rather than selling the technology, the end product (making life easier) should be the focus. Those whose jobs inevitably get displaced can be retrained to fit into other vacancies that smart cities make available.

Usually, Africa's demography is discussed in a negative light as a liability for the continent. While this is true to a certain extent, as seen in the high rate of migration to Western countries and

hence a brain drain, along with the large population that aggravates poverty, this liability can still be transformed into an asset. Africa needs to look inward and leverage its human resources and talents to build homegrown solutions that solve its unique problems using what it has. For instance, Africa is best suited for harnessing solar energy due to its tropical climate.

Implications and Policy Recommendations

Each stakeholder, from the politicians and the lawmakers to the local government officials, as well as the developers, the partners and the citizens, all have a role to play to see this move from ideas to reality. Citizen and grassroots participation is essential. Smart cities are for the people. The following are policy recommendations for smart cities stakeholders.

1. Consistent and deep communication with citizens to help change their perspectives and mindsets. In Africa, most people view those who use public transportation as being poor. This stigma can only be removed when people realise that having fewer personal cars on the road and more public buses would make their movements easier and has nothing to do with their net worth.
2. Infusing culture into our smart cities. There is an African culture according to which a girl proves her suitability for being a wife by going to the stream to fetch water and balancing the container on her head all the way home. Now someone wants to install a borehole in the compound and a tap in the kitchen. How will girls in that community be able to prove that they are wife material?
3. African smart cities should reject the cookie-cutter approach to building smart cities. What works for a community comprising predominantly farmers will be different from what works for a community consisting predominantly of fishermen and fisherwomen.
4. Collecting and analysing data. When Cape Town's water crisis started, the first move was to identify leakages and then moderate water usage. In fact, using water for non-essentials like filling swimming pools was banned. This is a practical example of collecting and analysing data to solve a water crisis in a smart way. Digital sovereignty manifests in various ways, but one of the initial ways it was understood is having access to and control over one's data. Just because data is open does not mean it is accessible. Africa has a reputation for lacking access to or control over its own data because the means of collection and processing it is in the hands of a third party.
5. Build for diversity and inclusion. African smart cities should not assume that everyone is tech-savvy. Smart cities have always been criticised for widening the digital divide. On a continent where this gap is wider than that of others, conscious efforts need to be taken to build smart cities that close the divide through diversity and inclusion by default. For instance, it will be beneficial to have instructions, tutorials and other guides in native languages. Also, just as

ramps are provided for people with disabilities, they should not be neglected in digital inclusion.

6. Africa is well known for leapfrogging technology adoption. Generally, we skipped landlines and jumped to mobile phones. African smart cities are an opportunity to leapfrog development by harnessing frontier technologies like blockchain, artificial intelligence, 3D-printing drones, virtual reality, biotechnology, robotics, etc. Another way digital sovereignty manifests on the African context is having developmental autonomy. By focusing on human resources in terms of skills and capacity, Africa can transition from being only consumers of digital infrastructure to creators too.
7. Distributed and people-centric. Leveraging the power of the collective, African smart cities should be co-produced by the community. Citizens should participate actively in identifying their needs, developing a solution and implementing it. Governments with smart city plans should not only see citizens as ceremonial consultants or assume that a one-time perfunctory dialogue/trialogue event will suffice. To see a high measure of success with African smart cities, the approach should be bottom-up, not top-down.
8. Innovative regulations. Unlike planned smart city initiatives like Akon City in Senegal, and others in Tanzania, Rwanda, South Africa, Ghana and Nigeria, urbanisation in Africa just happens. This is likely how distributed African smart cities would crop up. Regulations should then try to strike a middle ground where citizens have the freedom to innovate and the laws still maintain order. If there are existing laws inhibiting this freedom, they can be changed; laws are not set in stone like Moses' tablets containing the Ten Commandments.
9. A new understanding of data. In the grand scheme of things, data is a priority component of smart cities, particularly on the level of basic amenities such as water, good roads, etc. If Africa is to exercise digital sovereignty over its data, there needs to be a new understanding of data. Currently, ownership and even access to data are attributed to the entity collecting and processing it. The blind spot here is that, if this data is not generated, it would not exist. Until it is viewed from this angle, citizens cannot decide the what, who, why, when and how of their data.
10. It is not about smartness, but sustainability. In meeting Sustainable Development Goals like SDG 11, others – like SDGs 8, 12 and 13 – need to be considered (United Nations, 2015).

Discussion

Rather than a conclusion, this ends with a discussion, because the concept of smart cities is dynamic and will continue to be on the agenda centuries from now. The future of Africa is urban and digital. Smart cities will play an integral role in preserving digital sovereignty in Africa, and the ability to utilise intelligence in responding to environmental and other issues is the reason

smart cities are dynamic. When we talk about smart cities in Africa, let's leave no one behind. In Africa, in the spirit of ubuntu, smart cities are because we are.

References

African Smart Cities. (2021). *Making African cities great* [online]. Available from: https://africansmartcities.info/ [Accessed 27 July 2021].

Agbodjinou, S.K. (2020). African smart cities in 2030. *The Journal of Field Actions: Field Actions Science Reports*, Special Issue 22:40-43. Available from: https://journals.openedition.org/factsreports/6267 [Accessed 27 July 2021].

Edmond, C. (2019). Cape Town almost ran out of water. Here's how it averted the crisis [online]. *World Economic Forum*. Available from: https://www.weforum.org/agenda/2019/08/cape-town-was-90-days-away-from-running-out-of-water-heres-how-it-averted-the-crisis/.

Eko Atlantic (2021). [online] Available at: https://www.ekoatlantic.com/ [Accessed 27 Jul. 2021].

Muggah, R. & Hill, K. (2018). African cities will double in population by 2050. Here are 4 ways to make sure they thrive [online]. *World Economic Forum*. Available from: https://www.weforum.org/agenda/2018/06/Africa-urbanization-cities-double-population-2050-4%20ways-thrive/.

Smart Cities Council. (2015). *Smart Cities Readiness Guide* [Online]. Available from: https://smartcityalliance.ca/site/assets/files/1465/readiness-guide-v2-8-24-2015.pdf.

Smart City Expo. (2019). His Excellency Paul Kagame, President of the Republic of Rwanda's Speech. Available from: https://www.newtimes.co.rw/news/kagame-smart-cities-drive-africas-urbanisation.

United Nations. (2015). *The 17 Goals* [online]. Available from: https://sdgs.un.org/goals.

Chapter 9

Contesting Digital Colonialism Narratives in Africa and their Framing Effects

Jacquelene Mwangi

Introduction

Conceptualising a narrative of digital sovereignty with reference to African nations is an uphill task. This difficulty, I argue, stems from both state-centric notions of 'digital sovereignty' and from the polar opposite notion of 'digital colonialism'. Both focus on the existence or lack of control over the internet, data and related infrastructures, with the former representing an ambition/aspiration and the latter representing the current reality facing African nations. Digital sovereignty, it is often argued, is much needed in order to avoid a new era of digital colonialism. This view is fallacious for two reasons: first, it overlooks the nature of the state and the exercise of state power on the African continent and 'the double-edged sword of digital sovereignty' that it presents, i.e. digital sovereignty enables a state to protect its citizens from foreign interests but also allows repressive governments to control its citizens (Chander & Sun, 2021). Secondly, it overlooks the various local contexts that shape the quotidian uses of the internet on the continent: the fact that African nations do not have 'digital sovereignty' does not necessarily mean that they are victims of monolithic digital colonialism. In this essay, I argue for a shift to a 'people-centred' narrative of digital sovereignty that highlights contextual elements of resistance that make up the everyday uses of the internet and digital platforms in Africa, thus opening up opportunities to consider more egalitarian forms of internet governance in this context.

Contesting the Framing Effects of 'Digital Colonialism'

The term 'digital colonialism' describes, in various ways, the position of power that Chinese and Western technology companies wield over global southern states, including those in Africa. Michael Kwet (2019:7-8) describes this aptly: Under digital colonialism, foreign powers, led by the United States, are planting infrastructure in the Global South engineered for its own needs, enabling economic and cultural domination while imposing privatized forms of governance. To accomplish this task, major corporations design digital technology to ensure their own dominance over critical functions in the tech ecosystem. This allows them to accumulate profits from revenues derived from rent (in the form of intellectual property or access to infrastructure) and surveillance (in the form of big data). It also empowers them to exercise control over the flow of information (such as the distribution of news and streaming services), social activities (like social networking and cultural exchange) and a plethora of other political, social and economic and military functions mediated by their technologies.

Other scholars have also considered this question, most notably Abeba Birhane (2020), Danielle Coleman (2019) and Nick Couldry and Ulises Mejias (2019), who all specifically draw inferences between historical colonialism and the new era of digital colonialism/data colonialism/algorithmic colonisation. In the face of this inequality, is it possible to articulate a narrative of digital sovereignty in Africa? I consider this question while contesting the very narratives of digital colonialism that have structured this conversation.

Context Matters

Fundamentally, we cannot understand technology and inequality in different societies on the basis of similar factors – the effects of technology are a product of its interaction with ideology and institutions, *but* under a background of historical circumstances of political, economic and social struggle that differ from population to population (Benkler, forthcoming).

The notion of digital colonialism has mostly emerged as an extension of critiques of big tech companies in the US and Europe (as exemplified in Shoshana Zuboff's (2019) work on surveillance capitalism) to global southern countries.[7] Although helpful in this regard, narratives of digital colonialism universalise technological diffusion and its effects, regardless of the historical and material realities of the different societies in question. While also useful in explaining the place of transnational tech corporations in the global digital economy, these narratives fail to take into account the confluence of legal-political and economic factors in each state's vision of its digital economy, and how these factors affect digital development and governance. Notably, Bulelani Jili (2020) discusses the ways in which African agency is overlooked in contemporary Africa-China relations. He notes that, while the political imbalance between African states and China is a matter of concern, African governments exercise more agency than is purported in China-Africa developmental relations, and gives examples of how governments in Ethiopia, Zimbabwe and Uganda have actively shaped their digital development (including surveillance) in collaboration with China and multinationals like Huawei (Jili, 2019, 2020) Similarly, narratives of digital colonialism shield the actions of states from scrutiny – it is not that African states are so helpless in the face of the demands of big tech, but the ideologies propagated by these corporations often and typically complement many states' sociotechnical imaginaries. For instance, Kenya's digital transformation strategy sees Kenya's role in Africa's digital economy as being to serve as a "test bed for new ideas enabling multi-sided platforms in emerging digital economy context" (Republic of Kenya, 2019:82). The only error in this vision is that it sees Africa's digital economy as being separate from the global digital economy that shapes and constrains it. Other than that, it is fully

[7] Some scholars, however, extend this discussion to the global level rather than to global south countries only. See, for example, Nick Couldry and Ulises Mejias (2019), who argue that the current era we live in involves a double transformation of capitalism and a new colonialism – data colonialism.

on board with multi-sided platform models and recognises the role of private sector enterprises as "primary drivers of digital economy across digital infrastructure, financial services, platforms, entrepreneurship, skills and values" (Republic of Kenya, 2019:76). The country's vision of a digital regulatory policy also complements this narrative and reflects the lukewarm attitude that many African governments have towards big tech corporations, except when they directly challenge state power, as seen in Nigeria (Maclean, 2021) and Uganda (Dahir, 2021).

The vision of a digital regulatory policy must take cognizance of the fact that digitization is a business project, and accordingly, room must be provided for the development of enterprising investments, product innovation and new data-based services (Republic of Kenya, 2019:76). Another problematic aspect of the notion of digital colonialism is that it obscures the agency of the 'colonised' populations and further marginalises them. Technology functions within a politically and culturally differentiated space, and its diffusion, use and/or resistance would be highly dependent on that context (Arnold, 2005) and, most importantly, is not determinate.

In fact, contrary to popular digital colonialism narratives, digital platforms operating in Africa function within a context of poverty, widespread informality/dualism, weak rule of law, hybrid political regimes, and diminished opportunities for political participation, all of which together influence the use of these platforms. These factors shape the agency of internet users: whereas there were previously limited opportunities for political participation, social media platforms have fuelled online activism across the continent and championed what I would call 'quotidian revolutions'' in many African countries, including Kenya (Nyabola, 2018), Nigeria, Ghana, Zimbabwe, Uganda, South Africa and Tanzania. Similarly, limited economic opportunities have fuelled the rise of the creative economy in African countries, with many people now earning their income through content creation on platforms like YouTube, TikTok and Facebook (Boakye, 2021). They have built huge online audiences and found ways to earn more money, besides the surveillance/advertising model of these platforms. Some content creators incorporate voluntary payment methods to supplement the income they receive from advertisements. Moreover, there is now widespread recognition by online audiences that content creators earn income through advertisements; some voluntarily watch online advertisements in support of their favourite comedians, for instance.

The framing effect of digital colonialism denies us the opportunity to examine the functions that digital platforms serve in different contexts, and to critically assess the distribution of power within the specific set of relations concerned. For instance, rather than completely dismiss platforms and the companies that own them as propagators of digital colonialism, one may want to examine the distribution of power between platforms and content creators, and uncover the ways in which

laws can change to increase economic opportunities for content creators. Recent research has shown that the power of social media platforms goes beyond free speech and constitutional ramifications to private law questions that affect the livelihood of small businesses, independent creators and political activists (Filmar *et al.*, forthcoming).

In sum, the notion of digital colonialism diminishes the agency of both states and individuals in the digital economy, presents an unfair choice between internet access and impending 'colonialism', universalises the process of historical colonialism – whose significance cannot be gainsaid and, lastly, makes the idea of digital sovereignty particularly untenable in the African context.

Searching for Digital Sovereignty

Digital sovereignty is largely an elastic concept that is invoked by different actors to legitimise the exercise of power and control over the digital landscape, including data, content, technologies and related infrastructure. States invoke it to assert control over their 'cyber-jurisdictions' for purposes of digital development and national security. Groups such as indigenous peoples and social movements invoke it as a form of anti-imperialist struggle to assert their right to control their technological systems and data, and their freedom to pursue their ends (Couture & Toupin, 2019).

In the African context, digital sovereignty has been discussed with regard to the development of a homegrown economy through digitisation; the growth of local technological start-ups; the integration of digital technologies into national sectors such as finance, health and agriculture; the establishment of smart cities; and the boosting of internet connectivity through building internet infrastructure, including local data centres. However, this discourse is more aspirational than practical at the moment and, even when moves are made to establish critical infrastructure such as data centres, it is typically through the financing and technical support from China's multinationals or US tech companies, which does not lay to rest concerns over external control of data (Erie & Streinz, 2021). The imbalance of power in the global digital economy renders efforts to attain this mode of digital sovereignty mostly untenable, yet unknown. Proposals have been made for African states to intensify efforts to reclaim infrastructural control by developing independent internet infrastructure to lessen dependencies (Fisher & Streinz, 2021), enacting strong data protection laws, mandating data localisation and, most recently, to carefully design the e-commerce protocol for the African Continental Free Trade Area to promote African interests (Kathure, 2021).

Fundamentally, digital sovereignty is a reflection of the distribution of power (Vatanparast, 2020) among different actors, and it would be a mistake to think of (1) actors as comprising of states and private technology corporations only and (2) the concept of digital sovereignty as being in fixed form. Here I echo the definition of power proposed by Roxana Vatanparast, viz. power is "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances" (Barnett & Duvall, 2005, cited in Vatanparast, 2020:6). Similarly, Yochai Benkler (forthcoming) defines power as a property of a relationship between A and B, describing A's capacity to shape B's behavior, outcomes, or context so that the respective behaviors, outcomes, or context of A and B's relations is closer to A's preferred relations than to B's short term or long term.

The previous section of this essay underscored the importance of internet users as legitimate actors who pursue certain political and economic goals with varied degrees of success, broadly defined. Conceptions of digital sovereignty in Africa need to reflect this reality – a reality that is grounded in people-centred approaches to development and freedom. This conception echoes anti-imperialist notions of technological sovereignty that have been advanced in the context of indigenous peoples and social movements. If applied within the African context, it may also allow the fulfilment of policy-oriented objectives concerning data governance through data collectives, data trusts and data cooperatives, which are very critical given the nature of hybrid political regimes and the risks of state surveillance.

Most importantly, this conception of digital sovereignty also opens up opportunities to examine how law mediates relations between states, private companies and internet users transnationally, and the ability to challenge legal arrangements that negatively affect the interests of users seeking economic and social justice. Such a conception of digital sovereignty further allows us to do what Vatanparast (2020) terms a re-politicisation of social problems, rather than allowing them to be managed by global expert regimes comprising of corporations, states and regulatory authorities.

Conclusions

Re-examining the framing effects of 'digital colonialism' opens up paths to a new contextualisation of digital sovereignty in the African context. While digital imperialism is a factor that nations have to contend with, re-politicising relations amongst states, corporations and internet users allows us to uncover not only the agency of African governments in allowing foreign domination in exchange for efficiency and digital development but, most importantly, the agency of users who pursue social and economic justice through their online activities – whether in political activism or content creation. We have further seen that conceptualising digital sovereignty as a reflection of the distribution of power among actors can enable the critical

examination of legal arrangements between states, tech corporations and justice-oriented users in order to improve the ends and outcomes of such users. With this conception, digital sovereignty in Africa would not be too bleak.

References

Arnold, D. (2005). Europe, technology and colonialism in the 20th century. *History & Technology*, 21(1):85-106.

Benkler, Y. (forthcoming). Power and productivity: Institutions, ideology, and technology in political economy. In *Political economy and justice*. Edited by Allen, D., Benkler, Y., Downey, L., Henderson, R. & Simons, J. Chicago: University of Chicago Press.

Birhane, A. (2020). Algorithmic colonialization of Africa. *SCRIPTed*, 17(2):389-409.

Boakye, B. (2021, April 19). Social media futures: Changing the African narrative. *Tony Blair Institute for Global Change* [Blog post]. Available from: https://institute.global/policy/social-media-futures-changing-african-narrative [Accessed 28 July 2021].

Chander, A. & Sun H. (2021). Sovereignty 2.0. *Georgetown Law Faculty Publications and Other Works*, 2404.

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24:417-439.

Couldry, N. & Mejias, U. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Palo Alto, CA: Stanford University Press.

Couture, S. & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10):2305-2322.

Dahir, A.L. (2021, January 13). Uganda blocks Facebook ahead of contentious election. *The New York Times*. Available from: https://www.nytimes.com/2021/01/13/world/africa/uganda-facebook-ban-elections.html [Accessed 28 July 2021].

Erie, M.S. & Streinz, T. (forthcoming). The Beijing effect: China's 'Digital silk road' as transnational data governance. *NYU Journal of International Law & Politics*.

Filmar, M.P., Elkin-Koren, N. & Gregorio, G.D. (forthcoming). Social media as contractual networks: A bottom up check on content moderation. *Iowa Law Review*.

Fisher, A. & Streinz, T. (2021). *Confronting data inequality*. World Bank Development Report 2021 background paper, IILJ Working Paper 2021/1, NYU School of Law, Public Law Research Paper No. 21-22. Available from SSRN: https://ssrn.com/abstract=3825724 or http://dx.doi.org/10.2139/ssrn.3825724 [Accessed 28 July 2021].

Jili, B. (2019, July 2). Tuning surveillance software with African faces. *Africa is a country* [Blog post]. Available from: https://africasacountry.com/2019/07/tuning-surveillance-software-with-african-faces [Accessed 28 July 2021].

Jili, B. (2020, April 20). Locating African agency in Africa-China relations. *Africa is a country* [Blog post]. Available from: https://africasacountry.com/2020/04/locating-african-agency-in-africa-china-relations [Accessed 28 July 2021].

Kathure, M. (2021, June 16). Africa's digital sovereignty: Elusive or a stark possibility through the AfCFTA? *Afronomicslaw* [Blog post]. Available from: https://www.afronomicslaw.org/category/analysis/africas-digital-sovereignty-elusive-or-stark-possibility-through-afcfta [Accessed 28 July 2021].

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the global South. *Race & Class*, 60(4):3-26.

Maclean, R. (2021, June 5). Nigeria bans Twitter after president's tweet is deleted. *The New York Times*. Available from: https://www.nytimes.com/2021/06/05/world/africa/nigeria-twitter-president.html [Accessed 28 July 2021].

Nyabola, N. (2018). *Digital democracy, analog politics: How the internet era is transforming politics in Kenya*. London: Zed Books.

Republic of Kenya. (2019). *Digital economy blueprint: Powering Kenya's transformation*. Available from: https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf [Accessed 28 July 2021].

Vatanparast, R. (2020). Data governance and the elasticity of sovereignty. *Brooklyn Journal of International Law*, 46(1):1-38.

Zuboff, S. (2019). *The age of surveillance capitalism*. New York: Public Affairs.

Chapter 10

Yes to Data Privacy, But Whose Data Privacy?

Michael Asiedu

Introduction

Digitalisation, which involves the manner in which various aspects of our lives are made possible through digital communication and media infrastructure (Brennen & Kreiss, 2014), has a significant effect on our lives. Virtually every part of our lives – from the way technology-savvy (techy) people use the internet to how a rural farmer in central Kenya receives meteorological information via mobile service (m-service) (Krell et al, 2021) – has a digital footprint. These digital footprints are made possible through the use of data. Data here involves personal information such as gender, age, location, address, etc. When data is mentioned, the concept of privacy is suddenly brought to the fore, especially with the global concern surrounding increasing threats to the data privacy of individuals, not only from governments but also from the technologies they use (Euronews, 2021). But whose privacy is referred to when the term is used? Is the rural farmer's privacy given the same prominence as that of the techy? This somewhat fundamental question of ownership, control and access to data is arguably one of the cornerstones of the broader contestation of digital sovereignty. This short paper contributes to the growing conversation. It does so by first situating some of the arguments on privacy and its attendant paradox in a setting closer to the rural farmer (individual) in Africa, whose data should matter too. Second, it highlights some of Africa's legislation on data privacy so far, and finally acknowledges that, while legislation on data privacy is non-negotiable, such legislation will be incomplete without a data access principle (DAP).

The fundamental notion of privacy is that of information being intrinsically sensitive to an individual, hence an individual is selective in relaying such information. The ability to be circumspect in how to deal with one's data is what forms our understanding of data privacy. Thus, we should decide who can have access to our data – whether we are operating online or participating in a national biometric registration exercise rolled out by the government; the fact that we do not is the problem. Data privacy or information privacy is therefore viewed as the legal concept, while how our data is protected deals with the technical framework necessary for the proper handling of sensitive data. This includes confidential data such as health records, financial data, as well as intellectual property data necessary to meet a given regulatory demand (The Storage Networking Industry Association [SNIA], 2021).

Setting the legal boundaries of what personal data is and what it is not is also not a routine demarcation. Any information that can contribute either directly or indirectly to uncovering the

identity of a natural individual (Article 4, General Data Protection Regulation [GDPR], 2018) could be classified as personal data. The assumption that data is personal also connotes that some data could not be personal (Finck & Pallas, 2020). The right to privacy is enshrined in a host of international and local legal documents, and this portrays its importance; when data is personal (personal data), it becomes vulnerable to privacy threats, but the same cannot be said for non-personal data (Makulilo, 2015). For instance, information about the budget of a public museum could easily be accessed (non-personal data), while information on the contributions of donors to that same museum could be shrouded in privacy laws and protection (personal data) if such donors so choose, unless the museum policies demand otherwise. Who decides which information is available, its value, how it is used and for what purpose itself evokes a paradox in terms of privacy.

A Privacy Paradox?

There are competing claims about the premium individuals place on their privacy (Barth & De Jong 2019; Hargittai & Marwick, 2016; Solove 2020; Wittes & Kohse, 2017). The first deals with behaviour valuation, where it is postulated that behaviour forms the utmost mode of measurement in terms of evaluating how people value privacy. It is argued that people place a low premium on their privacy and, in some instances, easily trade it for goods and services. It follows that, if people value their privacy in such a low manner, then there is no need for excessive privacy regulation (Hughes-Roberts, 2012; Solove, 2021). On the other hand, another argument deals with behaviour distortion, a scenario in which people's behaviour is not an accurate reflection of their preferences. Precisely, behaviour is distorted by factors such as manipulation and skewing, as well as biases and heuristics, etc. (Solove, 2020). For both arguments, Solove (2021) reveals the faulty logic embedded in them, for instance the behaviours involved in the privacy paradox demonstrate people making decisions on risk in very particular contexts. He is of the opinion, however, that people's decisions on privacy are much more general in nature; hence, using a select few cases to generalise broader conclusions on how people perceive privacy is a leap in logic, but one that is most certainly faulty. Again, people may make faulty data decisions based on unawareness and lack of insight (Barth & De Jong, 2019; Harsanyi, 1967). Thus, behaviour regarding privacy choices will not necessarily lead to a conclusion for minimal regulation, just as reducing behavioural distortion will not cure individual lapses to protect their own privacy (Solove, 2021).

Again, in the light of the first argument on behaviour valuation, recent occurrences involving data breaches with firms such as Cambridge Analytica, which affected elections not only in countries in the West but also in African countries like Nigeria and Kenya (Ekdale & Tully, 2019), have ignited concerns on the value people place on their personal data, even if these people are some of

Africa's largely urban class or netizens who are deemed more techy (Ekdale & Tully, 2019). While people on the grassroot level (perhaps the rural farmer in central Kenya) might not relate to Cambridge Analytica data breaches, they (he or she) certainly become concerned with m-service-related crimes involving mobile money (MoMo) fraud – what next could this fraudster do with his or her personal information such as mobile number, MoMo account details, address, etc. Yet, Srinivasan et al. (2018:4) portray in their research that "low-income population may be attuned in particular to exchange their details for welfare benefits". Such groups of people also tend to use information and communications technology (ICT) services rather passively; thus, only when they are mandated to do so to access critical services related to their livelihoods, as demonstrated by research in South Africa (Gillwald et al., 2018). These few examples reveal the embedded deficiencies (factors) within data privacy in Africa, for instance people with frequent access to ICT usage, let's say "digital haves" and "digital have nots", infrastructural deficits in terms of connectivity, more urban techy people in comparison to rural inhabitants, or plainly the high cost of data to access internet services (Corrigan, 2020; United Nations Conference on Trade and Development [UNCTAD], 2003). Here, the inability of people who are not using ICT services will not be due to a people lacking in agency, but rather a myriad of these factors or a combination of two or more. Hence, beyond the questionable dichotomies between the arguments put forward about the privacy paradox, privacy should be viewed through a broader lens rather than a binary lens, especially when Africa and its techy versus not techy people are in the picture. Also, our thinking on privacy should not be honed solely on the individuality nature of rights, as postulated by the Universal Declaration of Human Rights (UDHR), but inspiration could be drawn from its African counterpart in the African Charter on Human and People's Rights (ACHPR). Here, too, the concept of *Ubuntu* and the communal nature of African communities should be taken into consideration (Boshe, 2017; Razzano, 2021).

African Legislation and Data Privacy

In terms of legislation, the argument that African "group interests" (communal) should precede singular interests due to the culture of collectivism is contestable and would progressively wither. This is because more and more people will become aware of the many ways in which digitalisation will thrive on data and will demand to be in charge of how their data is used (Hanno et al., 2007). Essentially, privacy is not some communal claim to certain codes of conduct, cultural practices or even ancestral lands. It comprises identifiable details about a particular individual. Hence, the notion of privacy being a Western construct, in which the individual becomes the centre, would arguably triumph. Simply put, it is my data and I need to know what is done to and with it – here, the view of the rural farmer in central Kenya should matter in the same manner as that of the techy in an urban setting in Africa. The European Union (EU) Data Privacy Directive has almost become the default pacesetter: future models may therefore be tailored on it, albeit adjusted to

local relevance. Across Africa, it is encouraging to see emerging legislation on privacy and data protection. According to the UNCTAD, 28 countries (52%) have passed legislation, with a further nine countries (17%) with draft legislation. Nonetheless, 13 countries (24%) have no legislation, with four countries (7%) having no data at all. Among the 28 countries with legislation, 15 have data protection authorities (DPAs) (Boakye, 2021). Overall, these projections do not look all gloomy. However, what is clear (apart from the resources necessary in terms of implementation and infrastructure, which is a challenge not only in Africa but in the West as well) is the inability of this legislation to boldly enshrine data access principles (DAP), which could add an extra impetus to the overall data privacy debate. Below, I put forward enshrining DAP as a policy recommendation.

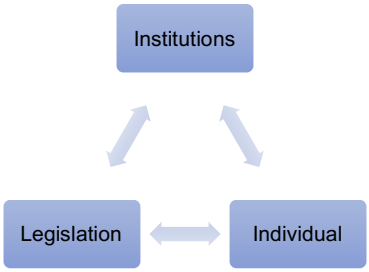
DAP as a Way Forward

DAP is not a new principle; in fact, it is "perhaps the most important privacy protection safeguard" (OECD, 1989, para 58; see also Bygrave, 2001). The General Data Protection Regulation (GDPR) includes it as the right of access. African legislation should boldly enshrine and champion it too, but this is a continent where right to information (RTI) bills in various countries are still a hard ask; less than half of African countries have such laws (African Freedom of Expression Exchange [AFEX], 2017). Enshrining DAP and championing it boldly will lead to what I call the "Trifactor Approach" in addressing data privacy issues. A trifactor approach is a combination of institutions, legislation and individual agency to deal with issues of privacy, acknowledging that attempting to address privacy issues should be a three-pronged approach. Individual management of privacy is a complex endeavour that is almost impossible to achieve holistically. Essentially, enacting appropriate legislation alone cannot solve the problem, likewise designated institutions alone cannot get the job done, but perhaps this is where the individual comes in with the trifactor approach, which is when and if legislation and future data privacy acts (DPAs) include DAP in their formulation. This DAP will operate in such a way that the individual (citizen or resident) has the right to request his or her data from a data holder or controller in theory (Tsui & Hargreaves, 2019). Here, customers could ask public institutions, private companies that operate with customer data such as telecommunication companies, social media companies, delivery services, etc. about the status of their data when they feel concerned. In Hong Kong, the principle was applied to allow residents to alert data holders if their information changed or was inaccurate (see Tsui & Hargreaves, 2019).

In countries in Africa, however, the DAP could be applied not only for residents to update their details when something changes about them or they realise that information is incorrect, but also to legitimately demand answers on how their personal data is being stored and used, or whether there is a third party involved about which they know nothing. This is based on the understanding

that data protection institutions (DPIs), including government authorities and legislation, cannot do the job alone. The individual here comes in to complete the three-pronged approach (trifactor) to make data holders accountable.

Figure 1. The Trifactor Approach to Data Privacy



Source: Author's diagram

The DAP itself gives power to the person (citizen or individual) involved, and the person becomes aware of which details about him or her are easily obtainable by a third party. Even more importantly, the DAP empowers each person on a structural level, in the sense that each person demonstrates a level of surveillance of institutions holding data, even if this is limited. It therefore is something of a countersurveillance approach (Tsui & Hargreaves, 2019) – watching the institutions watching us to promote responsibility, accountability and transparency. An added incentive is the fact that the DAP allows people to act for collectives as well; for instance, civil society and community leaders could champion the rights of Africa's not so techy people, including the rights of the rural farmer in central Kenya. Essentially, while everybody's right to access and data privacy matters should triumph on an individual basis, this would also create room for a collective approach. In this way, data privacy becomes intrinsic, not only for techy people, but for "non-techies" as well.

References

African Freedom of Expression Exchnage [AFEX]. (2017). 22 African Countries have passed access to information laws. Available from https://www.africafex.org/access-to-information/22-african-countries-that-have-passed-access-to-information-laws.

Barth, S. & De Jong, M.D.T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and Informatics*, 34(7):1038-1058. https://doi.org/10.1016/j.tele.2017.04.013.

Boakye, B. (2021). Tech policy in Africa: Emerging trends in internet law and policy. *Tony Blair Institute for Global Change*. Available from: https://institute.global/policy/tech-policy-africa-emerging-trends-internet-law-and-policy.

Boshe, P. (2017). *Data protection legal reforms in Africa*. Doctoral thesis, University of Passau, Germany.

Brennen, S. & Kreiss, D. (2014). Digitalization and digitization. *Culture Digitally*. Available from https://culturedigitally.org/2014/09/digitalization-and-digitization/.

Bygrave, L.A. (2001). Core principles of data protection. *Private Law and Policy Reporter*, 7(9):169. Available from http://www.austlii.edu.au/au/journals/PLPR/2001/9.html.

Corrigan, T. (2020). *Africa's ICT infrastructure: Its present and prospects*. Policy Briefing 197, African Perspectives Global Insights, South African Institute of International Affairs. Available from https://www.africaportal.org/publications/africas-ict-infrastructure-its-present-and-prospects/.

Ekdale, B. & Tully, M. (2019). African elections as a testing ground: Comparing coverage of Cambridge Analytica in Nigerian and Kenyan newspapers. *African Journalism Studies*, 40(4):27-43. doi:10.1080/23743670.2019.1679208.

Euronews. (2021). Big tech companies exposed to privacy challenges after EU Court decision. Available from https://www.euronews.com/2021/06/15/big-tech-companies-exposed-to-privacy-challenges-after-eu-court-decision.

Finck, M. & Pallas, F. (2020). They who must not be identified – Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1):11-36. https://doi.org/10.1093/idpl/ipz026.

General Data Protection Regulation (GDPR) (2018). https://gdpr-info.eu.

Gillwald, A., Mothobi, O. & Rademan, B. (2018). *The state of ICT in South Africa*. Policy Paper No. 5, Series 5: After Access. Available from https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf.

Hanno N.O., Britz, J.J. & Olivier, S.M. (2007). Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa. *International Information & Library Review*, 39(1):31-43. doi:10.1080/10572317.2007.10762729.

Hargittai, E. & Marwick, A. (2016). "What can I really do?" : Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10:3737-3757.
Harsanyi, J.C. (1967). Games with incomplete information played by "Bayesian" players, I-III Part I. The basic model. *Management Science*, 14(3):159-182. Available from http://www.dklevine.com/archive/refs41175.pdf.

Krell, N. T., Giroux, S. A., Guido Z., Hannah, C., Lopus, S. E., Caylor, K. K. & Evans, T. P. (2021.) Smallholder farmers' use of mobile phone services in central Kenya, Climate and Development, 13:3, 215-227, DOI: 10.1080/17565529.2020.1748847.

Makulilo, B.A. (2015). Myth and reality of harmonization of data privacy in Africa. *Computer Law and Security Report*, 31(1):78-89. https://doi.org/10.1016/j.clsr.2014.11.005.

OECD. (1989). *OECD guidelines on the protection of privacy and transborder flows of personal data*. Available from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Razzano, G. (2021). Understanding the theory of collective rights: Redefining the privacy paradox [Concept Note]. *Research ICT Africa*. Available from https://researchictafrica.net/publication/concept-note-understanding-the-theory-of-collective-rights-redefining-the-privacy-paradox/.

Roberts, T.H. (2012). A cross-disciplined approach to exploring the privacy paradox: Explaining disclosure behaviour using the theory of planned behavior. *UK Academy for Information Systems Conference Proceedings, Paper 7*. Available from http://aisel.aisnet.org/ukais2012/7.

Solove, D.J. (2021). The myth of the privacy paradox. *89 George Washington Law Review 1 (2021), GWU Legal Studies Research Paper No. 2020-10, GWU Law School Public Law Research Paper No. 2020-10*. Available from SSRN: https://ssrn.com/abstract=3536265 or http://dx.doi.org/10.2139/ssrn.3536265.

Srinivasan, J., Bailur, S., Schoemaker, E. & Seshagiri, S. (2018). The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication*, 12:1228-1247.

The Storage Networking Industry Association (SNIA). (2021). *What is privacy?* Available from https://www.snia.org/education/what-is-data-privacy.

Tsui, L. & Hargreaves, S. (2019). Who decides what is personal data? Testing the access principle with telecommunication companies and internet providers in Hong Kong. *International Journal of Communication*, 13:1684-1689. Available from https://ijoc.org/index.php/ijoc/article/view/8232/2620.

United Nations Conference on Trade and Development (UNCTAD). 2003. *Data protection and privacy legislation worldwide*. Available from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Wittes, B. & Kohse, E. (2017). *The privacy paradox 11: Measuring the privacy benefits of privacy threats*. Center for Technology Innovation at Brookings. Available from https://www.brookings.edu/wp-content/uploads/2017/01/privacy-paper.pdf.

Chapter 11

Africa's Tech Solutionism vs Digital Sovereignty – Digital ID Systems in Post-Pandemic World

Oarabile Mudongo

Introduction

The ambition of bolstering digital sovereignty, self-determination and strategic autonomy has recently become a focal point of global digital policy discourse. With so many different interpretations of digital sovereignty by various scholars (e.g. Fleming, 2021; Pohle & Thiel, 2020), a clear or at least consistent understanding of what this means, what it entails and why it matter is still to be discovered, particularly in Africa (Vahisalu, 2019; Velluet, 2021). This notion is frequently associated with diverse interpretations in the socio-political-economic context. Several authors have tried to define digital sovereignty in broader terms as overcoming dependency on foreign data and digital assets, implying that states are working to achieve resilience in cyberspace, and autonomy (Moerel & Timmers, 2021).

While Africa battles COVID-19 (Schwikowski, 2021), the pandemic has also served as a political lens and amplifier for data-driven technologies (Botes & Pepper, 2020; Taylor, Sharma & Martin, 2020:35). The novel coronavirus pandemic has highlighted the significance of transitioning to and embracing, contactless interactions. The pandemic has reshaped people's relationships with technology, state control and democracy in our societies, with many African nations under government-imposed lockdowns and curfews, or being subject to surveillance, either through contact tracing technologies or digital identity systems. As a result, many African governments have taken the lead in driving the adoption and deployment of digital identity systems (Milken Institute, 2020; Toesland, 2021).[8] However, at the intersection of these technologies, data privacy and human rights have been emerging as key issues underlying Africa's digital policy space, and the lack of compliant policy frameworks for digital ID implementation necessitates policy intervention.

Digital ID Revolution: Trends in Africa

Digital ID systems offer significant benefits to bridge the digital gap and increase access to digital services. They are a crucial component of financial inclusion, including access to public services,

[8] See the project site of the Milken Institute's Global Market Development Practice on COVID-19 Africa Watch, which tracks major developments and policy announcements from across the continent here: https://covid19africawatch.org/the-case-for-digital-identity-in-africa-during-and-post-covid-19/

economic growth, migration (which is vital to participate fully in our modern society), and even dealing with crises such as the Covid-19 pandemic (Joshi, 2021). Across Africa, many states have undertaken efforts to embrace digital identity systems. As a result, providing a legal identity for all by 2030 is one of the main focuses for achieving the United Nations Agenda for Sustainable Development. African states have been leading various digital ID projects in this area, in sectors such as public service, trade and economic development, with the mandate to execute and fulfil the Sustainable Development Goals (SDGs) and the 2020–2030 African digital transformation strategy (African Union, 2019). Many experts have contended that progress toward this goal should begin in Africa, home to more than 40% of the world's undocumented people (World Bank, 2017). But one of the questions that must be addressed in the context of these developments (to make a case) is why now, in the midst of the pandemic, governments are pushing the subject of digital identity. To better understand the trends of digital ID in Africa, this article brings to light emerging developments and potential influences that these technologies are likely to have in the post-pandemic period, as well as broadening our understanding of the interplay between government, economies, and the civil population in the provisioning of public services.

The deployment of biometric and digital identity systems across Africa has been mapped from pre-pandemic to current scenarios – from Ethiopia's Digital ID for Refugees, which provides a comprehensive and seamless service to UNHCR refugees and other private partners (Taye, 2019), Togo's Novissi, a financial transfer scheme designed to assist people in need during a pandemic,[9] to the Zimbabwean biometric voter ID system and Huduma Namba in Kenya (Macdonald, 2021a, 2021b). These are a few of the many examples of how governments have been utilising these technologies to transform the biometric and identification ecosystem on the African continent. And this demonstrates just how much effort states put into investing in these systems, while also opening up the constitutional guarantees of citizens in a limited sense.

The overall benefits of digital IDs are sometimes linked intimately to financial inclusion. Furthermore, having a service strategy that benefits citizens and demonstrating a strong political will to change are critical considerations. However, given the post-pandemic era and these specific circumstances, digital IDs may bring beneficial digital sovereignty in an ideal society. This is in contrast to the following optimistic futuristic scenarios: Solutions developed by the private sector based on state-sponsored digital identity systems, data being used to generate algorithmically determined identity verification, or digital identity that is decentralised and controlled by the user – many experts highlight the lack of public and civil society involvement, which raises concerns

[9] https://novissi.gouv.tg/en/home-new-en/

about human rights, data privacy, and protection in the use of these technologies (Beduschi, 2021).

Yet these systems can perpetuate "exclusion-by-design" and are often deployed unchecked, hence much of the potential effects of these systems have been associated more widely with exclusionary practices, unintended adverse consequences affecting mostly vulnerable and marginalised populations, discrimination and biased algorithms. For instance, persons with disabilities, such as those who do not have hands, can be turned away because they are unable to submit fingerprints. Several researchers are calling for the development and adoption of a policy framework to address these issues (Van der Spuy, 2021), whereas others doubt the readiness of African governments to embrace digital identity systems because of their susceptibility to abuse (Van Veen & Cioffi, 2021). Although a legislative framework may seem an adequate alternative option to address these challenges, the background to this argument is that Africa still has insufficient data protection and privacy laws. From a total of 54 countries, only 28 (52%) have legislation on personal data, nine (17%) have their legislation at the draft stage, 13 (24%) have no legislation and four (7%) countries have no data or legislation at all.[10]

However, considering the risks associated with the design and implementation of digital ID systems, especially the manner in which they are built as massive, monolithic, national ID initiatives, the potential arises that, if the information is misused, it may allow the persecution of individuals by authorities based on their ethnic origin.

Even in the presence of a legal framework aimed at protecting fundamental rights, the design and deployment of digital ID systems requires a risk-based assessment approach. Often, these systems are prone to vulnerabilities, such as human rights violations in the form of exploitation of people's personal data, ultimately infringing on their fundamental rights to privacy. In addition, states can use such technologies as tools for repression, creating a "surveillance state" in the way data is collected, processed and misused by authorities. Without existing governance frameworks, inequality is likely to increase the risk of exclusion of marginalised groups. In the case that actors fail to evaluate such dangers, the aim should be delineated properly and lawful, and such technologies should not be adopted unless there are no other, less-invasive means to achieve the same goals. With the expansion of surveillance technologies in Africa, the desire for African governments to control the flow of information in society and to spy on people has always persisted. Indeed, numerous African state security agencies have focused on this over the years.

[10] See the latest data of the United Nations Conference on Trade and Development on Data Protection and Privacy Legislation Worldwide: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Now, with the adoption of digital ID systems, these old wounds between state-citizen relationships are being reopened, which might erode trust.

Digital Sovereignty: Privacy, Surveillance and Rights

Most rules that still regulate the internet today were developed in the early 1990s, when the global internet public policy development process was still in its infancy (Gilliland, 2019). While the internet ecosystem was utterly different in the 1990s, most of its principles have recently sparked a divisive debate regarding the regulation of the global digital space. An exceptionalist and dominant view emerging from the literature presented the digital environment as a new alternative space where states, in particular, were viewed as illegitimate to enforce state sovereignty in cyberspace (Johnson & Post, 1996). Governments could intimidate, but they could not control user behaviour online; laws could be developed but not enforced, and private companies possessed de facto digital corporate sovereignty. As a result, self-regulation was adopted as the appropriate governing mechanism. A non-exceptionalist viewpoint, on the other hand, was less prevalent at the time. And now we have a world where states believe that the digital space can and should be regulated and that states have the legal authority to do so (Goldsmith & Wu, 2006). Many governments have attempted to establish control over the digital space, and the exceptionalist viewpoint is now irrelevant in today's digital world.

For instance, in the global north, leaders of the European Union recently have been calling for Europe's digital sovereignty to "foster the Digital Single Market in all its dimensions, where innovation can thrive and data can flow freely", whereas in the global south, countries like South Africa proposed a draft National Data and Cloud Policy to "promote South Africa's data sovereignty and security" (Dyer, 2021; ERR News, 2021). With these developments, the bigger question today is not whether the digital space is or should be regulated at all, but rather how. What should be the models of governance and who should assume this responsibility?

The problem of digital solutionism and the consequences of identification systems in the context of privacy, surveillance and human rights are central to this discussion. It is not an exaggeration to argue that these technologies have gradually taken on a central role in the way our societies operate. However, the primary question remains: will Africa's goals for digital sovereignty be realised with the imperialist technological dominance of global technology solutions tied by narratives of techno-solutionism and rescuing? This is especially relevant considering that existing public-private partnerships and multilateral agencies have been promoting the use of these technologies in Africa pre- and post-pandemic to connect communities to financial and public services. While the outcomes of these tech solutions have yet to be seen, their presence is obvious in several areas, particularly those that target marginalised communities.

At the core of these debates is the concept of 'data colonialism', which is critical for understanding not only how society interacts with new technologies, but also – and most importantly – how these technologies work in our society. Data colonialism is often characterised as the appropriation of big data by global technology companies in the data realm. Lately, this has become a widespread problem across the African continent. The underlying human relationship with data can be linked to implications that perpetuate inequalities, particularly 'digital inequality' in the global South (Van der Spuy, 2020). Zuboff (2018) warns us about the need to pay close attention to how powerful technology companies use our individual data. This is because these firms are the primary drivers of emerging technologies such as digital ID systems. Through these systems, they have been able to amass a massive amount of human-generated data produced by these technologies, which is changing the foundation of our society (Zuboff, 2018). This critical analysis can assist us in asking serious questions of state actors, as our response will ultimately determine whether or not a democratic society can thrive beyond digital identity technology. This is necessary because 'surveillance capitalism' is all about exploiting personal data with the primary goal of making profit out of it. Digitally networked systems produce big data, which is susceptible to generating an unequal class system that pits the controllers against the governed. This happens specifically through public-private partnerships in which the interests of private companies versus government do not always fulfil democracy ideals for people.

Realistic and holistic assessment of how citizens are accounted for across the 17 goals of the Sustainable Development Goals (SDGs) has been a crucial task for the United Nations mandate to measure progress toward digital policy (The Earth Institute, Columbia University, & Ericsson, 2016:28-31). Goal 16, on "peace, justice, and sustainable institutions", aims to "[p]romote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels". Goal 16.9, on identity, is included in this: "By 2030, provide legal identity for all, including birth registration."[11] Identity is crucial – the ability to establish who we are can give security and is a vital component of our right to exercise our basic rights.

This is especially evident in cases involving unregistered citizens, who frequently lack papers to demonstrate their identity, leaving them vulnerable to prejudice and abuse. While the SDG agenda on digital identity is an important issue to debate, there still are significant gaps in many African countries on the seriousness of human rights risks involved in digital IDs. Despite the fact that governments, multilateral agencies and tech companies actively adopt and encourage the use of

[11] https://sdgs.un.org/goals

digital ID systems, civilians often have limited knowledge of how they contribute to social inequality and violations of human rights, particularly among the poor and most vulnerable. This is why we have to interrogate existing public-private partnerships between states and the business sector to understand this business model.

Lack of "Oversight", Transparency and Accountability

Reflecting on the effects of COVID-19 on globalisation and multilateralism, as well as what it means for Africa's digital sovereignty and its ambitions in the global digital policy discourse, it is clear that many African countries have been striving to reposition themselves in order to meet and fulfil their aspirations. This necessitates the development of data protection regulations and other legal frameworks to govern how identification systems are used to collect personal data in this pandemic. If states and technology corporations are able to use these technologies, they must be subjected to robust policy requirements that strive to protect people and their personal privacy. Historically, identity data has only been accessed and possessed by the state, but the move to digital identification systems, through its operational processes, necessitates that third parties have access to user data. These third-party companies include, for example, technology corporations that deploy, operate and manage these systems.

As a result, states must implement tight access control and encryption measures to ensure that only authorised trustees, including third parties, can read or acquire data legally. Because these innovations are frequently deployed at the national level, state actors should take the initiative to impose control and accountability measures on companies that build these solutions and the clients who implement them, thereby ensuring complete data protection at all stages of the data development cycle. Citizens have the right to obtain knowledge about what information is being gathered about them and for what purpose, how their data will be used in decision-making, and to be notified of any changes to any situation, such as use for a particular reason or the motive to share the knowledge with a third party. Furthermore, transparency about identity systems' policies and infrastructure is paramount, especially for users who interact with these systems. They need to understand the frameworks, safety measures and processes in relation to consequences.

Recurrent issues relating to digital IDs include how transparency versus personal intents affect the roll-out of digital ID systems. Yet if reforms are imperative or cooperative among stakeholders, we need to consider the magnitude of data gathering and how individual and collective rights to privacy are affected. There are questions that are very critical to consider, such as: who benefits and is excluded from such technological initiatives; who has the right to access the data and for what reasons; and are the rights of citizens guaranteed against privacy breaches by any individuals, groups of individuals or private corporations.

Policy Implications and Recommendations

Numerous lessons are evolving from other digital ID systems that Africa can use as a model. The Indian Aadhar digital ID system might be a good example. Here, researchers have developed and used evaluation frameworks with three types of checks – "rule of law tests", "rights-based tests" and "risks-based tests" – to evaluate the potential impacts of the identity system. However, it is important to take into account that the Aadhar ID system has been subjected to security breaches and misuse of data. As a continent, what significant lessons can we gain from the Indian Aadhar identity system? Perhaps this framework might be adopted as a benchmark approach for assessing digital IDs in distinctively African contexts with our unique current problems.

However, existing regulatory and policy strategies have not addressed how digital identity systems may perpetuate exclusion errors and inequality in the developing countries of the global south, particularly in Africa. There are benefits linked to digital ID systems, such as improved record keeping and generation of administrative data, which can improve financial inclusion and credit market efficiency, since data records are used for operational purposes.

Despite the fact that existing regulatory and policy measures have not addressed how digital identity systems may perpetuate exclusion errors and inequality in developing countries of the global south, notably in Africa, there are also benefits linked to digital ID systems, such as improved record keeping and the generation of administrative data. These improve financial inclusion and credit market efficiency, since data records are used for government operational purposes. Therefore, we need to invest in multi-stakeholder efforts to develop a trust and interoperability framework for digital identification across the African continent and benefit from the opportunity to participate in the process directly.

While having a constructive discussion about policy approaches, we need to focus more on policies that protect individual privacy from the misuse of data, while also attempting to improve the lives of socially and economically disadvantaged people. African countries, in particular, must consider better ways to balance their technological development ambitions to foster inclusion and equality in digital technologies.

This article has explored some of the emerging digital ID and biometric identity systems in Africa and what we mean when we relate digital ID with achieving digital sovereignty in the post-COVID era. We looked at underlying concepts of privacy, human rights, data colonialism and surveillance capitalism, which are central to digital ID operations and digital sovereignty in Africa. In conclusion, as policymakers, we must ask whether we dare roll out digital IDs in our societies

without understanding their capabilities. Further, how can we assess the geopolitical and national interests of multilateral agencies that are part of this agenda? These questions are pertinent because, in relation to what happens after the pandemic and the threats that emerge as a result of these technologies, we stand to bear witness to our democratic governance being challenged, along with the danger that no one will take responsibility.

References

African Union. (2019). *The digital transformation strategy for Africa (2020-2030)*. Available from: https://www.tralac.org/documents/resources/african-union/3013-the-digital-transformation-strategy-for-africa-2020-2030/file.html.

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3:e15. doi:10.1017/dap.2021.15.

Botes, M. & Pepper, M. S. (2020, June 24). Balancing privacy with public health: How well is South Africa doing? *The Conversation*. Available from: http://theconversation.com/balancing-privacy-with-public-health-how-well-is-south-africa-doing-140759.

Cochetti, R. (2019, July 24). I helped write the rules for the internet in the 1990s: This is what we missed. *The Hill*. Available from: https://thehill.com/opinion/technology/454497-i-helped-write-the-rules-for-the-internet-in-the-1990s-this-is-what-we.

Dyer, L. (2021, April 12). South Africa: New draft national data and cloud policy. *Bowmans*. Available from: https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-new-draft-national-data-and-cloud-policy/.

ERR News. (2021, March 2). Estonia, EU countries propose faster 'European digital sovereignty'. *ERR*. Available from: https://news.err.ee/1608127618/estonia-eu-countries-propose-faster-european-digital-sovereignty.

Fleming, S. (2021). What is digital sovereignty and why is Europe so interested in it? *World Economic Forum*. Available from: https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/**.**

Goldsmith, J. & Wu, T. (2006). Who controls the internet? Illusions of a borderless world. *Columbia Law School. Scholarship Archive*. Available from: https://scholarship.law.columbia.edu/books/175.

Johnson, D. R. & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48(5):1367-1402. doi:10.2307/1229390.

Joshi, M. (2021, April 30). Digital identity can help advance inclusive financial services. *World Economic Forum*. Available from: https://www.weforum.org/agenda/2021/04/digital-id-is-the-catalyst-of-our-digital-future/.

Macdonald, A. (2021a, July 1). Biometric voter rolls at different stages in Zimbabwe, Papua New Guinea, Nigeria: From policy proposals to online pre-registration. *Biometricupdate.com*. Available from: https://www.biometricupdate.com/202107/biometric-voter-rolls-at-different-stages-in-zimbabwe-papua-new-guinea-nigeria.

Macdonald, A. (2021b, January 31). Kenya's Huduma Namba digital ID scheme could exclude millions of citizens, Forum warns. *Biometricupdate.com*. Available from: https://www.biometricupdate.com/202101/kenyas-huduma-namba-digital-id-scheme-could-exclude-millions-of-citizens-forum-warns.

Milken Institute. (2020, November 10). The case for digital identity in Africa during and post-COVID-19. *COVID-19 Africa Watch*. Available from: https://covid19africawatch.org/the-case-for-digital-identity-in-africa-during-and-post-covid-19/.

Moerel, L. & Timmers, P. (2021). *Reflections on digital sovereignty*. EU Cyber Direct, Research in Focus Series. Available from: https://ssrn.com/abstract=3772777.

Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). Available at: https://doi.org/10.14763/2020.4.1532.

Schwikowski, M. (2021, March 11). Africa's battle with COVID-19 continues, one year on. *Deutsche Welle*. Available from: https://www.dw.com/en/africas-battle-with-covid-19-continues-one-year-on/a-56838418.

Taye, B. (2019). Digital ID in Ethiopian refugee camps: A case study. *The Engine Room*. Available from: https://digitalid.theengineroom.org/assets/pdfs/[English]%20Ethiopia%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf.

Taylor, L., Sharma, G. & Martin, A. (2020). *Data justice and COVID-19: Global perspectives*. London: Meatspace Press. Available from: https://issuu.com/meatspacepress/docs/msp_data_justice_covid-19_digital_issuu.

The Earth Institute, Columbia University & Ericsson. (2016). *Digital identity and the sustainable development goals*. The Earth Institute, Columbia University, pp. 28–31. Available from: https://www.jstor.org/stable/resrep15879.9.

Toesland, F. (2021, February 5). African countries embracing biometrics, digital IDs. *Africa Renewal*. Available from: https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids.

Vahisalu, R. (2019, May 15). Digital sovereignty: The key to safeguarding Africa's booming digital economy. *Global Voice Group*. Available from: https://www.globalvoicegroup.com/digital-sovereignty-the-key-to-safeguarding-africas-booming-digital-economy/.

Van der Spuy, A. (2020, Mach 23). Colonising ourselves? An introduction to data colonialism. *Research ICT Africa*, 23 March. Available from: https://researchictafrica.net/2020/03/23/colonising-ourselves-an-introduction-to-data-colonialism/.

Van der Spuy, A. (2021, June 21). Why digital ID matters. *Research ICT Africa*. Available from: https://researchictafrica.net/2021/06/21/why-digital-id-matters/.

Van Veen, C. & Cioffi, K. (2021, April 6). Everyone counts! Ensuring that the human rights of all are respected in digital ID systems. *NYU School of Law: Center for Human Rights and Global Justice*. Available from: https://chrgj.org/2021/04/06/everyone-counts-ensuring-that-the-human-rights-of-all-are-respected-in-digital-id-systems/.

Velluet, Q. (2021, April 16). Can Africa salvage its digital sovereignty? *The Africa Report*. Available from: https://www.theafricareport.com/80606/can-africa-salvage-its-digital-sovereignty/.

World Bank. (2017). The state of identification systems in Africa: Country briefs. *The World Bank*. Available from: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/298651503551191964/The-state-of-identification-systems-in-Africa-country-briefs.

Zuboff, S. (2018). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Penguin Publishing Group. Available from: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

Chapter 12

Big Tech: Not-so-Simple Politics

Odilile Ayodele

Introduction

When Twitter CEO Jack Dorsey announced in 2020 that he was moving to Africa in his personal capacity, it was a signal that the new frontier in technology was on the African continent. Before Dorsey's announcement, there were steady investments on the African continent, but his anticipated move shone a light on the continent's potential. The African continent represents one of the most exciting expansion opportunities: Africa has one of the world's youngest populations, with almost half of its 1.3 billion population having a median age of 19.7 (Population of Africa, 2021). The continent is expected to balloon to a population of 2.5 billion by 2050, with half of that number being under 25 (One, 2017). As internet access improves across the continent, the opportunity to grow over several sectors, including agro-business and fintech, is undoubtedly appealing. The 'Africa Rising' narrative of the early 2000s buoys much of this investment, with similar interest from scholars, non-governmental organisations (NGOs) and international institutions (Beresford, 2016; Frankema & Van Waijenburg, 2018). Yet academic and contemporary discourse on the incursion of information technology behemoths has focused mainly on the potential effects of sub-activism or the apparent descent towards authoritarianism across the continent.

The term 'Big Tech' refers to the biggest five information technology companies – Amazon, Apple, Google (Alphabet), Facebook and Microsoft. These five US-based companies are significant because of their outsized market capitalisation, which is reported to being almost US$8,4 trillion (Wilhelm, 2021), and the ability of their products to influence political and social life across the globe (Galloway, 2017).

In this article, I do not engage in discussions on the effect of Big Tech on authoritarianism or as a tool of sub-activism. Instead, I explore the global connectivity politics of Big Tech in Africa, which, as I posit, is a continuation of the politics inherent in communications technology investment that is marked by power imbalances between powerful companies and under-resourced African governments.

Emerging technologies have long been part of the political landscape of African countries. Historically, they were a placeholder for development, power and dispossession. For numerous reasons, including a lack of financial capacity, the expected agency of states is mainly deficient. Moreover, across the continent, regulatory frameworks, and the ability to engage with powerful

companies, are not adequate. The problem with the frameworks in place is twofold: first, the inherent power asymmetry between Big Tech and African governments; second, the historically slow pace at which ICT policies and regulations are formulated on the continent. Wangwe (2007:14) warns that Africa regulators were "not equipped to deal with emerging policy and regulatory issues such as spam and consumer concerns regarding privacy". The Digital Trends Report of the International Telecommunications Union ([ITU] 2021) draws attention to the regulatory inefficiencies still present in a number of African countries. They point out that: and as the COVID-19 crisis has laid bare, inequalities are increasing within and between countries, not least because current governance and regulatory frameworks and their implementing mechanisms are failing to deliver more equitable outcomes (ITU, 2021:36).

In this article, I go beyond concerns about an extraction-based approach by technology companies to look at how these investments do not follow traditional investment patterns, and then suggest that African governments need to be more proactive in their relationships with powerful technology companies.

Debates

Africa has become a site of interest for big technology firms that have traditionally looked elsewhere for investments outside of Silicon Valley (Quartz, 2020). When referring to Big Tech, the companies discussed are US-based Apple, Facebook, Microsoft, Amazon and Google. The involvement of Big Tech on the African continent is controversial. At the root of the controversy are apprehensions around Africa's tapering digital sovereignty, which in itself is further complicated because there is no universal understanding of the digital sovereignty concept. Much of the accepted interpretations are embedded in concepts from the global North. However, there are emerging interpretations of digital sovereignty from North American and Australian First Nations and China (Floridi, 2020; Kukutai & Taylor, 2016; Ortega, 2018). All of these various interpretations are potentially instructive for African countries as they begin to grapple with the concept of digital sovereignty within continental and national structures. Notable common interests are digital autonomy, the protection of grassroots innovation, and data protection and privacy. The questions related to this are who owns the data? how will the data be used? are sunset clauses available? The data protection regimes that also cover these questions originate from the European Union, the United States and China. Where Global South countries, particularly those in Africa, fit into these regimes is still unclear. African governments are on the back foot with regard to deciding which regime suits their purposes. There are numerous reasons, including the extant need for access to technology transfers, the dearth of necessary digital skills (International Finance Corporation [IFC], 2019), and the need to improve infrastructure to facilitate the digital economy (Global Business Outlook, 2020).

Much of the critique around Big Tech in Africa centres predominantly on three key concerns:

- Data colonialism
- Stagnation of local innovation systems
- The inability to regulate the tech companies within the state

A thread running through all three concerns relates to the lack of data autonomy. Data colonialism is a significant concern for scholars and policy practitioners alike (Elmi, 2020; Pilling, 2019). Information technology companies have the financial capacity that significantly overshadows the GDP of many African states; for instance, the 2020 combined revenue of Apple, Microsoft, Amazon and Google sat at US$1,2 trillion (Ovide, 2021; Wallach, 2021). The level of financial capacity has meant that non-state actors are now participants in multilateral negotiations, such as at the International Telecommunications Union and the World Trade Organization. The deeper involvement of non-state actors also means that the nature of international politics has shifted. Also, for African countries still trying to assert their agency in these institutions, more powerful actors make the playing field more complex.

As US and Chinese tech companies flood the market, there is understandably discontent from some quarters about potential data colonisation (Benyera, 2021; Couldry & Mejias, 2020) or supplanting the local tech ecosystem (Diphoko,2020; Frost et al., 2019) around the nature of the investment. Although Big Tech invests in local start-ups, much of the investment, arguably, focuses on what they see as priorities.

In 2021, South Africa's competition commission finalised its paper on Competition in the Digital Economy, which is one of the ways it intends to regulate Big Tech operations in the country (Competition Commission, 2021). One of the major points is the requirement, as a means to counter anti-competitive behaviour, that technology companies inform the commission of acquisitions of smaller companies. South Africa's move is reflective of the current wave of policies and regulations to counter the dominance of Big Tech around the world (Dans, 2021; Hiebert, 2021; McNamee, 2020; Wheeler, Verveer & Kimmelman, 2020). For instance, most technology companies are platform based and their operations are transnational, which makes it difficult to develop appropriate regulations. For African countries, the debates around developing a regulatory framework are further complicated by the disparate approaches to regulations – often shaped by geopolitical alignments to stronger powers – and the fact that there is no overarching continental approach to the regulation of big technology firms. Moreover, ICT access across the continent is unequal, and moves towards digitalisation further exacerbate inequality, as only a few benefit from the digital economy (Krönke, 2020; Mlaba, 2021; UNCTAD, 2019).

Perspectives

As Manning (2019) points out, the growth of Global South countries is dependent on technology transfers. Ahere (2021) reminds us that technology transfers have always been a site of contention between the global North and Africa in particular. The former is being accused of restraining Africa's development capacity by focusing on the 'transfer of product rather than the skills and capacity to manage the technology throughout its life cycle'. Although Ahere was not specifically referring to digital technology transfers, the argument still is valid. As the big technology firms deepen their footprint on the African continent, there are valid questions about whether their investment is superficial. In other words, how much human resource and material capacity is being built in the region or makes their investment relate to the use of products and extraction of local data.

Moreover, the requirements of the digital economy interface directly with the conditions of the non-digital, physical trade-based economy. For instance, both digital and non-digital economies need basic infrastructure, such as electricity, to function. They also require the population to have a certain degree of basic literacy. Ultimately, this means that engagements are necessary, but need to be guided to help bridge infrastructure and literacy gaps – not only for the benefit of the technology companies, but also for the benefit of host nations. Tech companies such as Google and Facebook have invested heavily in new infrastructure, such as undersea cable networks. Google is hiring many base-level coders as contractors (Forrest, 2017). However, there is little space for these workers to move beyond this stage. The question that still needs to be answered is whether this level of investment is mutually beneficial. If infrastructure is designed for ease of use for the private sector, and human capital is developed so that there is little room for growth, is this then not colonialism in a different form? On the other hand, big tech companies, Google included, are responsible for billions of dollars in tech start-up ventures on the continent (Graham, 2013; Perkins, 2021; Pimenta & Gajria, 2020).If an appropriate supra-national framework were already in place, for instance the African Union framework for the digital economy, it would be easier to ascertain if these investments match up to the vision the continent has for itself and what it needs.

Digitisation efforts on the continent have been driven by external actors – both the private sector and the global North. Consequently, African countries are always a step behind in developing an appropriate regulatory system to support digitisation in a way that makes sense for its specific context. South Africa, for instance, has seen a level of policy uncertainty in the ICT sector, and this has had negative implications for investments (Brown & Brown, 2008; Corrigan, 2020). Kenya, on

the other hand, has had a greater level of policy and regulatory stability, despite some implementation and cybersecurity challenges, which has paid positive dividends with regard to their preparedness to harness the benefits of the digital economy (Nyambura Ndung'u, Lewis & Mothobi, 2019). Stuart (2021) argues that a coherent ICT infrastructure policy and regulations – on both a regional and continental level – are an important driver for Africa's participation in the digital economy. The African Union ([AU] 2020b) Digital Transformation Strategy (2020 to 2030) is meant to help African countries tap into the digital economy. It is supposed to act as a blueprint for a harmonised approach to digitalisation on the continent and serve as impetus for the pooling of infrastructure (an important feature needed for the continental trade agreement and future e-commerce protocol). It builds on previous instruments, such as the Policy and Regulatory Initiative for Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), the African Continental Free Trade Area (AfCFTA), the Single Air Transport Market (SAATM), and the Free Movement of Persons (FMP), with the intention of building a single digital market (SDM).

Nevertheless, it runs the risk of suffering the same fate as the AU's (2014) Malabo Convention, which was the most wide-ranging cybersecurity framework in existence at the time of development. At the time of writing this article, most AU member states had still not adopted or ratified the convention, only 14 states out of 55 had signed the document, whilst only eight states had ratified the document (African Union, 2020a). A solid cybersecurity framework is an important pillar for the digital economy and a motivator for further investment. The reason for the Malabo Convention not taking off was a misunderstanding about the value of having such a framework and political contestations between AU member states. As a result, African countries are in holding patterns that are essentially set by companies originating from China, the US and the EU. From this it can be concluded that receptiveness to companies from specific geographic origins may be related to existing trade patterns and development partnerships.

Implications

In 2021, the African Continental Free Trade Agreement (AfCFTA) became active – a significant milestone towards Africa's economic integration. Although an e-commerce protocol was not released immediately, it will come into force after the competition policy, intellectual property rights and investment protocol have been negotiated (Ogo, 2020), and it is clear that digital technologies have been underscored as a critical component of Africa's growth and integration agenda. What does this mean for Big Tech companies? Suppose we answer this optimistically, and AU member states take digitisation efforts seriously in the first five years of the AfCFTA. In that case, tech companies would have to look towards entering robust private-public partnerships (PPP). The main vehicle to facilitate this would be under instruments such as PRIDA, PIDA, etc. PPPs should be cognisant of African digital sovereignty in the formulation of their agreements. A

critical warning by Kilic (2021) relates to lobbying power, which could give Big Tech the ability to take advantage of trade agreements. This arguably would be an essential consideration for the framers of future agreements, as well as for scholars. In the case of the emerging African agenda around the digital economy, who are the key lobbyers? What voices are dictating the discussions going forward?

The last consequence relates to the failure of implementation. The vision for Africa's digital economy is ensconced in Agenda 2063 – Africa's continent-wide development plan. Failure to ensure that big tech, and smaller players, work in line with this vision would guarantee that Africa's renewal plans would never come to fruition.

References

African Union. 2014. *Convention on Cyber Security and Personal Data Protection*. Available from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

African Union (AU). 2020b. *The Digital Transformation Strategy for Africa (2020-2030)*. Available from: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

African Union (AU). 2020a. *List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection*. Available from: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

Ahere, J. (2021). New actors and democratic governance in a rising Africa. *Frontiers in Political Science*, 2. https://doi.org/10.3389/fpos.2020.630684.

Benyera, E. (2021). *The Fourth Industrial Revolution and the recolonisation of Africa: The coloniality of data*. Milton Park: Taylor & Francis.

Beresford, A. (2016). Africa rising? *Review of African Political Economy*, 43(147):1-7.

Brown, W. & Brown, I. (2008). Next generation ICT policy n South Africa: Towards a human development-based ICT policy. In *Social dimensions of information and communication technology policy* (pp. 109-123). Edited by Avgerou, C., Smith, M.L. & Van den Besselaar, P. Boston: Springer.

Competition Commission. (2021). *Competition in the digital economy v. 2*. Available from: http://www.compcom.co.za/wp-content/uploads/2021/03/Digital-Markets-Paper-2021-002-1.pdf.

Corrigan, T. (2020). *Africa's ICT infrastructure: Its present and prospects*. SAIIA Policy Briefing no. 197, June. Available from: https://saiia.org.za/research/africas-ict-infrastructure-its-present-and-prospects/.

Couldry, N. & Mejias, U.A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4):336-349.

Dans, E. (2021, May 2). Around the world, governments are readying to regulate Big Tech. *Forbes*. Available from: https://www.forbes.com/sites/enriquedans/2021/05/02/around-the-world-governments-are-readying-to-regulate-bigtech/?sh=68881a605935.

Diphoko, W. (2020, July 31). The rise of big tech and how it will impact startups. *IOL*. Available from: https://www.iol.co.za/technology/software-and-internet/the-rise-of-big-tech-and-how-it-will-impact-startups-b158930e-674f-4885-8131-782da1b30c63.

Elmi, N. (2020, November 11). Is big tech setting Africa back? Available from: https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3):369-378.

Forrest, C. (2017, July 28). Google to train 10M Africans in online tech skills, 100K as software developers. *Tech Republic*. Available from: https://www.techrepublic.com/article/google-to-train-10m-africans-in-online-tech-skills-100k-as-software-developers/.

Frankema, E. & Van Waijenburg, M. (2018). Africa rising? A historical perspective. A*frican Affairs*, 117(469):543-568.

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

Galloway, S. (2017). *The four: The hidden DNA of Amazon, Apple, Facebook and Google*. New York: Random House.

Global Business Outlook. (2020). *Africa's efforts in digital transformation is vast*. Available from: https://www.globalbusinessoutlook.com/africas-efforts-in-digital-transformation-is-vast/.

Graham, F. (2013, October 15). Why the world's technology giants are investing in Africa. *BBC News*. Available from: https://www.bbc.com/news/business-24524260.

Hiebert, K. (2021, July 4). Efforts to regulate Big Tech risk becoming too fragmented. *Business Day*. Available from: https://www.businesslive.co.za/bd/opinion/2021-07-04-efforts-to-regulate-big-tech-risk-becoming-too-fragmented/.

International Finance Corporation (IFC). (2019). *Digital skills in Sub-Saharan-Africa: Spotlight on Ghana*. Available from: https://www.ifc.org/wps/wcm/connect/ed6362b3-aa34-42ac-ae9f-c739904951b1/Digital+Skills_Final_WEB_5-7-19.pdf?MOD=AJPERES&CVID=mGkaj-s.

International Telecommunications Union (ITU). (2021). *Digital trends in Africa 2021: Information and communication technology trends and developments in the Africa region 2017-2021*D. Available from: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf.

Kilic, B. (2021). *Digital trade rules: Big Tech's end run around domestic regulations*. , Brussels: Heinrich Böll Stiftung. Available from: https://eu.boell.org/en/2021/05/19/digital-trade-rules-big-techs-end-run-around-domestic-regulations.

Krönke, M. (2020). *Africa's digital divide and the promise of e-learning*. Afrobarometer Policy Paper no. 66. Available from: https://media.africaportal.org/documents/pp66-africas_digital_divide_and_the_promise_of_e-learning-afrobarometer_policy_s1oxzDa.pdf.

Kukutai, T. & Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda*. Canberra: ANU Press.

Manning, R.A. (2019). Techno-nationalism vs. the Fourth Industrial Revolution. *Global Asia*, 14(1): 14-21. Available from: https://www.globalasia.org/data/file/articles/1df3d336677b2c19afd2f11fe6eb5b05.pdf.

McNamee, R. (2020, July 29). Big Tech needs to be regulated. Here are 4 ways to curb disinformation and protect our privacy. *Time*. Available from: https://time.com/5872868/big-tech-regulated-here-is-4-ways/.

Mlaba, K. (2021, August 3). *How is South Africa's digital divide making inequality worse in the country?* [*Global Citizen Blog*]. Available from: https://www.globalcitizen.org/en/content/south-africa-digital-divide-makes-inequality-worse/.

Nyambura Ndung'u, M., Lewis, C. & Mothobi, O. (2019). After access: The state of ICT in Kenya. Policy paper series 5: After access: Assessing digital inequality in Africa, Policy Paper No. 9. *Research ICT Africa*. Available from: https://researchictafrica.net/publication/after-access-the-state-of-ict-in-kenya/.

Ogo, I. (2020, June 25). *An agenda for the AfCFTA protocol on E-commerce* [Tralac Trade Law Centre Blog]. Available from: https://www.tralac.org/blog/article/14692-an-agenda-for-the-afcfta-protocol-on-e-commerce.html.

One. 2017. *The African century*. Available from: https://s3.amazonaws.com/one.org/pdfs/ENG-Brief-TheAfricanCentury.pdf.

Ortega, A. (2018, May 29). *Digital sovereignty*. [Elcano Blog. Available from: https://blog.realinstitutoelcano.org/en/digital-sovereignty/.
Ovide, S. (2021, April 29). 'A perfect positive storm': Bonkers dollars for big tech. *New York Times*. Available from: https://www.nytimes.com/2021/04/29/technology/big-tech-pandemic-economy.html.

Perkins, N. (2021, April 30). Google to continue accelerator program, launches 40,000 developer scholarships. *AfroTech*. Available from: https://afrotech.com/google-developer-scholarships.

Pilling, D. (2019, July 5). Are tech companies Africa's new colonialists? *Financial Times*. Available from: https://www.ft.com/content/4625d9b8-9c16-11e9-b8ce-8b459ed04726.

Pimenta, S. & Gajria, N. (2020, November 11). *Understanding Africa's $180 billion internet economy future* [Google Blog]. Available from: https://blog.google/around-the-globe/google-africa/understanding-africas-180b-internet-economy-future/.

Population of Africa. (2021). *Worldometer*. Available from: https://www.worldometers.info/world-population/africa-population/.

Quartz. 2021. *Beyond Silicon Valley*. Available from: https://qz.com/on/beyond-silicon-valley/
Stuart, J. (2021, March 17). *How should the AfCFTA approach ICT infrastructure regulation?* [Tralac Trade Law Centre Blog]. Available from: https://www.tralac.org/blog/article/15142-how-should-the-afcfta-approach-ict-infrastructure-regulation.html.

UNCTAD. (2019). *Digital Economy Report: Value creation and capture: Implications for developing countries*. Available from: https://unctad.org/system/files/official-document/der2019_en.pdf.

Wallach, O., 2021. 'The World's Tech Giants, Compared to the Size of Economies', *Visual Capitalist*, 7 July. Available from: https://www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/. [22 July 2021].

Wangwe, S. (2007). *Evolution, status, and impact of ICT on economic development and transformation: An overview*. Available from: https://media.africaportal.org/documents/WangweS_AnOverviewpaperonICT.pdf.

Wheeler, T., Verveer, P. & Kimmelman, G. (2020, September 23). *The need for regulation of big tech beyond antitrust* [Brookings Blog]. Available from: https://www.brookings.edu/blog/techtank/2020/09/23/the-need-for-regulation-of-big-tech-beyond-antitrust/.

Wilhelm, A. (2021, May 1). Big Tech is now worth so much we've forgotten to be shocked by the numbers. *TechCrunch*. Available from: https://techcrunch.com/2021/05/01/big-tech-is-now-worth-so-much-weve-forgotten-to-be-shocked-by-the-numbers/.

Chapter 13

Artificial Intelligence (AI) and Content Governance in Sub-Saharan Africa

Sylvia Ndanu Mutua

Introduction

Most countries across the world have been facing online content challenges, which have at times resulted in the manipulation of public opinion formation, a reduction in public trust in government institutions and the media, dishonouring of political leadership, influencing voter decisions, as well as deepening societal divides (Ndlela, 2020). All these challenges are emerging in the context of an accelerating digital economy characterised by the development of innovative technologies, such as augmented and virtual reality (AR/VR), artificial intelligence (AI), robotics and the Internet of Things (IoT), among others. Moreover, the growing adoption and utilisation of these new technologies have altered not only how we communicate and interact with each other, but also how illegal and harmful online content is produced and distributed in cyberspace (Brkan, 2019). The rapid proliferation of this illegal and harmful online content has consequently raised concerns about the regulation of online content and irresponsible internet user behaviour in the cyberspace. It is unclear how this relates to content governance.

AI Technology Concerns (User Perspectives)

Although AI[12] systems and technologies have plenty of benefits, scholars such as Brkan (2019) and Marsden, Meyer and Brown (2020) have raised ethical concerns, exposing human rights challenges as well as the subversion of democratic principles in political processes, especially in young and emerging democracies. According to Bradshaw and Howard (2018) and Ndlela (2020), these concerns include: the infringement of user privacy; the personalisation of online content, resulting in partial information blindness (filter bubble); algorithmic unfairness, which may lead to discriminatory practices such as gender and racial biases; audio/audio-visual manipulation without internet user consent; and also potential user manipulation. Scholars further note that AI communication technologies have also been employed to carry out nefarious activities such as the creation and distribution of fake news using deep fakes, micro-profiling, illegal data harvesting, hate speech amplification using bots and fake accounts, pushing clickbait content to optimise social media consumption, and the misuse of online platforms for foreign influence operations (Bradshaw & Howard, 2018; Howard, Woolley & Calo, 2018).

[12] A note on terminology: The phrase artificial intelligence (AI) as used in this article broadly refers to computer systems that can perform tasks associated with intelligent beings, implying the ability of a system to perform tasks characteristic of human intelligence, such as learning and decision-making.

Effect of AI Technology Concerns

The effect of these ethical concerns, especially on politics and democracy, has been evident during general elections cycles in Western countries, as well as in sub-Saharan Africa. In their 2018 global inventory of organised social media manipulation, Bradshaw and Howard (2018) noted that in most of the 48 countries surveyed (which included African states such as Egypt, Kenya, South Africa and Zimbabwe), the use of online platforms to sabotage elections and weaken the public trust in democratic institutions was a widespread phenomenon. In 30 out of the 48 countries examined, they established evidence of political bots, data analytics and AI being employed to poison the information ecosystem, polarise the voting areas and advance scepticism and distrust of the electoral institutions, consequently undermining the integrity of these democratic processes (Bradshaw & Howard, 2018). These findings were similar to those of Milan and Treré (2019) and Ndlela (2020), who noted that, in some of the emerging African democracies, the state actors employed the power of algorithms and bots in communicating their campaign messages, with some of these messages bordering on hate speech and incivility. In so doing, they altered public perceptions of the political reality at the time and consequently created a misguided and misinformed electorate (Mare, 2018).

Debates on the Janus face of AI in Content Governance

Several debates have emerged on the utilisation of AI technologies in content governance. This article adopts Vafopoulos's (2006) analysis of the Janus face of AI technologies to explore these debates. Vafopoulos's (2006) analysis acknowledges AI technological benefits as reflected in the knowledge-based development of the technology, while its negative effects are exposed by human rights and personal privacy violations. Knowledge is considered a valuable input and output of the processes of societal development.

In the context of AI systems, it is imperative to note that they provide a very stable, powerful and cost-beneficial solution to prevent illegal and harmful content in cyberspace. Llansó, Van Hoboken, Leerssen and Harambam (2020) observe that this is done through automated detection of the potentially illegal or harmful online content and subsequently the automated evaluation and enforcement of a decision to remove, label/tag, demote, demonetise or prioritise the content in question. In contrast, those arguing against AI technologies note that the utilisation of AI in content governance exposes the technical realities of content filtering, which at times infringes on the protection of the freedom of expression and privacy as espoused in the international human rights law framework and pronounced in the Universal Declaration of Human Rights (Llansó et al., 2020).

Gillespie (2020), in supporting the use of AI in content governance, notes that it serves as the perfect solution to the growing challenges associated with the large quantity, velocity and variety of user-generated data. This is in addition to the rise in incidents of online content violations, the consequences of the online harms extending beyond the platforms, and the increased criticisms of the platforms for failures to govern the content on their platforms. Moreover, the global impact of the COVID-19 pandemic further has compelled most of the online platforms to heavily utilise AI in content governance. This is after sending most of their content moderating staff to operate from home (Magalhães & Katzenbach, 2020).

In the recent past, governments and social media platforms have adopted and funded proactive detection and automated evaluation initiatives governing online content, especially on social media platforms. This has been done through AI-assisted fact-checking mechanisms to complement human fact-checking in the identification, verification and correction or deletion of online content, especially on social media platforms (Cartwright, Weir & Frank, 2019). In addition, AI content-moderation solutions have also been utilised for the effective removal of illegal and harmful online text, such as hate speech, sexual content, and child abuse, violent and terroristic content. They have also been successful in the identification and removal of fake bot accounts through bot-spotting and bot-labelling techniques (Cartwright et al., 2019; Graves, 2018).

Other than texts, AI technologies have also been employed in automated image detection and identification. These approaches have been used to detect the presence of certain features or elements in an image, such as logos, symbols, nudity or weapons (Afchar et al., 2018). Other advanced AI tools use skin tone detection together with image parsing processes to identify body parts distribution as well as faces, thus generating classifiers that detect and identify nudity and sexual activities (Bonomi, Pasquini & Boato, 2020). Technologies like hash matching, generative adversarial networks (GAN) and optical character identification tools have also been useful in the detection of manipulated images and videos (Yu, Davis & Fritz, 2019). These few but important instances illustrate the potential of AI to be fully leveraged with a high accuracy rate in governing online content.

On the flip side, given that the AI models are still under development and refinement, there have been some unintended repercussions, such as instances of false positives (flagging content as objectionable when it is not) as well as false negatives (missing content that should have been classified as objectionable). The upshot of the false positives is that it ends up causing a chilling effect, infringing on the freedom of expression and censorship of legitimate online content. On the other hand, the false negatives fail to address illegal and harmful online content and may also

cause a chilling effect on some people or groups' inclination towards online participation, therefore limiting digital inclusivity (Marsden & Meyer, 2019).

Graves (2018) notes that some of the mislabelled online content could be caused by concepts not yet mastered by the AI content moderation systems, such as linguistic barriers, human conceptualisations of sarcasm or irony, as well as country-specific cultural and political contexts. Lee, Resnick and Barton (2019), in addressing the human conceptualisation of AI systems, further note that system biases can emanate from the programmers who design and train the algorithms, or from incomplete, flawed or unrepresentative data. Llansó et al. (2020) caution that, if left unchecked, data that has been influenced by real-world inequalities and biases can have very dire consequences, such as reflecting or amplifying existing inequalities, failing to address harm, or causing illegitimate silencing of some people or groups. This leads us to the question of whether AI indeed is truly free from human error and bias.

Content Governance Implications for African Digital Sovereignty

It is indisputable that AI systems have become important to human communication. This is because the use of algorithms has revolutionised the way we access information, communicate, and interact with each other across time and space (Hancock, Naaman & Levy, 2020). That being said, however, it is unfortunate that in most sub-Saharan countries, the deployment of AI is still in its infancy. The majority of people are not even aware of the privacy concerns and/or the need to guard their information online. In addition, there is a dearth of comprehensive AI content governance frameworks to govern illegal and harmful online content in sub-Saharan Africa (Besaw & Filitz, 2019). The need for transparency and accountability, especially by social media platforms, has also been noted by several scholars (Common, 2020; Nahmias & Perel, 2021; Udupa et al., 2021). However, we must be cognisant that most of the cyber laws and data protection acts in some African states exempt the platforms from liabilities for illegal and harmful content on their platforms, and conveniently shift the consequences to the users. The above issues point to the few challenges that hinder sub-Saharan Africa from claiming sovereignty in the online content governance game.

As we advance an African narrative on digital sovereignty, we must shift our attention and focus from being mere consumers of these innovative communication technologies and actively participate in the design and creation of AI content-governance tools. Doing so will give African states more leverage to demand sovereignty for the governance of online content from their countries. Tworek's (2019) proposal for the formation of social media councils calls for an inclusive, multistakeholder solution to address the challenges of content governance in cyberspace. From an African perspective, this would entail all the players, be it private individuals, content creators,

investors – everyone who can participate in AI – focusing on being a part of the game and then demanding sovereignty.

African governments can play an active role by supporting these multistakeholder initiatives through their participation and also in giving policy direction that protects the local needs and interests of the African people. Also, in allowing the social media platform corporations to operate in their jurisdictions, African governments should insist on further collaborations between the social media platform corporations and African communities in defining the policies that will guide the AI in online content moderation. This implies advocating for people-centric efforts from the social media platform corporations to include ways to involve communities in the process of training AI systems and defining and designing the platform content regulations. Consequently, these regulations that the AI systems must enforce should reflect local and cultural realities in the African context.

Conclusions

This article recognises the central role of AI as a pivotal tool in defending the right to access information, as well as freedom of expression and its underlying values. AI is crucial in creating conditions for vibrant and robust democratic interactions and exchanges on online platforms. However, it also has the potential to infringe on fundamental human rights. Consequently, our quest to advance African digital sovereignty in online content governance demands that African governments play a proactive role and work together with the relevant AI stakeholders in harnessing AI technology for content governance. There is a dire need for collaborations and multi-stakeholder initiatives in developing rigorous and transparent processes to streamline and consistently incorporate diverse and potentially conflicting human feedback into the development of AI for content moderation.

The creation of an active and powerful African-centred multi-stakeholder initiative is therefore important to disrupt the existing inequalities and also to guarantee the required accountability and transparency in African content governance. In a cyberspace dominated by Western-based platforms and organisations, it becomes very important to represent and protect the interests and needs of African people. This is necessary because online content from the African continent ought to be governed according to African values, uniqueness, culture and philosophies.

References

Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I. (2018, December). Mesonet: a compact facial video forgery detection network. In 2018 *IEEE International Workshop on Information Forensics and Security (WIFS)* (pp. 1-7). IEEE.

Besaw, C. & Filitz, J. (2019). *AI & global governance: AI in Africa is a double-edged sword*. United Nations University Centre for Policy Research. Available from: https://cpr.unu.edu/publications/articles/ai-in-africa-is-a-double-edged-sword.html.

Bonomi, M., Pasquini, C. & Boato, G. (2020). Dynamic texture analysis for detecting fake faces in video sequences. *Journal of Visual Communication and Image Representation*, 79:103-239.

Bradshaw, S. & Howard, P.N. (2018). Online Supplement to Working Paper 2018.1: Challenging truth and trust: A global inventory of organized social media manipulation. *The Computational Propaganda Research Project*. Available from: https://blogs.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct_appendix.pdf.

Brkan, M. (2019). Artificial intelligence and democracy: The impact of disinformation, social bots, and political targeting. *Delphi - Interdisciplinary Review of Emerging Technologies*, 2(2):66-71.

Cartwright, B., Weir, G. R. & Frank, R. (2019). Fighting disinformation warfare with artificial intelligence. In *Cloud Computing 2019: Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 73-81). Edited by Duncan, B., Lee, Y. W., Westerlund, M. & Aßmuth, A. Available from: https://www.researchgate.net/profile/Bob-Duncan/publication/333024381_CLOUD_COMPUTING_2019_Proceedings_of_the_Tenth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization/links/5cd74276a6fdccc9dda36ae0/CLOUD-COMPUTING-2019-Proceedings-of-the-Tenth-International-Conference-on-Cloud-Computing-GRIDs-and-Virtualization.pdf#page=84

Common, M.F. (2020). Fear the reaper: How content moderation rules are enforced on social media. *International Review of Law, Computers & Technology*, 34(2):126-152.

Gillespie, T. (2020). Content moderation, AI, and the question of scale. *Big Data & Society*, 7(2):1-5. doi:10.1177/2053951720943234.

Graves, D. (2018). Understanding the promise and limits of automated fact-checking. *Reuters Institute for the Study of Journalism*. Available from: https://www.reutersagency.com/wp-content/uploads/2019/03/reuters-institute-graves-factsheet-180228.pdf.

Hancock, J.T., Naaman, M. & Levy, K. (2020). AI-mediated communication: Definition, research agenda, and ethical considerations. *Journal of Computer-Mediated Communication*, 25(1):89-100.

Howard, P.N., Woolley, S. & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, 15(2):81-93.

Lee, N.T., Resnick, P. & Barton, G. (2019). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Washington, DC: Brookings Institute.

Llansó, E., Van Hoboken, J., Leerssen, P. & Harambam, J. (2020). *Artificial intelligence, content moderation, and freedom of expression*. Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression. Available from: https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Artificial_Intelligence_TWG_Llanso_Feb_2020.pdf.

Magalhães, J.C. & Katzenbach, C. (2020). Coronavirus and the frailness of platform governance. *Internet Policy Review*, 9. Available from: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-68143-2.

Mare, A. (2018, May 31). Social media, fake news, and echo chambers in Zimbabwe. *Newsday*. Available from: https://www.newsday.co.zw/2018/05/social-mediafake-news-and-echo-chambers-in-zimbabwe/.

Marsden, C. & Meyer, T. (2019). Regulating disinformation with artificial intelligence: Effects of disinformation initiatives on freedom of expression and media pluralism. *European Parliament*. Available from: https://op.europa.eu/en/publication-detail/-/publication/b8722bec-81be-11e9-9f05-01aa75ed71a1.

Marsden, C., Meyer, T. & Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation? *Computer Law & Security Review*, 36:105-373.

Milan, S. & Treré, E. (2019). Big data from the South(s): Beyond data universalism. *Television & New Media*, 20(4):319-335.

Nahmias, Y. & Perel, M. (2021). The oversight of content moderation by AI: Impact assessments and their limitations. *Harvard Journal on Legislation*, 58:145-152.

Ndlela, M.N. (2020). Social media algorithms, bots, and elections in Africa. In *Social media and elections in Africa, Volume 1: Theoretical Perspectives and Election Campaigns* (pp. 13-37). Edited by Ndlela, M.N. & Winston, M. Cham: Palgrave Macmillan.

Tworek, H. (2019). Social Media Councils. *Models for Platform Governance,* (pp. 97-99). Available from: https://www.cigionline.org/static/documents/documents/Platform-gov-WEB_VERSION.pdf#page=99.

Udupa, S., Hickok, E., Maronikolakis, A., Schuetze, H., Csuka, L., Wisiorek, A. & Nann, L. (2021). *Artificial intelligence, extreme speech and the challenges of online content moderation*. AI4Dignity Project, München Ludwig-Maximilians-Universität, Munich. https://doi.org/10.5282/ubm/epub.76087.

Vafopoulos, M. (2006). Information society: The two faces of Janus. In *Artificial intelligence applications and innovations.* AIAI 2006. IFIP International Federation for Information Processing, vol. 204. Edited by Maglogiannis I., Karpouzis K. & Bramer M. Boston, MA: Springer. https://doi.org/10.1007/0-387-34224-9_75.

Yu, N., Davis, L.S. & Fritz, M. (2019). Attributing fake images to GANs: Learning and analyzing GAN fingerprints. *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 7556-7566). Available from: https://openaccess.thecvf.com/content_ICCV_2019/html/Yu_Attributing_Fake_Images_to_GANs_Learning_and_Analyzing_GAN_Fingerprints_ICCV_2019_paper.html.

Padmashree Gehl Sampath and Fiona Tregenna
Editors