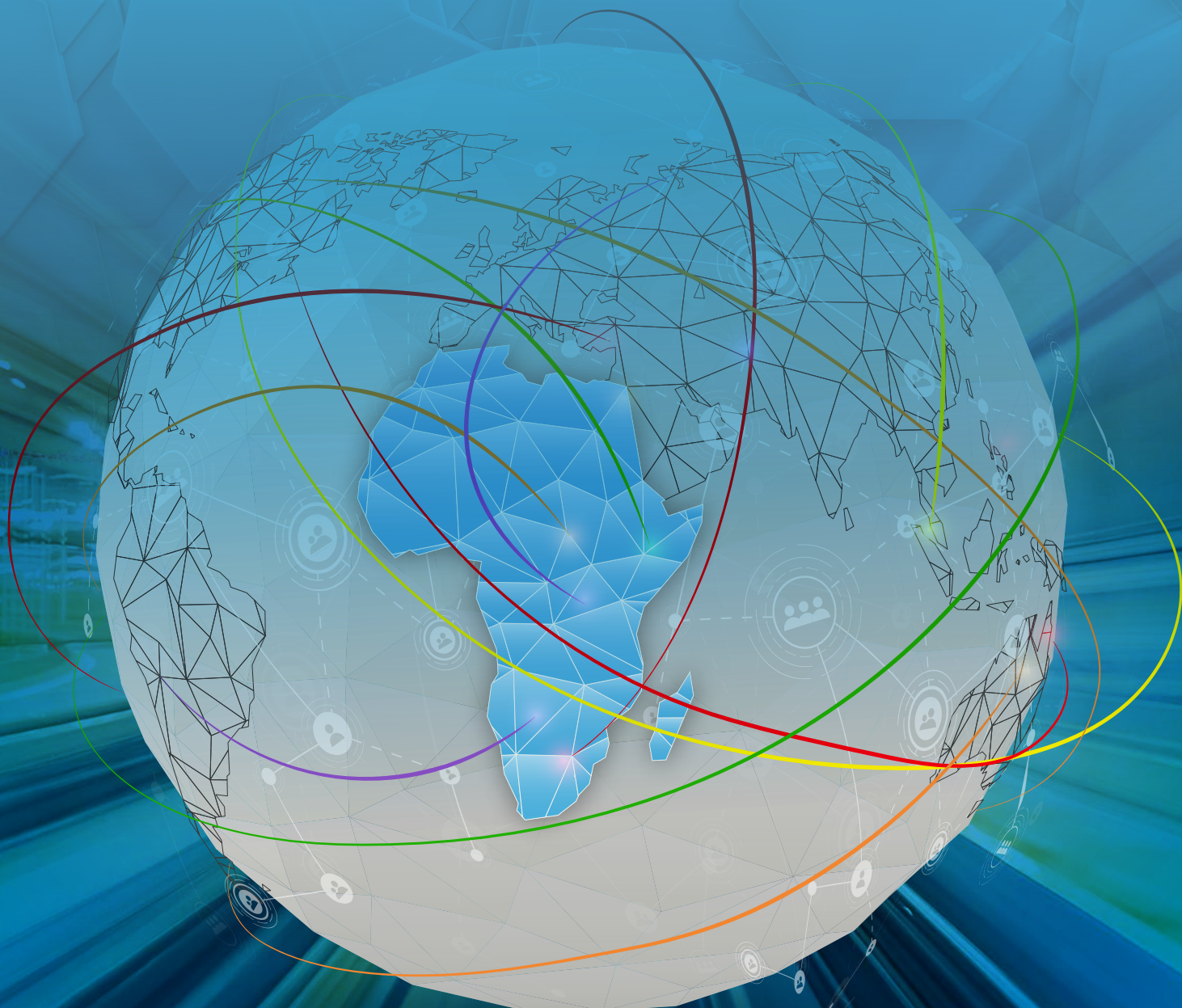
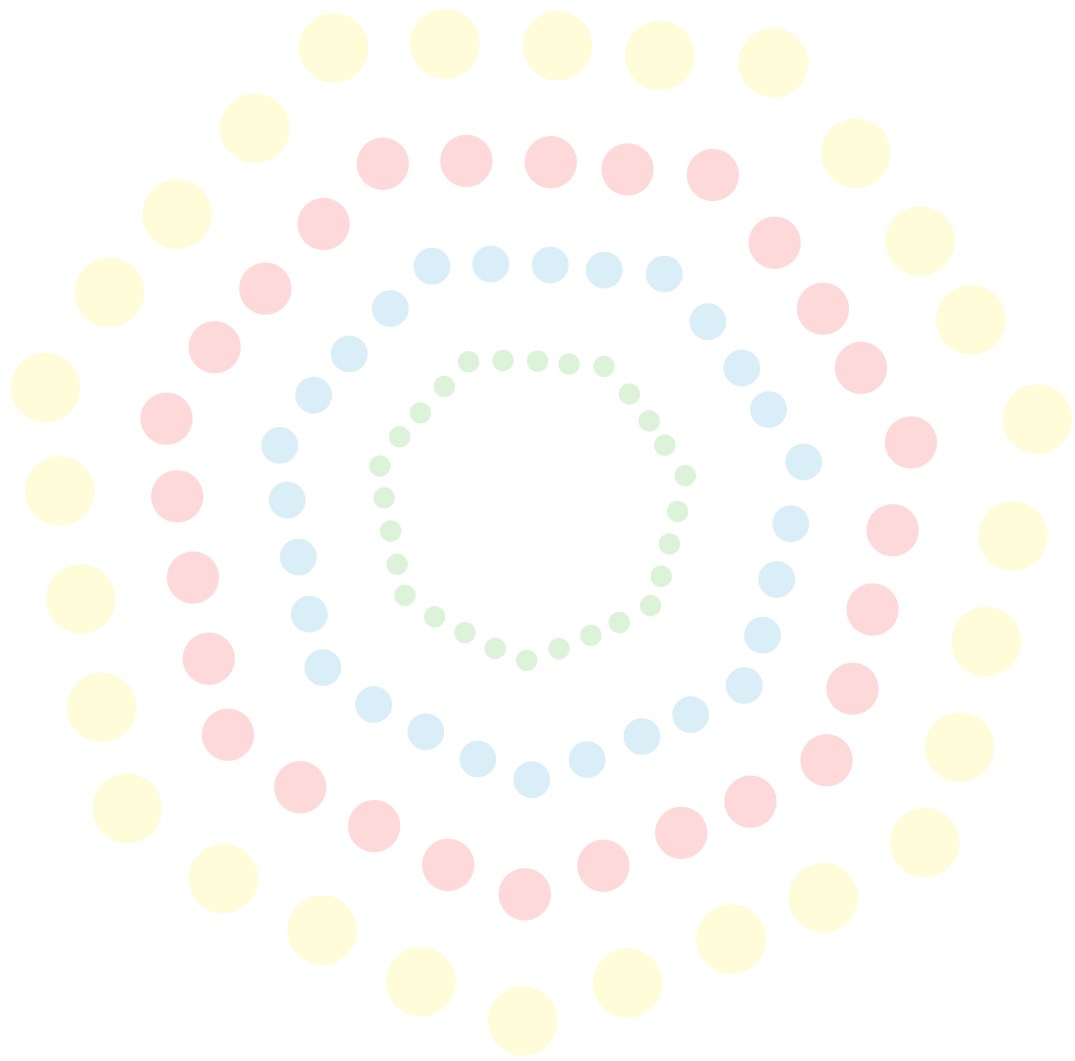


FRAMING, MAPPING & ADDRESSING CROSS-BORDER DIGITAL POLICIES IN AFRICA

AN INTERNET & JURISDICTION POLICY NETWORK
REGIONAL STATUS REPORT





The Report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) and authored by a research team at [Research ICT Africa](#) (RIA) under the supervision of Dr. Alison Gillwald and researchers Dr. Andrew Rens, Dr. Dunia Prince Zongwe, Hanani Hlomani and with project management by Naila Govan-Vassen.

The Report represents the author's best endeavor to map the current ecosystem and trends in Africa on the basis of desk research and stakeholder surveys and interviews. The completeness of the information cannot be guaranteed, however, as this Report constitutes a first regional baseline with regard to the state of cross-border digital (and data) policies in Africa.

I&JPN is grateful for the financial and institutional support of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ) which enabled the production of this Report.

The views expressed in this document, which has been reproduced without formal editing, are those of the authors and do not necessarily reflect the views of the Secretariat of the Internet & Jurisdiction Policy Network, stakeholders engaged in the Internet & Jurisdiction Policy Network, or the financial supporters of the Report.

The report has been designed by Hubble Studios, South Africa.

REPORT CITATION AND COPYRIGHT

Internet & Jurisdiction Policy Network (2022). "Framing, Mapping and Addressing Cross-Border Digital Policies in Africa: An Internet & Jurisdiction Policy Network Regional Status Report".

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



FOREWORD

Developing interoperable cross-border digital policies is an increasingly complex policy challenge, yet it lies at the forefront of leveraging digital technologies and the data economy to improve societies and reach the Sustainable Development Goals (SDGs).

For the past ten years, the Internet & Jurisdiction Policy Network has been working to support multistakeholder cooperation across sectors and regions. It has become increasingly clear that scalable and coherent policy solutions cannot be developed without a comprehensive understanding of the highly complex and dynamic digital ecosystem of multiple actors, initiatives, and trends across many cross-cutting and often competing policy objectives and silos.

New and innovative policy approaches are needed now more than ever to facilitate data sharing and leverage digital technologies to reach the SDGs. This is nowhere more evident than in Africa, where, as in other regions of the world, following the COVID-19 pandemic, the digital transformation of economies, governments, and societies is sharply accelerating.

Against the backdrop of the ambitious strategic frameworks of the Agenda 2063, the African Continental Free Trade Area (AfCFTA) and the recently endorsed AU Data Policy Framework we have embarked to enable peer-to-peer knowledge exchange of stakeholders in the region as they frame, map, and address cross-border digital policy challenges, through the collaborative methodology of the Internet & Jurisdiction Policy Network Regional Status Report: Framing, Mapping and Addressing Cross-border Digital Policies in Africa.

Authored by Research ICT Africa, the Report builds on the unique methodology of the Internet & Jurisdiction Policy Network to mutualize knowledge of key regional stakeholders from states, companies, technical operators,

international organizations, academia, and civil society through interviews, surveys, and workshops. It is a regional follow-up to both the Internet & Jurisdiction Global Status Report 2019, and the Internet & Jurisdiction and ECLAC Regional Status Report in 2020.

The Report explores why policy coordination is important to building an inclusive and vibrant digital economy in Africa. It identifies key trends taking shape across the region and presents opportunities and challenges for government, private sector, and civil society actors to consider.

The analysis showcases regional stakeholder perspectives and identifies ways to cooperatively govern cross-border digital issues. A key message of the Regional Status Report is that incremental implementation of cross-border digital policies should progress toward harmonization and consider development capacities and national contexts without requiring simultaneous conformity.

By laying out key trends concerning the handling of digital policy issues on the continent, the Report is intended to provide a baseline for policymakers within Africa and globally to enhance their understanding of the current opportunities and challenges as Africa seeks to design policy and technical innovations to leverage the digital economy for sustainable and inclusive development. We hope that the findings will contribute to the broader continental project of data policy harmonization envisioned in the [Digital Transformation Strategy](#) of the African Union Commission.

As Africa seeks to build its path and strengthen its regional voice in global policy debates, we hope that this report, and the community that helped to develop it, will support further dialogue and evidence-based research to foster coordination on cross-border digital policies across the region.



Martin Hullin
Deputy Executive Director
Internet & Jurisdiction Policy Network

TABLE OF CONTENTS

FOREWORD	4
EXECUTIVE SUMMARY	7
ACKNOWLEDGMENTS	13
INTRODUCTION	22
The challenge of Digitization and Datafication	23
Data value creation	24
Overview of African Policy	26
The Need for the Report	27
Methodology	27
Timeline	28
Engagement process and timeline	28
Early findings	28
1. POLICY CONTEXT	31
I. African policy response	33
II. The African Continental Free Trade Area (AfCFTA)	34
III. Data protection and privacy	35
a. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)	36
b. The 2010 Supplementary Act on Personal Data Protection of The Economic Community of West African States (ECOWAS)	36
c. Cyberlaw and cybercrime law	37
i. The 2008 East African Community Framework for Cyberlaw	38
ii. The 2013 Southern African Development Community Model Law Harmonizing Policies For The ICT Market In Sub-Saharan Africa	38
IV. Intellectual Property Law	39
a. Copyright law	39
b. Sui Generis database protection of non-original databases	40
c. Patent law	40
d. Trade Secret Protection	41
V. Competition law	41
2. TOPICAL TRENDS IN AFRICA	44
I. Trusted Environments	44
a. Internet shutdowns	44
b. Disinformation	46
c. Fake News	47
d. Cybercrime and Cybersecurity	48
e. Surveillance	50
f. Online Gender-Based Violence	51

	g.	Human Rights Online	51
II.		Inclusive Economy	52
	a.	Competition	52
	b.	Taxation	53
	c.	Financial Inclusion and Mobile Money	54
	d.	Digital trade	54
	e.	Infrastructure	55
	f.	Internet connectivity	56
	g.	Digital ID	58
	h.	Data Centers	59
	i.	E-governance	60
III.		The need for coordination and harmonization on digital policy	61
	a.	Reasons for Cooperation	63
	b.	External influence on African regulation and policy	64
	c.	Single narrative in global policy fora	66
	d.	The need for a meta-narrative	66
3. POSSIBLE SOLUTIONS IN AFRICA			69
I.		Developing shared infrastructure	69
II.		Harmonized legal standards	70
	a.	The opportunity for coordination offered by the African Continental Free Trade Area	71
	b.	Need for African countries to cooperate	71
	c.	Cross-border data flow	74
	d.	Mutual protection of personal data	76
	e.	Africa-wide standards for non-personal data	76
	f.	Open data	77
	g.	Communal Data Governance	77
	h.	Experimentation through cross-border sandboxes for data	79
MOVING FORWARD			83
REFERENCES			86
ANNEX A: THE RESEARCH PROCESS			87
I.		The knowledge dialogue workshops	87
II.		The launch of the data collection phase	90
	a.	The Menti online poll at the AfIGF in Malawi	90
III.		Data collection	91
	a.	Desk research	92
	b.	High-Level Interviews	92
ANNEX B: KEY ORGANIZATIONS WORKING ON GLOBAL DATA GOVERNANCE SOLUTIONS IN AFRICA			94

EXECUTIVE SUMMARY

AT A GLANCE

- African countries should increase their coordination on data policies.
- Data sovereignty can be realized without data localization through reciprocal protection of personal data and continental policies to share benefits.
- Data policies require human rights safeguards in order to create a trusted and functioning online environment.
- Incremental implementation of data policy should progress toward harmonization and take into account development capacities and national contexts without requiring simultaneous conformity.
- There is generally a data deficit in the continent, particularly of accurate data and data sharing structures that can foster the attainment of the Sustainable Development Goals.
- Shared data infrastructures, including a distributed network of data centers, needs to be progressively developed to enjoy the benefits of scale and scope.
- A common African voice in international fora should advocate for data policies that support inclusive development and uphold both individual and collective rights.

ABOUT THE REPORT

The *Internet & Jurisdiction Policy Network Regional Status Report: Framing, Mapping and Addressing Cross-border Digital Policies in Africa* is an exploration of how cross-border data flows can be unleashed to contribute to continental objectives of economic and social development while respecting national sovereignty imperatives, including the safeguarding of citizens from potential harm. Research began by identifying digital cross-border issues. Cross-border data flow rapidly emerged as the most crucial and immediate, albeit under-rated cross-border issue. As a result, the Report provides an overview of the current state of data policy with a mapping of laws and conventions in the context of the new [African Union Data Policy Framework](#) with a focus on cross-border digital issues. A central objective of that ground-breaking initiative is an interoperable and integrated data system for the single market and ultimately, the harmonization of policies to foster development across the continent. As stakeholders point out however, the test of the success of this Framework will be in its implementation at the continental level through its domestication by member states. Previous timely and necessary digital conventions have been adopted but not ratified by a sufficient number of states for them to become binding and are thus not implemented by most member states.

In acknowledgment of this challenge, the African Union has developed an implementation and action plan for member states and will facilitate a capacity-building program to respond to the identified needs of member states. By expanding the multifaceted research method first adopted for the production of the pioneering [Internet & Jurisdiction Global Status Report 2019](#), and later deployed by the [Internet & Jurisdiction and ECLAC Regional Status Report 2020](#), the findings in this Report are based on a large-scale collaborative contribution and review process, combining the expertise of the key stakeholders engaged in the Internet & Jurisdiction Policy Network and beyond.

The initiative is intended to complement existing continental mechanisms for stakeholder engagement across Africa to share knowledge, consult each other, interact with stakeholders around the world and develop a shared understanding of capacity around digital policy issues.

The Report explores why cross-border policy coordination is important to building an inclusive and vibrant digital economy in Africa. It identifies key trends taking shape across the region and presents opportunities and challenges for government, private sector, and civil society actors to consider. The Report showcases regional stakeholder perspectives and identifies ways to cooperatively govern cross-border digital issues. The findings will contribute to the broader continental project of data policy harmonization, market integration, and socio-economic development envisioned in the [Digital Transformation Strategy](#) (DTSA) of the African Union Commission. The Report's findings should resonate with policymakers in Africa and globally.

The Introduction sets out the challenges of digitization and datafication, the methodology used for the research, and briefly describes the research process and early findings. The policy context is detailed in Chapter 1, that discusses continental policy responses to digitization, datafication and the tectonic policy development that is the inception of the African Continental Free Trade Area (AfCFTA). Chapter 1 also sets out data protection and privacy, cybercrime laws, intellectual property, and competition law drive cross-border digital issues. In Chapter 2, the Report discusses topical trends of cross-border digital issues in Africa. A wide range of trends is reviewed under the descriptors of a trusted environment, inclusive economy, infrastructure, and the need for digital policy coordination. Possible solutions to some of the issues raised by the research are presented in Chapter 3, including developing shared infrastructure, harmonizing legal standards, agreeing on cross-border data flow, and developing a common African narrative. Chapter 4 contains conclusions framing the challenges.

OVERARCHING TRENDS

Desk research and the series of consultations in the preparation of this Report have surfaced high-level trends and messages from more than 100 consulted stakeholders.

AFRICA IS CONFRONTED WITH SIMILAR CHALLENGES AS OTHER REGIONS IN DEVELOPING ITS DIGITAL POLICIES

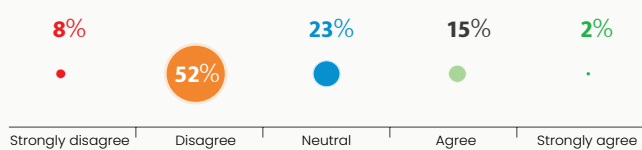
Desk research and the series of consultations in the preparation of this Report have surfaced high-level trends and messages from more than 100 consulted stakeholders.

The present Report is a follow-up to two previous initiatives by the Internet & Jurisdiction Policy Network: its 2019 Global Status Report and 2020 Regional Status Report regarding Latin America and the Caribbean. Several challenges around digital policies for Africa appear similar to the ones encountered in other regions, in particular:

- The difficult handling of interdependencies between policies conducted in **separate knowledge and policy silos** (e.g., trade, security, privacy protection, etc.);
- The risk of possible **incompatibilities between unilateral measures** adopted among a large number of countries, the cumulative effect of which can make some issues even harder to solve;
- The growing tension between aspirations to both **protect the free flow of data and ensure digital sovereignty** through measures such as data localization;
- The difficulty to fully participate in the global debate about data policies, which is largely driven by actors outside of the region and makes African countries “standard takers” rather than “standards makers”;
- The growing concern about the **extractive nature of the data economy** and the wealth inequalities it creates and amplifies.

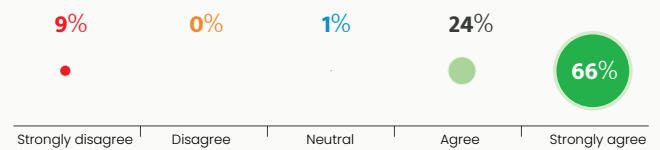
An overarching theme is the **need for stronger coordination** among countries in the continent and the recognition that it is currently not sufficient.

Figure 8



Answers to the statement:
There is strong coordination among African countries regarding digital policy issues.

Figure 9



Answers to the statement:
African countries need to work more together on digital issues

AFRICA ALSO FACES SPECIFIC CHALLENGES

Beyond the above problems, with which all countries are confronted, Africa has specific characteristics stemming from its general social and economic situation that must be taken into account when developing the ambitious set of digital policies that are needed. They include:

- The **sheer size of the continent**, in terms of the number of countries involved and the overall territorial footprint, with vastly diverse environmental and topographic situations;
- The **very disparate levels of overall development**, both among and within countries, with considerable issues regarding primary needs and potential climate change related risks;
- The **very uneven geographic distribution of populations**, with dense urban centers and very dispersed rural populations;
- The persistence of **societal and political tensions** and even violent conflicts in some parts of the continent, with too many correlated measures of internet shutdowns;
- The **coexistence of a continental integration effort with multiple sub-regional groupings** (with strong historic roots), which adds a layer of coordination challenges;
- The level of overall development and **uneven availability of reliable energy infrastructure**, which is critical for powering the digital economy.

A CLEAR AMBITION TOWARD DIGITAL INTEGRATION IS EMERGING

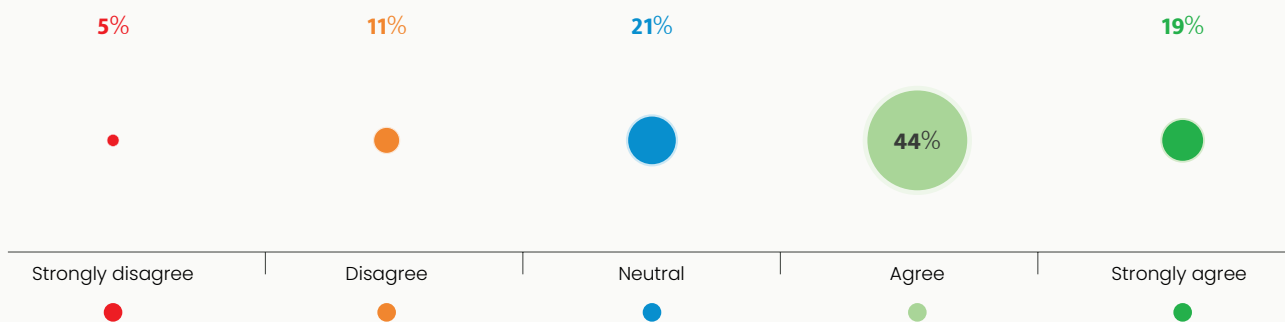
Several initiatives highlight the growing consciousness of the importance of digital and in particular data policies for the development of the continent. They manifest the ambition of Africa to build a dynamic, inclusive, and integrated digital economy offering the scale and scope necessary for data value creation. Such initiatives include:

- [Agenda 2063](#), the 2013 overarching development strategy for Africa, emphasizes “inclusive growth and sustainable development” through increased capacity for innovation, science and technology;
- The African Union’s (AU) [Digital Transformation Strategy](#) (DTSA) addresses legacy deficits in continental cooperation and cohesion, and seeks to establish a digital single market in Africa by 2030;
- The AU [Data Policy Framework](#) presents detailed recommendations to guide the formulation of domestic policies, strengthen cooperation among countries, and promote intra-Africa flows of data.

In parallel, an ambitious agreement establishing an [African Continental Free Trade Area](#) (AfCFTA) was adopted in March 2018. Although it entered into force in 2019 and 44 countries have already ratified it as of 2022, the specific protocols related to digital and data-related policies are still under negotiation. There is however a significant hope that this framework will enable the creation of an African digital single market.

Figure 19

African Continental Free Trade Area enables the achievement of a common digital single market in Africa.



However, a note of caution regarding the challenges of harmonization comes from the low formal adoption of the 2014 AU [Convention on Cyber Security and Personal Data Protection](#) (Malabo Convention). As of 2022, it has only been ratified by 13 countries and as a result, hence, it has not yet come into force.

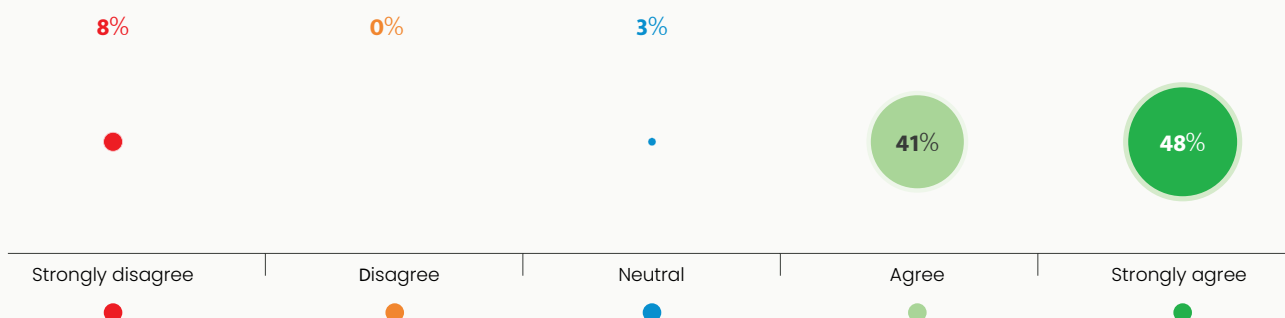
DATA GOVERNANCE WILL BE A KEY, STILL UNDERAPPRECIATED, PART OF DIGITAL POLICIES

Of all the policies dealing with the development of a more equitable digital society, the governance of data constitutes a foundational element to generate social and economic value. There is in that regard, a broad recognition that:

- Ensuring **cross-border data flows**, not only among African countries but also with the rest of the world, is critical for the development of a prosperous digital economy in the continent;

Figure 22

Data flows are beneficial



- This requires nonetheless significant convergence of diverse regulatory frameworks **guaranteeing high levels of protection** in terms of, inter alia, privacy, law enforcement access to data, or content moderation;
- A particular attention needs to be devoted to the **equitable distribution of the value created** by the sharing of data among actors in situations of power imbalances.

STRUCTURING QUESTIONS

The following four structuring questions are put forward as a contribution to the ongoing debate on digital policies in Africa. They are naturally not exhaustive, but examples of a framing approach to formulate, at various levels, common challenges to foster the necessary cooperation. The methodology can be applied to other issues.

What path toward harmonization?

The stark disparity of legal and economic development situations among African countries makes achieving full harmonization a particularly difficult objective. This is still true even in the European Union, which builds upon decades of convergence among less numerous and more similar economies, and benefits from strong regulatory instruments that the African Union does not possess to the same degree.

Not hampering further progress in the most advanced countries can conflict with the desire to establish sufficiently common rules across the continent. **A flexible approach toward progressive convergence** might be necessary to accommodate the different situations without introducing excessive distortions of the competition landscape.

A dedicated discussion needs to take place to determine the right combination of legal interoperability and full harmonization to create the necessary cooperation between different country groupings. More generally, further development of rule of law and political legitimacy are essential to creating trusted environments leading to effective cooperation.

What digital infrastructure strategy?

The success of any digital ambition for Africa depends on access to reliable digital infrastructure. Enormous progress has been achieved in the last ten years in terms of connectivity, through the multiplication of undersea cables connecting the continent to the global network and terrestrial backbones internally, even if the connectivity of very low density rural communities remains a challenge.

However, the situation remains very different in terms of location of **data centers**, due to often unreliable electric power, unfavorable climate conditions and legal and political instability. Thus African actors still need access to cloud services located outside of the continent that can provide the necessary degree of reliability and security protections.

A dedicated strategy to **progressively develop this layer of the data infrastructure** on its territory should form an integral part of any general digital ambition for Africa, taking into account the optimal locations for such data centers, which may not immediately exist for every country. A corollary is that generalized data localization measures would prevent the construction of a coherent and progressively scalable continental infrastructure and ultimately hurt the development potential of many actors.

How to leverage data sharing for development?

Data is essential to achieve the Sustainable Development Goals (SDGs), which are of critical importance for Africa, for instance in terms of access to water, food, health, or energy, and with regards to urban planning or climate change mitigation.

A major part of a **data for development strategy for Africa** should encompass the strengthening of reliable national statistics, the standardization of data formats in various sectors to foster interoperability and reuse for analysis, encouragement of the creation of data-sharing communities (e.g. data commons, collectives, trusts, or stewardships), and, when appropriate, two-way cooperation between private entities and public authorities (including local ones).

In that regard, the [Datasphere Governance Atlas](#), a publication of the Datasphere Initiative documents a range of such initiatives around the world that can provide useful inspiration.

How to strengthen the voice of Africa in the global data governance fora?

Data governance is becoming a topic high on the international agenda. Yet, these discussions mostly take place in fora where African actors are not present at all (e.g. G7, OECD) or marginally represented (G20), in spite of it representing 17% of the world population (and 25% by 2050).

As a result, African actors are on the receiving end of regulations adopted elsewhere (in particular by the EU). Moreover, the continent as a whole is a battleground for competing regulatory visions of the US, the EU and China, which complexify its efforts at regional integration.

The development of a **specific narrative by Africa** regarding the future of the digital society is a prerequisite to strengthening its voice in the global debate. This can cover in particular: the necessary assessment by other regions of the extraterritorial impact of their regulations, and the more equitable distribution of social and economic value than the current data extractive economy provides.

Africa cannot develop its digital strategies without taking into account the global environment in which it necessarily operates and new interfaces to global processes must be developed to carry the voice of the continent.

ACKNOWLEDGMENTS

In-house coordination was provided by Tracy Sinkamba Faustin, International Research & Project Management Coordinator with research assistance from Joshua Joshua, Consultant (Nigeria) and Waiswa Abudu-Sallam, Consultant and Head Legal Affairs at the Communications Commission Uganda. Overall supervision, strategic guidance and input was provided by Martin Hullin, Deputy Executive Director with additional strategic support and contributions from Bertrand de La Chapelle, Executive Director of the I&JPN. The team is also thankful for the editorial support and contributions from Sophie Tomlinson, Director of Communications, Natalia Loungou, Events and Communications Coordinator, Carolina Rossini, Director of Research and Partnerships - Datasphere Initiative, and Mariana Rozo-Paz, Research Assistant - Datasphere Initiative. We also acknowledge Dr Tomiwa Illori, Postdoctoral Research Fellow, Centre for Human Rights, University of Pretoria as a senior contributor to the Report and Adekunle Balogun, Consultant Content Writer & Editor, Centre for the Study of the Economies of Africa (CSEA) for copy edits.

AUTHORSHIP TEAM (Research ICT Africa-RIA):

AUTHOR:

Dr Alison Gillwald
Executive Director
Research ICT Africa (RIA)
South Africa

RESEARCH ASSISTANCE:

Dr Andrew Rens
Senior Researcher
Research ICT Africa (RIA)

Dr Dunia Prince Zongwe
Senior Researcher
Research ICT Africa (RIA)

Hanani Hlomani
Legal Researcher
Research ICT Africa (RIA)

Naila Govan-Vassen
Project Manager
Research ICT Africa (RIA)

PROJECT COORDINATION (Internet & Jurisdiction):

Tracy Sinkamba Faustin
International Research & Project
Management Coordinator
Secretariat of the Internet & Jurisdiction
Policy Network

RESEARCH ASSISTANCE:

Joshua Joshua
Consultant
Nigeria

Waiswa Abudu-Sallam
Senior Research Advisor/Head of Legal,
Uganda Communications Commission
Uganda

PROJECT TEAM (Internet & Jurisdiction):

Martin Hullin
Deputy Executive Director
Secretariat of the Internet & Jurisdiction
Policy Network

Bertrand de La Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction
Policy Network

PRODUCTION:

Secretariat of the Internet & Jurisdiction Policy Network, Paris, France

EDITING:

Sophie Tomlinson
Director of Communications
Secretariat of the Internet & Jurisdiction Policy Network

Natalia Loungou
Events and Communications Coordinator
Secretariat of the Internet & Jurisdiction Policy Network

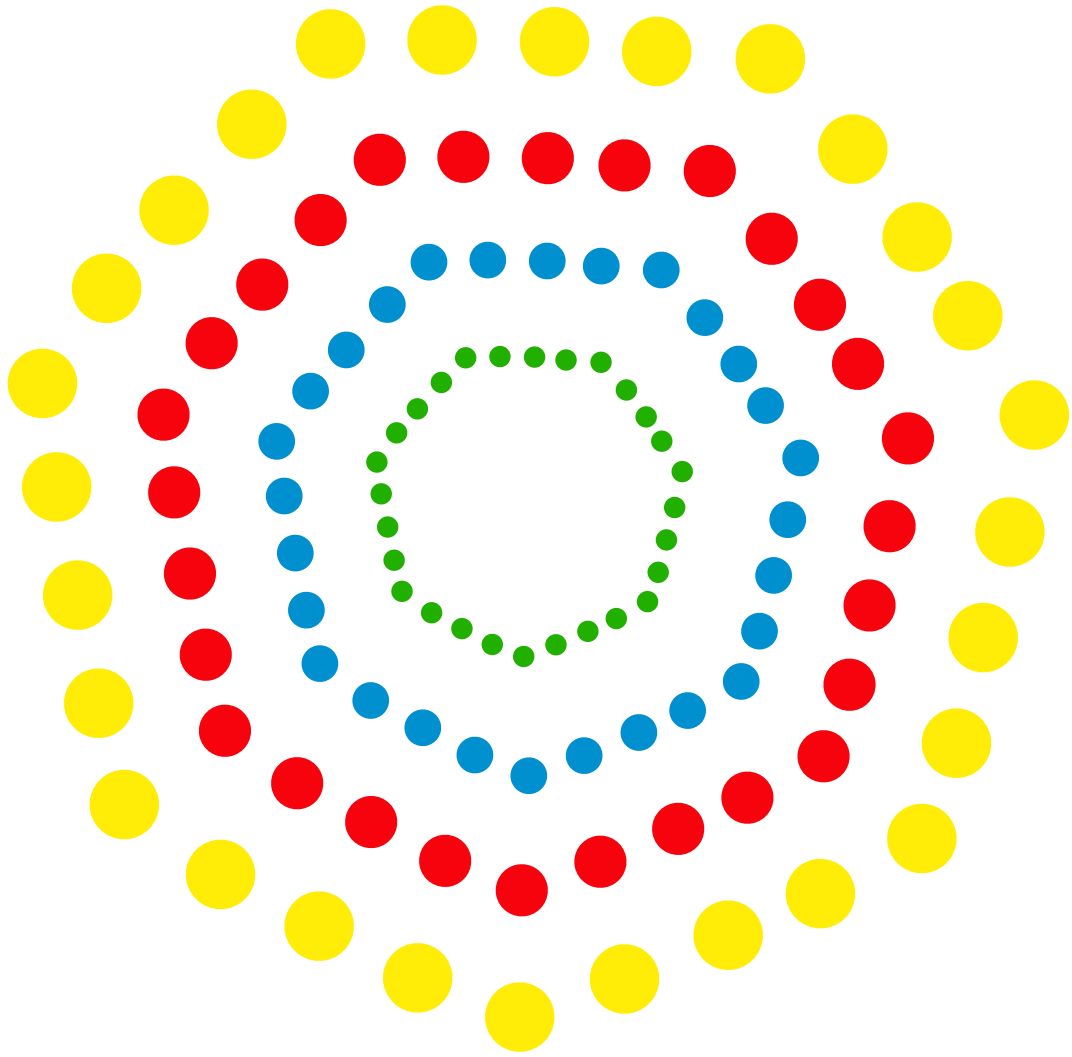
Carolina Rossini
Director of Research and Partnerships - Datasphere Initiative
Secretariat of the Internet & Jurisdiction Policy Network

Mariana Rozo-Paz
Research Assistant - Datasphere Initiative
Secretariat of the Internet & Jurisdiction Policy Network

Dr Tomiwa Illori
Postdoctoral Research Fellow, Centre for Human Rights, University
of Pretoria

Kunle Balogun
Consultant, Consultant Content Writer & Editor, Centre for the
Study of the Economies of Africa (CSEA)

DESIGN AND LAYOUT: [Hubble Studios](#), South Africa



We greatly appreciate the time and contributions of all Knowledge Dialogue workshop participants, survey respondents and interviewees. Without their valuable insights, this report could not have been produced.

Abdul Hakeem-Ajjola

Chair
Strategic Road Map Action Plan Committee of
the Nigeria Data Protection Bureau (NDPB)
Nigeria

Adedeji Adeniran

Director of Research
Centre for the Studies of Economies of Africa
(CSEA)
Nigeria

Akintunde Seriki

Content Lead, Digital Media and
Communications
Lagos State Traffic Management Authority
Nigeria

Andrew Partridge

Senior Economist
Research ICT Africa
South Africa

Annexious Chomo

Systems Analyst
Ministry Of Tourism
Malawi

Asma Awad

Network Operation Engineer
National Information Center
Sudan

Badriyya Yusuf

Researcher
Queens University
Canada

Banji Michelo

Manager Legal and Regulatory Affairs
Zambia Information and Communications
Technology Authority (ZICTA)
Zambia

Billy Boruett

Advocate
Kenya

Brian Tshuma

Co-Director
Southern Data Clinic
Ghana

Bulelani Jili

Meta PhD Fellow
Harvard University
USA

Bridget Boakye

Policy Lead
Tony Blair Institute
Ghana

Abigail Yeboah

Head of Administration
Data Protection Commission
Ghana

Afi Edoh

Master Student of Artificial Intelligence
Dakar Institute of Technology
Senegal

Alastair Tempest

Chief Executive Officer
Ecommerce Forum Africa
South Africa

Alice Kibombo-Ekanya

Librarian
Wikimedia User Group Uganda (WMUGU)
Uganda

Andrey Shcherbovich

Visiting Fellow
McGill University
Canada

Anthony Butler

Chief Technology Officer
IBM Saudi Arabia
Saudi Arabia

Avis Momeni

Secretary General / Digital Rights
Researcher Protege QV
Cameroon

Bahate Mwakasole

Team Lead Convenor
Digital Inclusion Campaign Team-Malawi
Malawi

Benard Kipkorir Koeh

Executive Director
Boresha Life Empowerment Kenya
Kenya

Berenice Fernandez Nieto

Researcher
Data-Pop Alliance
UK

Blessed Marecha

LLB Final Year Student
Midlands State University
Zimbabwe

Catherine Muya

Program Officer - Digital
Article 19
Kenya

Abubakar Orisankoko

Technology Law Specialist
Centre for Data Privacy Professionals
UK

Aji Fama Jobe

Digital Advocate and Software Developer
Women Techmakers Banjul
The Gambia

Alexander White

Privacy Commissioner
Office of the Privacy Commissioner for
Bermuda
Bermuda

Alinafe Nthondowa

IT Technician
Vortnet
Malawi

Aretha Mare

Project Manager - Data Governance Smart
Africa
Rwanda

Awua Aondongu

College Librarian
College Of Nursing Sciences
Nigeria

Balbine Manga

Coordinator
@JURIS.TIC
Cameroon

Benjamin Akintunde Akinmoyeje

PhD Informatics Research Student
Namibia University of Science and
Technology Namibia

Bernard Brian Cudjoe

AU-GFCE Liaison Officer
Global Forum on Cyber Expertise (GFCE)
Ghana

Bonface Witaba

Senior Researcher
Digital Agenda for Tanzania Initiative
Kenya

Bukola Oronti

Executive Council Member
Internet Society (ISOC) Nigeria Chapter
Nigeria

Cecil Agbley

Volunteer
Youth Alliance On Sustainability
Ghana

Charmaine Smith

Writer
Research ICT Africa
South Africa

Courage Chileegbo

Chief Technology Officer
Cygec IT Solutions
Liberia

Denis Pastory

Research Scientist in Applied Data Science
Tokyo University of Agriculture
Japan

Dirk Brand

Legal Consultant
Self-Employed
South Africa

Ernest Mafuta

Chairman
Affordable Internet Access SIG Zambia

Ewan Sutherland

Visiting Professor
Link Centre
University of Witwatersrand
South Africa

Folake Olagunju

Program Officer ICT
Economic Community of West African
States (ECOWAS)
Nigeria

Gabriel Karsan

Director
Emerging Youth Initiative
Tanzania

Gianluca Misuraca

Founder and Vice President
Inspiring Futures SA
Spain

Godfrey Mfuné

Member
Data Inclusion Campaign Malawi
Malawi

Hansol Park

Crime Prevention and Criminal Justice
Officer UNODC
South Korea

Hawi Rapudo

Project Officer/Director
Kijiji Yeetu
Kenya

Chiti Mbizule

Researcher
Kanzi Insights
Zambia

Davi Severiano Goia Cabral D'almada

Director of the Information and
Communication Center
National Regulatory Authority for ICTs
Guinea-Bissau

Dennis Redeker

Postdoctoral Researcher
Universität Bremen
Germany

Dorice Kaijage

Coordinator
Omuka Hub
Tanzania

Ethan Mudavanhu

Tech Lawyer
Access Partnership
South Africa

Fatou Sarr

Volunteer
Internet Society (ISOC), Senegal Chapter
Senegal

Francis Monyango

University of Nairobi
LLM student
Kenya

Gbenga Sesan

Executive Director
Paradigm Initiative
Nigeria

Gilles Bana

Global Trends Analyst
Cullen International
Belgium

Guilherme Fitzgibbon

Head of Political Sector, Embassy in Nairobi
Ministry of Foreign Affairs of Brazil
Brazil

Harold Fote

Monitoring and Evaluation Officer
National Planning Commission of Malawi
Malawi

Hayford Oppong

Director
Configured Technology Limited
Ghana

Clara Stinshoff

Junior Professional Officer
World Bank
USA

Deon Woods Bell

Senior Advisor, Global Policy
Bill and Melinda Gates Foundation
USA

Derrick Mkandawire

Freelance Systems Analyst
Academia
Malawi

Ephraim Percy Kenyanito

Senior Program Officer
Article 19
Kenya

Evelyn Namara

Program Manager & Researcher
Alliance for Affordable Internet
Uganda

Fitina Kalua

IT Officer
University of Livingstonia
Malawi

Franck Adopo

PhD Student - Data Protection Panthéon-
Assas University Paris
France

George Mhlanga

ICT Officer
Ministry of Health
Malawi

Glenn Mcknight

Information Officer
North American Regional At-Large
Organization (NARLO)
Canada

Günther Cyranek

Independent Consultant
Germany

Hatchson Mkwapatira

Business Development Manager
TurnKey Market Solutions (TMS)
Malawi

Ismael Abdulai

Partner
Renaissance Law Chambers
Ghana

Israel Masiano

Public Relations Officer
Ministry of Water and Sanitation
Malawi

Jimmy-Christel Ngoma

Senior Project Manager
International Telecommunications Union
(ITU) Ethiopia

JoEllen Urban

Senior Trade Advisor
United States Patent Office (USPTO)
USA

Joyce Mbughi

Program Officer
Evidence Action
Malawi

Juliet Nanfuka

Researcher
Tech Tapestry
Uganda

K Mohan Raidu

President
Internet Society (ISOC) India Hyderabad
Chapter
India

Kate Munuka

Regulatory Affairs & Policy Compliance
Manager
MultiChoice
Zambia

Khumbuzo Nkunika

Assistant Director-Communications
Ministry of Technology and Science
Zambia

Koffi Komenan Simon Pierre

Teacher Researcher
Virtual University of Côte d'Ivoire
Ivory Coast

Lale Tuzmen Aktas

Associate
Macmillan Keck
USA

Leandro Ucciferri

Global Partnerships Manager
Ranking Digital Rights
Argentina

Lizzie Lungu

IT/Programmer
Malawi Government - Department Of Civil
Aviation
Malawi

Ihueze Nwobilor

Program Officer
Paradigm Initiative
Nigeria

Jacqueline Rowe

Policy Officer
Global Partners Digital
UK

Joanna Kulesza

Professor
Lodz Cyber Hub / Uni Lodz
Poland

Joseph Ambali

Chief Operating Officer
Dotengee Nigeria Enterprises
Nigeria

Judith Murungi

Legal Research Assistant
DSI-Africa
Kenya

Julien Hounkpe

Professor
University of Abomey Calavi
Benin

Kamal Tamawa

Director of Public Policy, SSA
GSMA
Nigeria

Katharina Höne

Director of Research
DiploFoundation
Germany

Kholofelo Kugler

PhD Fellow
University of Lucerne
Switzerland

Kossi Amessinou

Coordinator - World Bank Projects Ministry of
Economy & Finance
Benin

Kouakou Fulgence

Member
Youth IGF
Ivory Coast

Lateef Ayinde

Graduate Teaching Assistant
Florida State University
USA

Levy Syanseke

President
Internet Society (ISOC) Zambia Chapter
Zambia

Lomosi Joseph Chinyumba

Repository Administrator
Mzuzu University
Malawi

Ikemesit Effiong

Head of Research
SBM Intelligence
Nigeria

Jimson Olufuye

Principal Consultant
Kontemporary Consulting Ltd
Nigeria

John Gumbo

Web Developer
Unitech
Malawi

Joseph Jarnecki

Research Analyst
Royal United Services Institute
UK

Juliet Maina

Group Senior Manager, Regulatory and
Public Policy
M-PESA
Kenya

June Okal

Fellow
Harvard Law - Harvard University
USA

Kashema Bahago

Research Associate
Centre for the Studies of Economies of
Africa Nigeria

Katitza Rodriguez

The Electronic Frontier Foundation
Policy Director For Global Privacy
Peru

Kirsten Van Camp

Policy Officer
European Commission
Belgium

Koech Benard

Executive Director
Boresha Life Empowerment Kenya Kenya

Lauren McCarty

Privacy and Data Policy
Meta
USA

Lillian Nalwoga

Director
Internet Society (ISOC) Uganda Chapter
Uganda

Louisa Kabwila

Fundraising & Communications Specialist
Ministry of Information & Digitalization
Malawi

Maateuw Mbaye

Program Assistant
Article 19
Senegal

Malekgoloane Malapane

Board Member
.ZA Domain Name Authority (ZADNA) South
Africa

Margaret Nyambura Ndung'u

Senior ICT Regulatory and Internet
Governance Expert
GFA Consulting Group GmbH
Ethiopia

Martin Gordon Mubangizi

Data Science Officer
UN Global Pulse Kampala
Uganda

Massima Jacquest

ITU Representative for Central Africa and
Madagascar
International Telecommunications Union
(ITU) Cameroon

Melissa Zisengwe

Program Officer
Civic Tech Innovation Network (CTIN)
South Africa

Merriam Manyozo

Chief Systems Analyst
Lilongwe City Council
Malawi

Michelle Mwelesa

Advocacy Officer
Civic Freedoms Forum
Kenya

Mohamed Farahat

Lawyer/Legal Researcher
North Africa Internet Governance Forum &
African Digital Rights Network
Egypt

Morisola Alaba

Coordinator
Nigeria Youth Internet Governance Forum
Nigeria

Moses Otsieno

Researcher
Cyber Policy Centre
Kenya

Nancy Kisangau

Associate
Oraro & Company Advocates
Kenya

Neema Lungangira

Member of Parliament
Parliament of Tanzania
Tanzania

Mahamoud Moustapha Daher

Member of Parliament
National Assembly of Djibouti and Member of
Pan-African Parliament
Djibouti

Manal Ismail

Chief Expert, Internet Policies
NTRA
Egypt

Mariam Jobe

Executive Secretary
Give1 Project Gambia
The Gambia

Martina Ferracane

Fellow
European University Institute (EUI)
Italy

Mbanandi Saka

Chief Editor
Youth Net & Counseling
Malawi

Melody Musoni

Senior Subject Matter Expert: Data Protection
SADC Secretariat
South Africa

Michael Ilishebo

Law Enforcement Officer
Zambia Police Service
Zambia

Mike Dumakude

Business Development Officer
Ngoma FACET Enterprises
Malawi

Mohammed Awal Alhassan

Outreach, Campaigns and Communication
Manager
Dagbani Wikimedians User Group
Ghana

Morris Namaona

Senior Clerical Officer
Ministry of Health
Malawi

Mphatso Jezman

Council For Nongovernmental Organisations
In Malawi (Congoma)
Malawi

Nashilongo Gervasius

Founder & Managing Consultant NamTshuwe
Digital
Namibia

Nicholas Gates

Senior Associate, Policy and Research Digital
Impact Alliance
UK

Manyi Arrey Orok-Tambe

Foreign Affairs Officer
Ministry of External Relations (MINREX)
Cameroon

Mark Dempsey

Team Leader
B&S Europe
Belgium

Mary Uduma

Coordinator
West African Internet Governance Forum
(WAIGF)
Nigeria

Megan Friday

Junior Economist
Acacia Economics
South Africa

Mercy King'ori

Lead Policy Analyst - Africa
Future of Privacy Forum
Kenya

Michael Pisa

Center for Global Development
Policy Fellow
USA

Modestus Amutse

ICT Committee Chairperson
Namibian Parliament
Namibia

Mohamed Chemani

Engineer
ARPCE - Regulation Authority
Algeria

Mohamed Ibrahim

Researcher
Swinburne University Of Technology
Australia

Moritz Hennemann

Professor
University of Passau
Germany

Mudessir Temam Imamu

Social Safeguard Specialist
TRANSIP
Ethiopia

Nazarius Kirama

President
Internet Society (ISOC) Tanzania Chapter
Tanzania

Nicole Gregory

Counsellor (Science, Tech and Innovaton)
Foreign Commonwealth Development
Office (FCDO) - UK Government
Kenya

Nompilo Simanje

Legal and ICT Policy Officer
MISA Zimbabwe
Zimbabwe

Odilile Ayodele

Senior Researcher
University of Johannesburg/IPATC
South Africa

Oluwakemi Adeyanju

Public Policy Manager
Meta
Nigeria

Patrick Sembo

Systems Analyst
E-Government
Malawi

Peterking Quaye

Founder & Executive Director
West Africa ICT Action Network
Liberia

Pren-Tsilya Boa-Guehe

Head of Pan-African Institutions
Google
USA

Rebecca Mukite

Manager Public and International
relations Uganda Communications
Commission
Uganda

Rosalind Kenny Birch

International Policy Advisor
UK Government - Department for
Digital, Culture, Media & Sport
UK

Sam Hall

UK Foreign, Commonwealth, and
Development Office
Ethiopia

Sandra Kachitsa Phiri

Global Youth Ambassador
Theirworld
Malawi

Scott Timcke

Senior Research Associate
Research ICT Africa
South Africa

Sergio Luis Cossa

CEO
Internet Policy & R4ICT Dev
Mozambique

Simon Munyeki Maina

Community Knowledge Facilitator
Arid Land Information Network
Kenya

Sodiq Omoola

Assistant Professor
Law, Faculty
International Islamic University Malaysia
Malaysia

Norman Angel Agong

Research Associate
Whitehead Communications Consult
Uganda

Olubunmi Osuntuyi

Secretary General
International Chamber of Commerce
Nigeria

Onica Makwakwa

Head of Africa
Alliance for Affordable Internet (A4AI) South
Africa

Patricia Boshe

Senior Researcher
Universität Passau
Germany

Pierre Dandjinou

VP, Stakeholder Engagement
ICANN
Benin

Ralph Oyini Mbouna

Director of Digital Transformation &
Services Smart Africa
Rwanda

Robert Walters

Senior Lecturer
Victoria University
Australia

Saara Imbili

Chief Policy Analyst
Ministry of ICT
Namibia

Samantha Chikepe

Legal advisor
First National Bank (FNB)
South Africa

Sandra Makumbirofa

Senior Economist
Research ICT Africa
South Africa

Sellah Yekha

Tutor
Discom Communications
Malawi

Shadrach Haruna

Director General
National Drug Agency
Nigeria

Simone Toussi

Project Office for Francophone/Central
Africa CIPESA
Cameroon

Souhila Amazouz

Senior Policy Officer
African Union Commission
Ethiopia

Nthabiseng Pule

Project and Outreach Manager
Cybersecurity Capacity Centre (C3SA)
Lesotho

Oluseyi Oyebisi

Executive Director
Nigeria Network of NGOs
Nigeria

Otto Saki

Program Officer
Ford Foundation
USA

Peter Makata

Network Support Engineer
Telekom Networks Malawi
Malawi

Praise Sunday

Cloud Engineer
ProgitNG
Nigeria

Raymond Onuoha

Tech Policy Fellow
Lagos Business School
Nigeria

Rory Macmillan

Partner
Macmillan Keck
Switzerland

Salyou Fanny

Country Coordinator
Internet Governance Forum (IGF) Ivory Coast

Samuel Dada

Program Officer
Africa ICT Alliance
Nigeria

Sandro Bazzanella

Digital Team Leader
African Union Commission
Ethiopia

Serge Koudjo

Manager
Joviale Services
Benin

Sherine Achieng

Advocacy Assistant
Niyel
Rwanda

Sitshengisiwe Ndlovu

Customs and Trade Expert Organisation of
Women in International Trade Zimbabwe

Stephanie Mainye

Legal Assistant, Center for IP and Information
technology Law
Strathmore University
Kenya

Steven Pacome Arnaud Akomian

Research Assistant
Paradigm Initiative
Ivory Coast

Tapiwa Cheuka

Trade Policy Officer
African Union
Ethiopia

Thabo Mashegoane

Chairman
Africa ICT Alliance (AfICTA)
South Africa

Tim Smith

General Manager
Canadian International Pharmacy Association
(CIPA)
Canada

Verengai Mabika

Senior Policy Advisor
Internet Society (ISOC)
Zimbabwe

Wilfred Warioba

Executive Director
Haki maendeleo
Tanzania

Yamba Dabone

University Joseph Ki-Zerbo
Burkina Faso

Stephen Walker

Director
Data for Development Network (D4D.net)
Canada

Suzete Centeio

Technician
ARME
Cape Verde

Teki Akuetteh

Executive Director
Africa Digital Rights Hub
Ghana

Thiago Sombra

Partner
Mattos Filho
Brazil

Tochukwu Nwankwo

Senior Librarian
University of Nigeria
Nigeria

Vincent David Mbombo

Programme Manager
Haki Maendeleo
Tanzania

Willard T Mugadza

Midlands State University
Lecturer
Zimbabwe

Yolanda Kisenyi

Policy Advisor
UK Government - Department for Digital,
Culture, Media & Sport
UK

Steven Frédéric Ondongo

Legal Advisor Ministry of Posts,
Telecommunications and Digital Economy
Republic of the Congo

Takafumi Ochiai

Senior Partner
Atsumi & Sakai
Japan

Thokozani Msowoya

Graduate
Malawi University of Science and
Technology Malawi

Towela Nyirenda-Jere

Head, Economic Integration
AUDA-NEPAD
South Africa

Tracey Lauriault

Associate Professor, Critical Media, & Big
Data Carleton University
Canada

Walid Zayed

Consultant
Trade Facilitation
Egypt

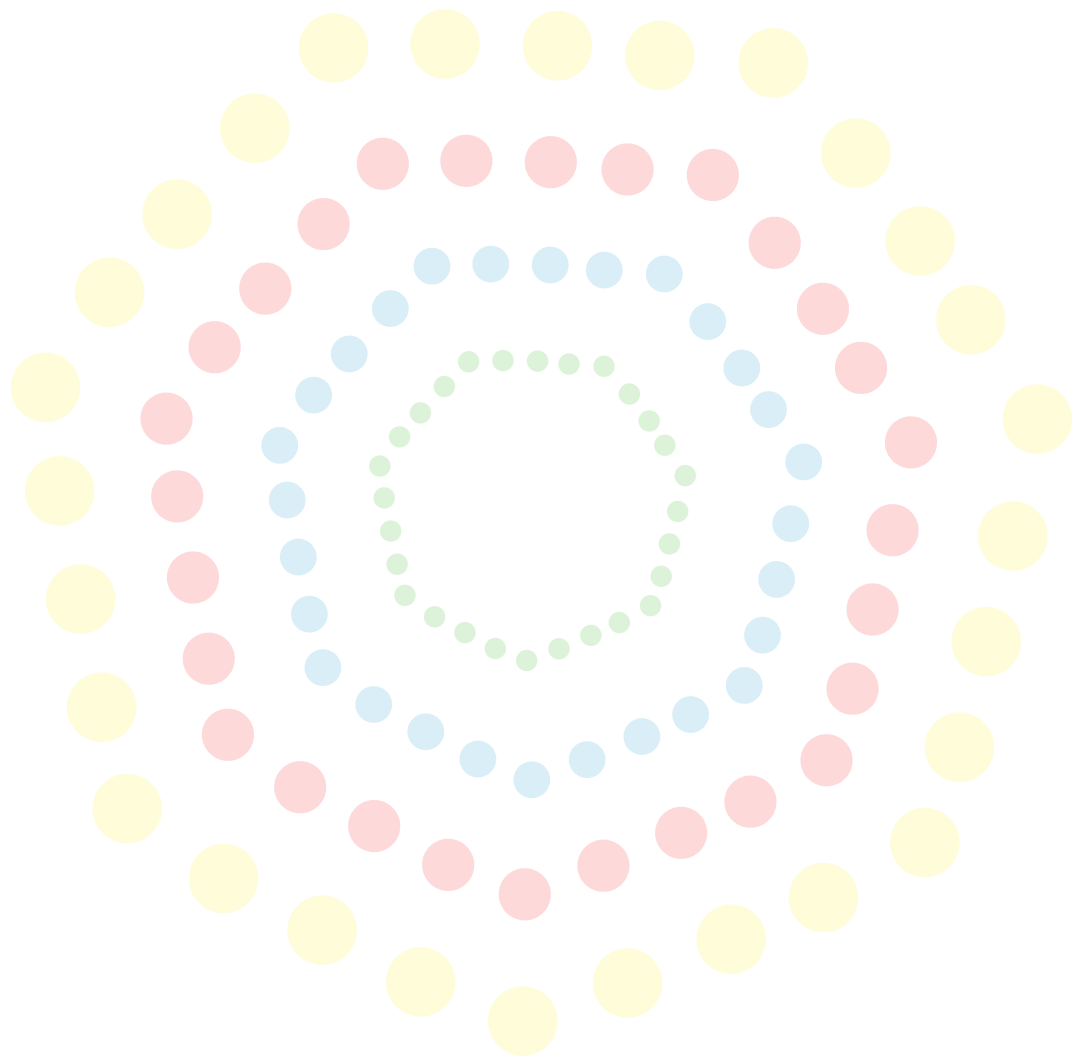
Wezzie Lukhere

Managing Director and Lead Consultant
CyberSofonet
Malawi

Winnie Kamau

Editor
Association of Freelance Journalists
Kenya





INTRODUCTION

With the emergence of data-driven digital technologies leading to innovations in service delivery and business, data has become an essential asset in the digital economy, be it global, regional or national. The introduction identifies the challenges that policymakers face to formulate appropriate data policies as a result of the intensification of the processes of digitalization and datafication.

The first chapter, titled 'Policy Context', addresses, in more detail, the global challenges of formulating appropriate policy for digital economies, especially with regard to the central role of data and cross-border data flows. Data is both structurally and generatively important to development. A wide range of issues raise cross-border questions. However, this should not obscure the fact that cross-border data flow, being both an important and urgent issue on which most policy progress, although incomplete, has been made, is the focus of the Report. This chapter also explains the significance of data, as well as gives the context for cross-border data flow.

The second chapter on Topical Trends in Africa documents overarching and topical cross-border digital policy trends. Two major issues that emerged from the conversations held are the need for coordination and harmonization on digital policy and external influence on African data policy. Part I of this chapter focuses on African trends around trusted environments. It is followed by Part II, which focuses on inclusive economy, by addressing the subjects of competition, taxation, financial inclusion, and mobile money. Also, Part II briefly highlights the infrastructure challenges and brings attention to the development of digital identity systems and data centers in the continent.

Part III investigates activities related to coordination and harmonization of digital cross-border policies. It also shares some of the collected perspectives of the Report contributors on important reasons for African countries to work together to regulate data.

Part III, moreover, emphasizes the need for forging common narratives about Africa as a dynamic, integrated economy offering the scale and scope required for data value creation and an enabling and certain data policy environment for local and foreign investment, trade, and innovation. Complementary narratives on the collaboration, coordination, and harmonization being undertaken by African countries should give credence to the creation of these conditions. Together with the narrative on African common interests and voice in matters of global governance that emerged from the study, complementary meta-narratives are needed to counter narratives of Africa as voiceless, uncoordinated, and constrained.

The third chapter discusses the possible solutions for Africa to frame digital and data policies. Part I examines Africa's need for a coordinated strategy for data infrastructure. While data center infrastructure is a requisite for successfully using data for development, the continent must also ensure a reliable power supply and high-speed data connection. Part II analyzes the need for harmonized legal standards. Stakeholders expressed the view that the AfCFTA presents the opportunity to create a digital single market through cross-border harmonization, in which data flows will enable economic development. While already there are binding international and continental conventions on human rights and charters on the Internet to create a trusted and functional data environment, these need far more actively informed digital policy and regulation. There is a strong sentiment that cross-border data flows with the necessary protection of personal data is essential for economic development and integration of Africa more competitively into the global economy. Indiscriminate data localization, particularly where there is no capacity locally to create value with it, will deprive countries of the efficiencies and productivity gains associated with improved data and information flows.

The remainder of this Introduction looks at the challenges of digitization and datafication, data value creation, provides an overview of African policy responses, and sets out the need for the Report, the methodology, and early findings.

THE CHALLENGE OF DIGITIZATION AND DATAFICATION

Governments and intergovernmental organizations around the world are grappling with the challenges of formulating appropriate policies to deal with intensifying processes of digitalization and datafication. Major multilateral reports such as the World Bank Development Report 2020¹ and the 2019 United Nations Conference on Trade and Development (UNCTAD) Digital Economy Report² highlight the importance of data, data flows, and data governance in public and private sector development and innovation, in trade, as well as explain it as the basis of international taxation regime reforms. The 2021 UNCTAD Digital Economy Report examines data flows as a critical enabler of economic development.³ Cross-border data flow has emerged as the most prominent and pressing cross-border digital issue. A finding from [early stakeholder workshops](#) held in respect of this study highlighted that data policy is a central and urgent concern. Participants voiced the necessity for data policies to shift the currently uneven distribution of opportunities both between and within countries so as to (1 enable Africa as a whole to benefit from the data-driven technologies and (2 ensure that these benefits are shared equitably among all its inhabitants.

The Report thus focuses on this issue while simultaneously reviewing a broad range of related cross-border digital issues. Due to the potential of data for development, most of the solutions are focused on data.

As data becomes a critical factor of productivity and innovation underpinning the global economy, ensuring cross-border flows is a prerequisite for access to efficient infrastructures (often localized abroad and for digital markets to become competitive. This is critical as Africa transitions to a digital single market under the AfCFTA. Therefore, policies and regulations that responsibly enable cross-border data flows are central to extending the scale and scope of value creation.

Common to the various frameworks emerging across the globe is the recognition that a trusted environment for data exchange, sharing, and flows in general, is essential to realizing data value. To this end, some countries on the globe have developed and implemented a range of policies and regulations to unilaterally govern the flow of data across borders in an effort to establish trust.⁴ Creating value from data requires a level of data interoperability. Unhindered access, use and reuse of data within any ecosystem are fundamental to leveraging the social and economic benefits of emerging technologies, and have thus taken center stage in data governance discourse.

Emerging data-driven technologies that allow innovations in new business models and services promise several positive outcomes: improved administrative efficiency and effectiveness; cost saving for corporations; faster and smarter work; real-time data analytics, and automated decision-making. However, these technologies also introduce new risks or change the possibility of existing risks. In addition to these global concerns, there are particular challenges for African countries including Internet connectivity, power generation, the need to create institutions and geographical barriers.

¹ 'World Development Report 2020: Trading for Development in the Age of Global Value Chains', Text/HTML (World Bank), accessed 20 October 2022, <https://www.worldbank.org/en/publication/wdr2020>.

² 'Digital Economy Report 2019 | UNCTAD', accessed 6 September 2022, <https://unctad.org/webflyer/digital-economy-report-2019>.

³ UNCTAD, 'Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow', United Nations publication (Geneva, 2021). https://unctad.org/system/files/official-document/der2021_en.pdf

⁴ AUC/OECD, Africa's Development Dynamics 2020: Digital Transformation for Quality Jobs (AUC, Addis Ababa/OECD Publishing,, Paris, 2021), <https://doi.org/10.1787/0a5c9314-en>.

Although the harms associated with the proliferation of data such as breaches of privacy are universal, the impacts are uneven. Even in systems where there are guardrails, such as requirement of informed consent by data subjects of the use of their data, the most marginalized often fall in between the rails. This is either because they are unable to exercise their rights that data protections offer or because they are marginalized from the data system altogether; hence, unable to enjoy any of the benefits.

In addition, the effective governance of data must deal with the global nature of data flows. This requires much greater levels of global cooperation and more engagement by African countries in international decision-making forums. Currently, standards and protocols are set in mature markets of the Global North to meet domestic and regional needs, while the Global South broadly and Africa, in particular, have historically been ‘standards takers’.

Associated with the rapid datafication of the economy and society is the increasing concentration of the ownership of, and ability to, derive value from data. Over 90% of the market capitalization value of the 70 largest platforms is estimated to be concentrated in two countries – China and the United States. By contrast, Europe accounts for only 4% and Africa and Latin America together for 1%.⁵

Large pools of data are accumulated by these few tech corporations, making them become *de facto* proprietary data assets in global centers of wealth and power with significant geopolitical implications. As big data becomes an increasingly important resource, this leaves countries in the Global South, as well as the marginalized communities all over the world, especially disadvantaged.⁶

Whether or not countries and regions are able to create the conditions for the harnessing of these processes of digitization and datafication, in order to create added value, increase efficiency and productivity, create new jobs, and optimize revenue-generating trade and taxation, will depend on the policies adopted and implemented. This is a common institutional challenge for developing countries. As stated by UNCTAD, “Harnessing [data’s] potential for the many, and not just the few, requires creative thinking and policy experimentation”.⁷ While this will present challenges at different levels of government, the globalized nature of data will nevertheless require greater global cooperation to overcome many of them.

The uneven distribution of opportunities and risks reflects the levels of human and economic development of countries and the existing inequalities between and within countries. The ability of countries and regions to counter these trends will be dependent on their ability to create an enabling environment for data-driven value creation that is more inclusive and equitable.⁸ However, legal and regulatory frameworks for data are still inadequate in many lower-income countries, which often have gaps in critical safeguards, as well as shortages of data-sharing initiatives.⁹ The Data Policy Framework adopted by AU Member States in 2022 has gone some way in filling this gap.

DATA VALUE CREATION

In the context of digital policies, data is the foundation of the digital economy. It is recognized as a public good, often not constrained by geographical boundaries, due to the decentralized architecture of the Internet. Data is valuable when it enables the government and the private sector to deliver public services

⁵ ‘Digital Economy Report 2019’, Digital Economy Report, 4 September 2019, https://unctad.org/system/files/official-document/der2019_en.pdf.

⁶ Alison Gillwald et al., ‘GPAI Data Justice Policy Brief: Putting Data Justice into Practice’ (Global Partnership on AI, November 2022), <https://gpai.ai/projects/data-governance/data-justice-policy-brief-putting-data-justice-into-practice.pdf>.

⁷ United Nations Conference on Trade and Development, Digital Economy Report 2019: Value Creation and Capture : Implications for Developing Countries, 2019.

⁸ Gillwald et al., ‘GPAI Data Justice Policy Brief: Putting Data Justice into Practice’.

⁹ World Bank, ‘Data for Better Lives.’ (Washington D.C.: World Bank, 2021), doi:10.1596/978-1-4648-1600-0.

effectively, a situation which requires understanding data demand, and how institutions can leverage it through data governance to enhance service delivery and address socio-economic challenges.

Data takes myriad forms, and its definition is highly contested. Data can be broadly categorized into personal and non-personal data, despite their blurred boundaries. What constitutes personal data shifts as technologies become better at inferring individually relevant data from apparently impersonal data. Data originates from multiple sources and can be used and reused across various industries and sectors in real time without detracting from anyone else's use of them. Until recently, unlike trade and the movement of physical goods, data, with its underlying open Internet architecture, was often not constrained by geographical boundaries. Data is heterogeneous and, as a result, is understood as many things: from digital bits and bytes, to values and statistics (processed data), to information (constructed data). What distinguishes the dominant forms of data being used in new data services is that it is user generated. Although data is increasingly understood as a valuable and even strategic resource, valuing data has presented a particular challenge that has exercised the minds of academics, multilateral agencies and policymakers. What there is consensus on is that data has in and of itself little value. It is only through the processing, transmission, storage and combination of data that value is added or extracted. In economic terms, data is understood as a public good that has variable returns. It is inherently non-rivalrous (at the technical level, it is infinitely usable without detracting from another person's ability to use it). It is also naturally non-excludable, which means that there are no natural barriers to multiple people using the same data at once. Although data may be rendered excludable through technological and legal means, these are not inherent features of data.¹⁰

Furthermore, the accumulation of data alone has no economic value – this requires complementary investments and activities. It is what organizations do with data that leads to value creation, both internally within the organizations and externally across the extended-data network. This value can theoretically be quantified by assigning monetary value to the collection of data, taking into consideration several cost and income-generating variables, like how organizations charge for user-generated data, or reconcile data management costs such as collecting, maintaining and publishing data. The value from data, either from the socio-economic benefits or public perspective, manifests when the fundamental conditions or enablers that allow governments or effectively regulated private companies to deliver improved public services or offer effective environmental stewardship are in place, and when citizens live healthier and economically secure lives through leveraging data.¹¹

Although the focus has been on the vast wealth that has been accumulated through private value creation, there is increasing recognition of the public value that can be realized from the effective production, management and sharing of public sector data. Effective value creation from public sector data requires a comprehensive approach to understanding data demand, and how it can be leveraged through adequate data governance to enhance service delivery and address socio-economic challenges. Public interest value can also be realized through data collected by private actors. Hence, it would be a mistake to label all such data as 'private'. Realizing data as a digital public good requires demand side valuation of resources such as data and not only traditional commercial supply valuation. It is the traditional commercial supply valuation that recognizes data as a critical input downstream and opens up the collective organization and regulation of data commons or lakes, and more equitable access to data through open data standards, in the form of comprehensive protections offered by alternative data stewardship models.

Data is key to making progress toward meeting the SDGs. National statistics and coordination are essential to data supporting development in cooperation with global intergovernmental organizations (IGO's).

¹⁰ African Union, 'AU Data Policy Framework' (African Union, 2022), <https://au.int/en/documents/20220728/au-data-policy-framework>.

¹¹ World Bank, 'World Development Report 2021: Data for Better Lives', Text/HTML, World Bank, 2021, <https://www.worldbank.org/en/publication/wdr2021>.

Africa is confronted with major developmental challenges, including in land and water use and rapid urban development. Sharing data collected and generated on these subjects is essential to finding solutions. There is still a scarcity of essential data for national, regional, and global development policymaking. Many governments still lack access to sufficient data about their whole population. This is especially true for the poorest and most marginalized individuals, who are precisely the group leaders that will need to concentrate on whether or not they want to eliminate severe poverty and all emissions by 2030 and, in the process, “leave no one behind”.¹² Big data can reveal social inequalities that were previously concealed. Women and girls, for instance, who frequently labor in the unorganized economy or at home, face social restrictions on their mobility and are underrepresented in both private and governmental decision-making. Much of the big data with the most potential to be used for public good is collected by the private sector. As such, public-private interplays are likely to become more widespread. The challenge will be ensuring they are sustainable over time, and that clear frameworks are in place to clarify roles and expectations on all sides.

OVERVIEW OF AFRICAN POLICY

Africa is at an important juncture in designing and implementing digital and data policies. The AU has led continental policy development on Digital Transformation Strategy for Africa (DTSA) and its [Agenda 2063](#), emphasizing a clear goal of “inclusive growth and sustainable development” through increased capacity for innovation, science, and technology.

The [DTSA](#) seeks to use the transformation effected by digital technologies to achieve Agenda 2063, and the United Nations Sustainable Development Goals. The strategy addresses legacy deficits in continental cooperation and cohesion, seeking to establish a digital single market in Africa by 2030. This requires regulation of data and the development and sharing of infrastructure, an enabling environment for investment and innovation and extensive skills development.

The strategy, as it applies to data, is further developed in the [AU Data Policy Framework](#). The Framework presents a set of detailed recommendations and arising actions to guide Member States through the formulation of policies in their domestic contexts, as well as the recommendation of measures to strengthen cooperation among countries and promote intra-Africa flows of data. Essential to capturing the benefits of data for socio-economic development is the creation of the appropriate infrastructural, regulatory and institutional capacities. Cross-border data flows are encouraged and enabled through mutual protection of personal data, and common data standards for non-personal data to enable interoperability.

Agenda 2063, the DTSA, and the AU Data Policy Framework declare that all Africans should have the opportunity to be included in the digital economy and benefit from datafication. Accordingly, African countries should present their interests in international policy fora. The Framework also refers to the need to redress the uneven distribution of opportunities, and harms, between countries globally and within countries in the continent through ensuring data justice.

¹² United Nations, ‘Big Data for Sustainable Development’, United Nations (United Nations), accessed 28 October 2022, <https://www.un.org/en/global-issues/big-data-for-sustainable-development>.

THE NEED FOR THE REPORT

The Internet and Jurisdiction Policy Network initiated a process to complement existing regional mechanisms for stakeholders from the African continent to share knowledge, consult one another, interact with stakeholders around the world, and develop a shared understanding of and capacity around digital policy issues.

This Report is the primary outcome of the project, intended to help frame, map and address cross-border digital policies across the African continent. It explores why policy coordination is important to building an inclusive and vibrant digital economy in Africa and identifies key trends taking shape across the region. The project proceeded through the use of regional mechanisms and partnerships, recurring knowledge dialogue workshops, data collection, in depth interviews and desk research. In an effort to analyze trends that are unique to Africa, the Report investigates how stakeholders across the continent view current policy-making efforts, as well as the challenges and opportunities digital transformation is bringing to businesses and communities across the region. The findings uncover some important reflections relevant for the AU [Digital Transformation Strategy for Africa \(DTSA\)](#) and efforts to establish a digital single market in Africa by 2030 and, globally, the UN Roadmap for Digital Cooperation.

This Report aims to provide information that proves useful to understanding some of the complexities of the data ecosystem, specifically the need for policy that promotes interoperability and enhanced data flows that are essential to opening up the continent to itself and the world, as well as contribute to the ambitions set forth in Africa's Agenda 2063 and the SDGs.

Respondents in dialogues, online data gathering and interviews emphasized different aspects of cross-border digital and data policy, ranging from protection of personal data and interoperability, to economic development and the need for human rights. The emerging approaches and concerns included in the Report intend to offer a baseline for further research to support evidence-based policymaking and cross-fertilization of relevant practices and learnings from the region. During the knowledge dialogue workshops, participants emphasized the importance of cross-border data issues as prominent and pressing cross-border digital issues. Given the complexity of cross-border data issues, the Report centers on those issues, while investigating a range of other cross-border digital issues.

We need to make sure that this I&J report on cross-border data does not end up on the shelves like other reports and is not used by anyone. Why I am saying this is because if legislators are made aware and capacitated to be champions of this report, we can ensure the implementation of the recommendations in this report.

- Senior governmental representative during the interview-based data collection phase of this Report

METHODOLOGY

The main research question is: What must Africa do to ensure the benefits of increased data flows, reduce current asymmetries in flows and limit associated harms?

Answering this required identifying important trends and emerging solutions. This research adopted a pragmatic and innovative mix of methods, which included undertaking high-level interviews with decision-makers across the continent (including the main continental organs), crowdsourcing an open interview platform, and undertaking a series of knowledge dialogues, involving the use of brief online polls, with Africans, and then with African and international participants on African cross-border data issues. This multiple-method approach provides a litmus test of diverse stakeholder perspectives on cross-border data flows in the context of intensifying global processes of digitalization and datafication, dynamic continental economic and social developments, and emerging data policy for a single continental market. This is then used to identify common principles and the intersection of interests, the tensions among different policy objectives, and the tradeoffs

that inevitably have to be made in policy. Early interactions helped pose the research question, as well as the additional questions that informed the research:

- What are the most pertinent cross-border digital issues?
- What should continental harmonization focus on to create a development-driven digital single market?
- How might data policy be harmonized?
- What potential is there for creating shared infrastructure, especially data centers?
- How can a trusted environment for value creation from data be created?
- How can African actors cooperate and increase Africa’s influence in global digital and data policy development?
- Can lessons be drawn from the EU’s integration experience: e.g. the distinction between Regulations and Directives?
- What combination of functional interoperability and fully harmonized approaches might best create the necessary coordination between African countries?

To analyze trends that are unique to Africa, the Report investigates how stakeholders across the continent view current policy-making efforts, as well as examines the challenges and opportunities that digital transformation brings to businesses and communities across the region. The findings uncover some important reflections relevant for the African Union [Digital Transformation Strategy](#) (DTSA) and efforts to establish a digital single market in Africa by 2030.

ENGAGEMENT PROCESS AND TIMELINE

November 4, 2021	Internet and Jurisdiction - Virtual Event launched project
December 13, 2021	The first knowledge dialogue workshop brought African stakeholders together to identify important issues of digital policy.
February 22, 2022	The second knowledge dialogue workshop with African and global stakeholders discussed important issues of digital policy and identified the demand for a common African narrative on cross-border data issues.
July 4, 2022	Report on the findings of the knowledge dialogue workshops.
July 19, 2022	A special panel at the African Internet Governance Forum discussed cross-border digital issues, including data flow, and launched the data collection process.
July - August 2022	Online data collection process.
August - October 2022	High level interviews.
October 25, 2022	Key findings workshop .
November 28, 2022	Launch of report at the Internet Governance Forum.

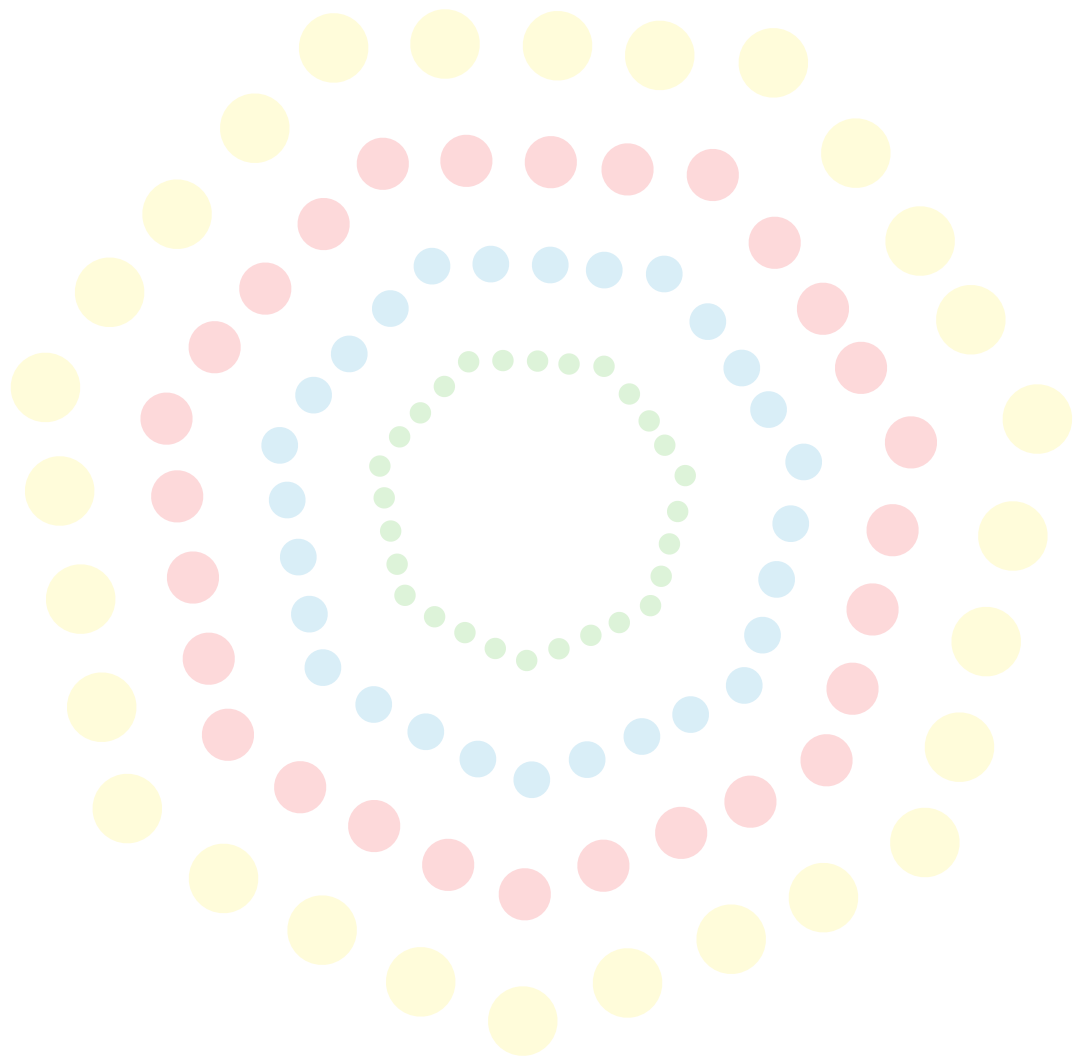
EARLY FINDINGS

The knowledge gained from the research is set out in the next three sections: describing the policy context, identifying the challenges of digital integration in Africa, and seeking possible solutions in Africa. These detailed findings were informed by findings that emerged early in the process.

1. Infrastructure is essential to realize value from digital technology, notably data and including network connectivity and capable data centers.
2. There is need for continental policies that enable harmonized or at least coordinated action for the construction of a digital single market;
3. There is need for continentally and globally harmonized, or at least, coordinated regulation of digital markets dominated by global platforms;
4. Global debates on digital regulation require that Africa to work out a common approach;
5. There are opportunities for Africa to participate in global policy and standards setting by developing a common position on data and the digital economy;

6. The value realized from data should be equitably shared;
7. The extractive nature of dominant forms of data value creation and monopoly profits have raised concerns about the harms to data subjects and the exclusion of data producers for enabling equitable data value realization;
8. There is need for a context for data policy of economic development that includes democratic transparency and accountability and rule of law, which are preconditions for creating the trust necessary for equitable data value creation;
9. There is need to develop a trustworthy and legitimate digital ecosystem, nationally and across borders.
10. Frontier technologies, especially the Internet of Things (IoT) and artificial intelligence (AI), require new governance capabilities across the globe.

This Report does not detail the challenges, which are associated with frontier technologies, but is cognizant that these emerging challenges require that appropriate data policies, discussed in the report, are put in place as soon as possible.



1. POLICY CONTEXT

Globally countries and regions are grappling with the challenges of formulating an appropriate policy for digital economies, especially with regard to the central role of data and cross-border data flows. Data are both structurally and generatively important to development. This chapter describes the nature of data and underlines the importance of cross-border flows in regional economic integration and development as well as the creation of stronger trade links among African states. Part I describes the African Policy Response; Part II focuses on the AfCFTA, while Part III discusses personal data protection and privacy including regional instruments. Part IV examines the complicated relationship between data and intellectual property regimes. Part V discusses the application of competition regulation to data.

Chapter 2 of the Report builds on this chapter and surveys current cross-border digital issues in Africa. A wide range of issues such as the lack of coherent approaches to issues such as cyber security, digital human rights and information disorders raise cross-border questions. However, this should not obscure the fact that cross-border data flow being both an important and urgent issue on which most policy progress, although incomplete, has been made, is the focus of this Report.

Creating economic value from data across the continent requires the harmonization of data policies and regulation, especially with respect to competition, tax and trade policy, which are key policies that enhance data value creation. The creation of value from data also requires enabling technologies such as cloud storage, cloud computing and high-speed Internet. The unhindered access, use and reuse of data within any ecosystem is equally fundamental to leveraging the potential socio-economic benefits of emerging technologies, and this has taken center stage in data policy discourse.

However, private value creation needs to be complemented by public value creation. Data access and sharing is key to addressing societal ambitions and the challenges of meeting the SDGs including goals on water, food security, urban planning, health and energy. Data is also key to addressing climate change, in managing public health crises such as COVID-19 and, also, in facilitating post-pandemic economic reconstruction. To ensure that data are useful in addressing developmental needs African countries need to develop common data standards and formats for interoperability. The provision of developmental data relies on appropriate governance for data commons, data communities, data stewardship and data trusts. Essentially, it relies on such mechanisms that allow data to be shared across borders to address common problems. Governance must encourage data cooperation among commercial, civil society and public actors.

Figure 1

Opportunities for Big Data and the SDGs

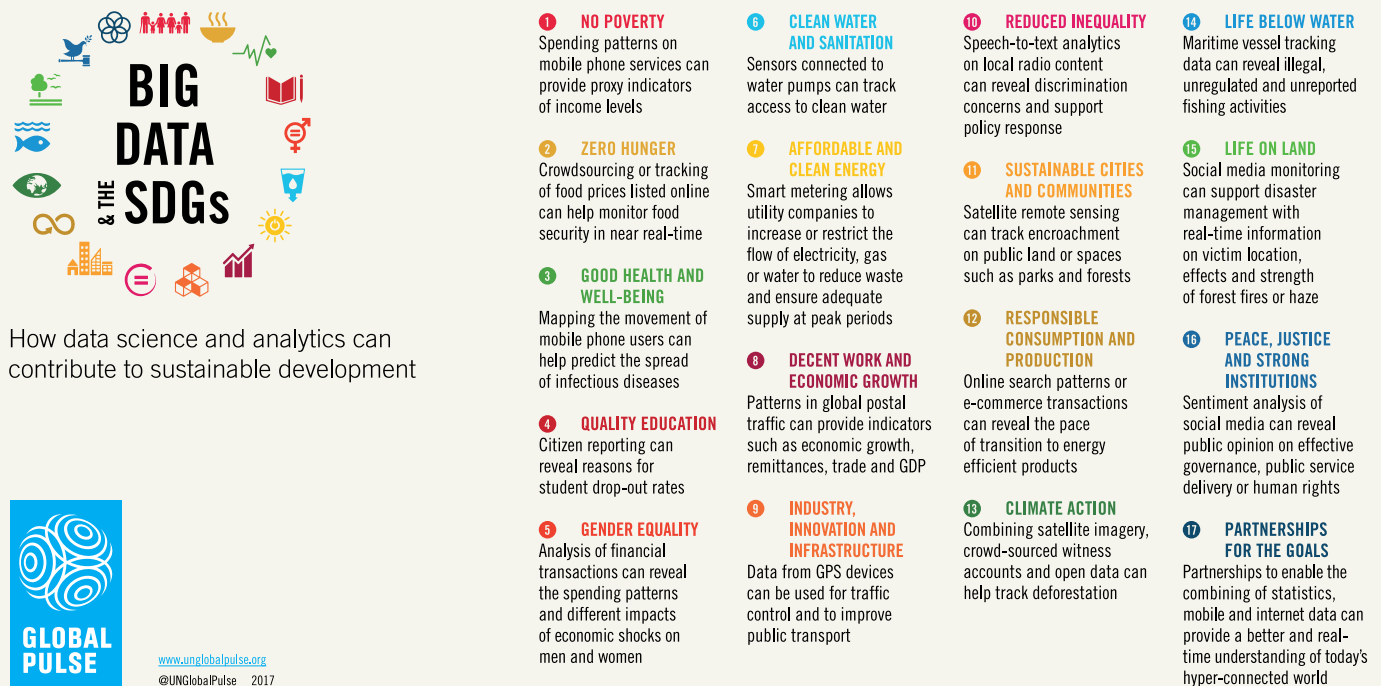


Image from UN Global Pulse 2017

Policies and rules are instrumental to establishing clear control over the division of duties and responsibilities with regard to data, as well as placing restrictions on how control over data may be exercised. Data developments have significantly outpaced the law and this is more apparent in Africa where some countries are neither as digitally ready as other nations across the world, nor as legally ready for the changes that digitization has brought to the fore. Until very recently, data has remained largely unregulated, or at least it has not been explicitly regulated. For the most part, in the absence of explicit data laws or regulations, data has been regulated across the five branches of the law in the continent, namely, data protection law, competition law, cyber security/ electronic communications and transactions law (in tandem with data localization laws), intellectual property law, and common law.

A recurring qualm at the core of the global digital economy is that cross-border data exchanges are not currently covered by any international agreements. There are divergent viewpoints on how to regulate them. Accordingly, there is demand for a coordinated approach not only in cross-border policies in the African continent, but also internationally.

The discussion of international, continental and regional agreements, strategies and frameworks that follows below is not exhaustive. In order to provide a basic overview of how the calls for a unified strategy are justified in light of the abundance of conflicting laws and regulations, a few significant ones have been drawn out for consideration.

I. AFRICAN POLICY RESPONSE

African leaders, working through the AU, have sought to utilize digital technologies to achieve their development goals in Agenda 2063.¹³ The strategies for doing so are set out in the DTSA.¹⁴ Particular attention is paid to data in the AU Data Policy Framework.¹⁵ The recommendations in the Framework call on member states “to promote and facilitate data flows within and among AU Member States by developing a Cross-Border Data Flows Mechanism that takes into account the different levels of digital readiness, data maturity as well as legal and regulatory environments of countries” and “facilitate data circulation across sectors and across borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security.”¹⁶

A key source on the opportunities that can be realized by cooperation across Africa on aspects of the digital economy emerges from the vision of the AU. At the highest level this is shown in Agenda 2063, which is Africa’s blueprint and master plan for transforming the continent into a global powerhouse. Also, it is a concrete manifestation of the pan-African drive for unity, self-determination, freedom, progress and collective prosperity¹⁷ (African Union Commission, 2015).¹⁸ The Agenda is made up of a number of goals and aspirations, which all Member States are encouraged to work toward, with the first aspiration being the key indicator of the AU’s attitude to a digital revolution for Africa. Aspiration 1 states that:

*“A prosperous Africa based on inclusive growth and sustainable development requires that Africa makes significant investments in education with the aim of developing human and social capital through an education and skills revolution emphasising innovation, science and technology.”*¹⁶

Another source is the [Digital Transformation Strategy](#) for Africa (DTSA) which argues that digital transformation is a driving force for innovative, inclusive and sustainable growth. Innovations and digitalization are stimulating job creation and contributing to addressing poverty, reducing inequality, facilitating the delivery of goods and services, and contributing to the achievement of Agenda 2063 and the SDGs.¹⁹ The DTSA’s main objective is to drive digital transformation and to build a secured digital single market in Africa by 2030 where free movement of persons, services and capital is ensured and individuals and businesses can seamlessly access and engage in online activities in line with the AfCFTA. To this end, the strategy emphasizes the need to harmonize policies, legislation and regulations and establish and improve digital networks and services with a view to strengthening intra-Africa trade, intra-investment and capital flows, and the socio-economic integration of the continent, while maintaining a relational balance with other continents in the context of networked economies.

On the other hand, the AU Data Policy Framework explicitly recognizes data as a strategic asset that is integral to policy-making, private and public sector innovation and performance management, and creation of new entrepreneurial opportunities for businesses and individuals. It thus argues that the central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives – from unleashing the economic and social potential of data to the prevention of harms associated with the mass collection and processing of personal data.

¹³ African Union Commission, ‘Agenda 2063 The Africa We Want’ (African Union Commission, 2015), <https://au.int/en/agenda2063/overview>.

¹⁴ African Union, ‘The Digital Transformation Strategy for Africa (2020 -2030)’, 2019, <https://www.tralac.org/documents/resources/african-union/3013-the-digital-transformation-strategy-for-africa-2020-2030/file.html>.

¹⁵ African Union, ‘AU Data Policy Framework’. <https://au.int/en/documents/20220728/au-data-policy-framework>

¹⁶ African Union, ‘Data policy Framework’ (2022). <https://au.int/en/documents/20220728/au-data-policy-framework>.

¹⁷ African Union Commission, ‘Agenda 2063 The Africa We Want’. <https://au.int/en/agenda2063/overview>

¹⁸ African Union Commission. <https://au.int/en/agenda2063/overview>

¹⁹ African Union, ‘The Digital Transformation Strategy for Africa (2020-2030)’, Report (Addis Ababa, Ethiopia: African Union Commission, 2020), <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.

The Framework notes that the cross-border transfer of personal and other data is becoming an increasingly important issue in the African context. However, the movement of data is often met with limitations, which, as the Framework adds, could result in the loss of business opportunities and the reduction of organizations' ability to trade internationally, leading to a reduced geographical footprint and loss of market competitiveness. With the above in mind, the intention of the Framework is made clear in the executive summary:

The purpose of this document is to provide the policy framework for African countries to maximise the benefits of a data-driven economy by creating an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation. This enabling environment refers both to the collaboration between in-country sectors, institutions and stakeholders, an alignment of their development priorities, and the harmonisation of policy across the continent in a manner that provides the scale and scope required to create globally competitive markets.

In more detail, the policy framework emphasises that building a positive data economy national and regional will require unprecedented levels of collaboration between stakeholders to disrupt the economic, political, and policy pressures already being felt from the global data economy. To this end, it encourages Member States to establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. The most promising site for a unified legal approach is the AfCFTA.

II. THE AFRICAN CONTINENTAL FREE TRADE AREA (AFCFTA)

The AfCFTA agreement is a project of Agenda 2063 which aims to create the largest free trade area in the world measured by the number of countries participating. It brings together the 55 countries of the AU and eight Regional Economic Communities (RECs) to create a single market for the continent. Despite geographic proximity, countries often have stronger trade links with former colonial powers, as well as the US and China, than with some of their neighbors. The aim of AfCFTA is to enable the free flow of goods and services across the continent and boost the trading position of Africa in the global market.²⁰ As part of its mandate, the AfCFTA seeks to eliminate trade barriers and boost intra-Africa trade. The AfCFTA entered into force on 30 May 2019, after 24 Member States deposited their Instruments of Ratification, following a series of continuous continental engagements since 2012. It was launched at the 12th Extraordinary Session of the AU Assembly of Heads of State and Government in Niamey, Niger, in July 2019. The commencement of trading under the AfCFTA was on 1 January 2021. Since the signing 44 countries have currently ratified this agreement.

The AfCFTA is being negotiated in two phases. The first phase consisted of negotiations on the Trade in Goods, Services, Dispute Settlement mechanisms, and Customs and Trade Facilitation. Phase 2, which applies more to cross-border data issues, and consists of negotiations on Intellectual Property Rights, Digital Trade, Investment, Competition Policy, and Women and Youth in Trade. The ongoing negotiations on the protocol on intellectual property (IP) rights are already showing an inclination to the liberalization of previously territorial goods (including data) with various stakeholders calling for extensive IP protection and maximizing private value so that IP rights holders benefit from the use of IP beyond their national territories. Likewise, the protocol on digital trade (still to be negotiated) is predicated

²⁰ 'African Continental Free Trade Area (AfCFTA) Legal Texts and Policy Documents - Tralac Trade Law Centre', accessed 18 January 2022, <https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html>.

on the ability of African nations to generate and consume digital goods, thus moving away from the notion that Africa as a continent is largely a consumer of digital goods. The protocol presents the opportunity to develop a framework that takes into account best practices in digital trade such as eliminating data localization requirements and enabling free cross-border data flows. A recent study²¹ on the possibility of regulating cross-border data flow under the AfCFTA protocol arrived at the same conclusion as this Report. African countries have different capacities and resources. Therefore, a protocol would have to include provisions for countries that are not able to immediately comply with all of the requirements for a trustworthy and technologically effective cross-border data sharing regime. The protocol could contain provisions that enable benefits of sharing in accordance with the extent to which a country is able to offer trustworthy and mutually beneficial data sharing. Although the study does not refer to the Data Policy Framework, it converges with it by suggesting that cross-border data sharing of personal data should be premised on reciprocal protection of the data from other African countries.

While the AfCFTA is still being negotiated there are important existing treaties and instruments that regulate one or another aspect of data. While these are incomplete and do not create a coherent scheme they must nevertheless be taken into account in determining data policy and consequent regulation.

III. DATA PROTECTION AND PRIVACY

The primary goal of data protection is to safeguard data subjects' personal information. In this sense it can also be said to pursue a privacy interest. This is mostly accomplished through outlining the rights of persons over their data, assigning responsibility over data, and establishing rules for how organizations and the government should handle and preserve 'personal data'. In light of this, there is a possibility that data transfers across borders could be slowed significantly since, in essence, data protection places a higher level of scrutiny on how data are gathered, processed and stored. In most cases across, wherever personal data is exchanged across the globe the prevailing requirements are that such data should be lawfully obtained (usually through freely given consent) for a specific purpose, and not be used for unauthorized activity such as profiling or surveillance by governments or any other third parties or used for different purposes without consent (unless otherwise required under the law) ([World Bank](#)). In addition, it is generally agreed that users should have certain rights over data about them, including the capability to procure their own data and to correct incorrect data about them, and to have the necessary arrangements available in order to remedy rights violations or secure these rights.

Most concerted efforts in the realm of data regulation in the continent have taken the face of data protection with the chief aim being to observe and safeguard internet users' privacy rights. Currently, the continent is confronted by multiple and unconcerted attempts at data protection. It is estimated that 33 of Africa's 55 countries have enacted or embraced some form of regulation, with the chief aim of protecting personal data.²² Regionally, legislative tools such as the 2008 East African Community Framework for Cyberlaws, the [2010 Supplementary Act](#) on Personal Data Protection of the Economic Community of West African States (ECOWAS), and the 2013 Southern African Development Community (SADC) [model law](#) harmonizing policies for the ICT market in sub-Saharan Africa, have been developed. Continentally, the AU developed the first pan-African framework with the African Union Convention on Cyber Security and Personal Data Protection ([Malabo Convention](#)) in 2014 which has not come into effect yet as the required number of ratifications has not been reached.

²¹ Alexander Beyleveld and Franziska Sucker, 'Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade' (Centre for the Study of the Economies of Africa, October 2022), <https://cseaafrica.org/cross-border-data-flows-in-africa-policy-considerations-for-the-afcfta-protocol-on-digital-trade/>.

²² 'Data Protection and Privacy Legislation Worldwide', UNCTAD, accessed 17 October 2022, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

Many data authorities in francophone African countries are members of [L'Association francophone des autorités de protection des données personnelles](#) (AFAPDP) an association of francophone data authorities that seeks to promote the protection of personal data, strengthen the capacities of its members and engage on data policy internationally. African members include Senegal, Mali, Niger, Morocco, Gabon, Mauritius, Tunisia, Côte d'Ivoire, but also lusophone São Tomé and Príncipe.

a. THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (MALABO CONVENTION)

The Malabo Convention was adopted in July 2014. The Convention presented the first steps toward creating a legislative framework for cyber security and data protection in the African region. It addresses three main areas that have previously not been regulated or inadequately regulated by the governments in the region. These are:

- electronic transactions; personal data protection, cyber security and cybercrime;

The Convention emphasizes the importance of adhering to national constitutions and international human rights law, with a particular emphasis on the African Charter on Human and Peoples' Rights.²³ It sets out the substantive principles with which data controllers must comply, and the rights of data subjects. The 'Basic Principles' include the requirement that the processing of data is based on consent (with specified exceptions); be lawful, fair and, for specific purposes (that the processor may not deviate from, and where necessary), that the collection be limited to data, "adequate, relevant and not excessive" for those purposes and generally retained for no longer than necessary for them; and that controllers and processors take reasonable steps toward making the data accurate and up-to-date; processing it transparently; and is keeping it with security and confidentiality.

A deeper look at the Convention reveals that its principles, its enforcement and other procedures are significantly influenced by the European approaches. The laws are dogmatic, with a moderately high level of administrative requirements. The level of detail of the data protection aspects of the Convention are such that an African country could extract them as the basis for national legislation, requiring only a modest amount of detail to be added. While the Convention's provisions are almost a 'model act', the extent to which they are consistent with sub-regional developments in Africa, particularly the ECOWAS Supplementary Act and the use of the SADC Data Protection Model Law, needs consideration.

b. THE 2010 SUPPLEMENTARY ACT ON PERSONAL DATA PROTECTION OF THE ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS)

The Supplementary Act on Personal Data Protection within ECOWAS (2010), which is a supplement to the ECOWAS Treaty, determines the content required of a data privacy law in each ECOWAS Member State, including the establishment of a data protection authority. The main aims of the ECOWAS Supplementary Act are the protection of privacy and promotion of free movement of information. These aims are found in recitals 10 and 11 of the preamble to the Act, rather than

²³ The Convention, which is heavily influenced by the EU's General Data Protection Regulation (GDPR) defines 'personal data' in terms of the direct or indirect identifiability of a person. It defines 'processing' in broad terms, and offers a definition of a 'data controller.' Its scope extends to both the public and private sectors, including automated and non-automated processing.

in its text. The Supplementary Act applies to any processing of personal data carried out in an Unión Económica y Monetaria de África Occidental (UEMOA) or ECOWAS Member State and does not apply to data processing carried out by an individual while engaged in his/her personal or domestic activities. The basic principles of data processing in the Supplementary Act are covered in Chapter V and these include:

- consent and legitimacy (Art 23);
- legality and fairness (Art 24);
- purpose, relevance and preservation (Art 25);
- accuracy (Art 26);
- transparency (Art 27);
- confidentiality and security (Art 28);
- choice of data processor (Art 29).

Chapter VI of the Supplementary Act outlines the rights of the individual whose personal data are subject to processing: the right to information, right of access, right to object, and right to rectification and destruction. It also contains provisions (Arts 42 to 45) on obligations of the data controller: confidentiality, security, preservation and durability. Of great importance in the outcomes of this policy is Article 36 of the Act which deals with the international transfer of personal data to non-ECOWAS Member States. It posits that such transfers are only possible where such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data. There is also the requirement that data controllers should inform the data protection authority prior to any transfer of personal data to a third country.

c. CYBERLAW AND CYBERCRIME LAW

Cybercrime laws give authorities the ability to prosecute people who commit a variety of crimes online. Depending on the nation, legal framework, and context in which the term is used, cybercrime may have several definitions. However, generally speaking, a nation should have laws in place that address criminal conduct aimed at the privacy, integrity, and availability of computer systems and networks, or the data stored and processed on them, as well as criminal acts committed using such systems, networks, and data as a tool. The World Bank Toolkit on Combating Cybercrime served as the source for this expansive definition of cybercrime.²⁴

Typically, and within the context of data regulation and governance, a cybercrime law will prescribe the unauthorized access, use or alteration to personal data or ID systems, including the criminalization of:

- unlawful access to ID systems or other databases that hold personal data;
- the unlawful monitoring/surveillance of ID systems or other databases holding personal data, or unauthorized use of personal data;
- the unauthorized alteration of data collected or stored as part of ID systems or other databases holding personal data;
- the unlawful interference with ID systems or other databases holding personal data;

In Africa, at the moment, the Malabo Convention is of paramount importance in this context. It speaks to the powers

²⁴ World Bank and United Nations, 'Combating Cybercrime: Tools and Capacity Building for Emerging Economies', Handbook (Washington, DC: World Bank, August 2017), <https://doi.org/10.1596/30306>.

of law enforcement in respect of cybercrime and adds that such powers must be prescribed by law, pursue legitimate aims, be necessary and proportionate, allow for effective remedies and be subject to guarantees against abuse. The Malabo Convention reflects a strong commitment by the AU Member States to establish a secure and trusted foundation for the information society. It covers a broad range of measures ranging from electronic transactions to the protection of personal data, cyber security and also cybercrime.

i. The 2008 East African Community Framework for Cyberlaw

The East African Community (EAC) adopted the EAC Framework for Cyberlaws Phases I and II in 2008 and 2011 respectively, addressing multiple cyber law issues including data protection. Phase I makes very brief data protection recommendations and, in general terms, merely encourages the adoption of international best practice. Phase I addresses the following issues:

- electronic transactions;
- electronic signatures and authentications;
- data protection and privacy;
- consumer protection and computer crime.

The second phase addresses mainly IP, domain names, taxation and freedom of information. The Framework has been criticised for not providing any minimum standards for its members to adhere to despite mentioning and recommending the adoption of international best practice. In the travaux préparatoires of the Framework, two minimum obligations were recommended with regards to the processing of data. The first required compliance with certain ‘principles of good practice’ in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security. The second recommended that an individual be furnished a copy of any personal data being held and processed and provided an opportunity for incorrect data to be amended. This has been worked into recommendation 19 of the Framework. The Framework, by failing to attach any annex of international code on data privacy – as has been done with other areas such as electronic transactions and electronic signatures – leaves a lot of ambiguity on the subject matter. The effectiveness of the Framework is yet to be determined.

ii. The 2013 Southern African Development Community Model Law Harmonizing Policies For The ICT Market In Sub-Saharan Africa

The SADC Data Protection Model Law 2013 speaks to the protection of an individual’s right to privacy and encourages the harmonization of data privacy policies and laws in the region. The scope of the Model Law applies to both automatic and non-automatic processing of personal data and covers both private and public data controllers. The core of the Model Law lies in parts IV, V, VI and VII which contain basic principles and conditions for processing personal data. These principles include:

- fair and lawful processing (Art 12(1));
- explicit purpose (13(1));
- legitimacy (Art 14);
- sensitivity (Art 15);
- data quality (Art 11);
- security (Art 24);
- openness (Art 29);

- accountability (Art 30).

Part VI of the Model Law contains the obligations imposed on data controllers such as the provision of information prior to processing; confidentiality; security; notification of the processing to the data protection authority; and accountability. The Model Law also speaks to the rights of the data subject in its part VII and mentions the right of access; right of rectification, deletion, temporary limitation of access; right of objection; and representation of the data subject who is underage. It also contains rules which prohibit transfer of personal data, not only to a non-SADC member but also to a SADC member state, which has not adopted the Model Law.

IV. INTELLECTUAL PROPERTY LAW

Information or raw data as we know it is not covered by any recognized property right, regardless of how valuable or private it may be. However, organizations with substantial IP portfolios have successfully stopped access by others to datasets gathered by the organization or through their own IP-protected data collection tools, thereby disrupting data flows. Some businesses have resorted to applying some contract law principles in situations where IP law falls short. Assigning control is crucial for cross-border data flow. This must take place in a legally cognizable way that is not reliant on IP since IP law, in particular, has established itself as the ‘weighted’ argument for ‘data ownership’.

a. COPYRIGHT LAW

In terms of Copyright law, the [Berne Convention](#) for the Protection of Literary and Artistic Works serves as an unofficial ‘umbrella law’ in so far as it concerns what is required for copyright protection to be granted albeit without any real formalities. To date 181 states are members of the Berne Convention and the majority of African states are contracting parties to the Convention. Since most data do not come within the scope of what is considered original, the primary condition for copyright protection –originality –often undermines the case for data protection. Since most data are factual in nature, copyright regulations do not apply to it. However, databases have occasionally been protected under modern incarnations of copyright law. For example, in jurisdictions such as South Africa, the Copyright Act recognizes the protection of tables and compilations, including compilations of data that are stored in a computer system or data that are used in conjunction with a computer.²⁵ However these must be the result of human skill and effort, and in some jurisdictions require at least a modicum of creativity. This puts in doubt copyright over databases assembled through automated processes. The emphasized lesson was that it is possible to have rights to a database (including the data contained within these databases) even if it is merely a compilation of publicly available information, but only if certain criteria are met.

This presents a dilemma and sows uncertainty. It seems the position as it stands is that:

- If data falls within any of the protected categories found in copyright law and meets the threshold requirements including human authorship, then it may be under copyright.;

²⁵ The extent of protection was confirmed in the South African case of National Soccer league v Gidani, wherein it was stated that compilations of data are indeed protected and that the requirement of originality was of little consequence where sufficient effort in compiling a work would be applied. Later on, the South African case of the Board of Healthcare Funders v Discovery Health Medical Scheme answered the question surrounding the ownership of individual data within databases and added that because databases are capable of protection in whole, then so should the contents of the database be protected as far as they relate to that particular database. More recently however, the South African case of Discovery Ltd and Others v Liberty Group Ltd introduced a new dimension to the question of data ownership that may belong in databases. The judgment to the case was instrumental in affirming that in instances where we are faced with personal data, the data subject (natural and legal person) and not the data collector or aggregator owns their personal data.

- Databases are capable of protection, at least if some degree of human skill, effort and creativity are employed in compiling them.
- However, under competition law, and common law regulation of competitive practices, data within databases, if personal in nature, will be owned by the data subject and competitors may not exclude others from accessing this information, at least with data subject consent.

b. SUI GENERIS DATABASE PROTECTION OF NON-ORIGINAL DATABASES

On the other hand, there is sui generis database protection of non-original databases that is confined to the European Union (EU). Sui Generis protection is focused mostly on the protection of the data within a database as a whole. The TRIPS agreement and the World Intellectual Property Organization (WIPO) Copyright Treaty do not impose any obligation on African countries to grant copyright rights over non-original databases. However, countries could choose to do so. However, should they do so, those rights will not extend beyond their borders, thus granting rights to the nationals of other countries that are not afforded to their own nationals in those other countries. WIPO, despite a lack of international instrument backing protection, claims that it is important to recognize that databases are worthy of protection for purposes of developing information infrastructures at a global scale while ensuring that users are guaranteed appropriate access.²⁶ Despite the EU introducing the idea of protecting non-original databases at WIPO's diplomatic conference, the matter has not been pursued further by WIPO. As a result, only the EU at the moment, recognizes the sui generis protection of non-original databases.

c. PATENT LAW

Patents have also been used to claim ownership of data. A patent is an exclusive right that is granted for an invention but not for a discovery. Most countries that are parties to the [Paris Convention](#) for the Protection of Industrial Property and the WIPO [Patent Cooperation](#) Treaty agree that in order for an invention to be worthy of patent protection, it must be new, have an inventive step, and be capable of being used in trade, industry or agriculture. However, since data by its very nature will not satisfy the criteria for innovation in this particular case, there is little likelihood of patent protection. The extent of the patentee's rights, insofar as they apply to a patented innovation that may deal with the gathering, aggregation, or distribution of data, is what we are particularly concerned with. In other words, how much of the patented invention – as well as any potential data the patented invention may produce or collect – is protected by the patent. In many cases, patent protection gives the patent holder the sole right to prevent others from producing, using, trading, importing, disposing of, or offering to dispose of the invention, so that only the patent holder will have the sole right to profit from the invention and receive any other benefits for as long as the patent is in effect.

Therefore, when a company is actively engaged in producing gadgets that collect and store data, patent law is frequently

²⁶ In distinguishing between database protection through copyright and sui generis protection, the European Court of Justice (ECJ) in *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others* elucidated the purpose of the database directive, which was to “stimulate the creation of data storage and processing systems in order to contribute to the development of an information market ... and not to protect the creation of materials capable of being collected in a database”. The ECJ held in the *Football Dataco* case that a sui generis right is granted only if there is a sizable investment in obtaining, verifying, or presenting the contents of the database. This effectively excludes machine-generated databases and big data which use technologies that have automated these processes.

²⁷ For the past 27 years, the company IBM has consecutively filed and held the most patents in the United States. At the end of 2019, IBM had a total 9 262 patents filed, with Samsung Electronics a distant second with 6 469 patents. If these figures are anything to go by, this means that ultimately, the device' industry is, has been and will continue to be dominated by large corporations who have huge IP portfolios. If the reasoning that data ownership is facilitated by patent protection, we run the risk of again enabling exclusion in the data economy based on the power of pre-existing IP portfolios. In this light, data originating from the devices that transmit data across various 4G and 5G networks may be used to the exclusion of others because of patent rights or they may try to obtain licensing fees from interested parties who may be trying to access data that is exchanged within the device system or stored in the cloud connected to the specific device that they produce. And while it has been established that as a general rule data are incapable of being owned, the firms providing the collection mechanisms or other devices have managed to obtain IP rights to these data sets.

invoked. It is thus asserted that ownership of data is an extension of the patent right, and that as the patent holder of a particular device that gathers or analyzes data, ownership of the data contained within must also belong to the patentee.²⁷ However these claims have not been validated in courts. Countries are free under international law to explicitly exclude extension of patent protection to data generated by an invention.

d. TRADE SECRET PROTECTION

Another justification for data exclusion has been through the use of trade secret protection mechanisms. Trade secrets are described as information that is communicated in secret within a business enterprise and that has some commercial value. This means that the information must be communicated only to a select few, and to the exclusion of others, because it is of high importance and commercially valuable. In addition, there must be efforts to keep the communication secret such as contractual prohibitions on disclosure. In the field of data, it is easy to see why this form of legal control would be claimed by many firms. The purpose of trade secret protection is not necessarily to establish a new IP right or to encourage secrecy. Instead, it safeguards trade secrets against unfair misappropriation. Article 39 of the TRIPS Agreement requires members to offer protection of undisclosed information against unfair competition. TRIPS is binding on World Trade Organization members. Forty-four African states are members although many of these are Least Developed Countries that do not yet need to implement all the provisions of TRIPS. There has not been much development made in terms of trade secrets and data, but it has been established in countries like South Africa that any material, which is already publicly available, cannot be deemed proprietary information. Additionally, the protection of trade secrets is only given in cases of competition that is against ethical business standards. That is frequently not the case with data that is factual in nature or that is not unique.

An individual datum may not be considered a trade secret, but aggregated data or meta-data that is communicated in secret and so not accessible to the general public, and that has commercial value, might be. To put this in perspective, it should be noted that data owners rarely disclose their data collection methods or the conclusions they draw from the data. Therefore, a company that has the ability to withhold such crucial information is in a position of power and may make it more difficult for smaller companies to share, access, reuse, and redistribute the data for their own benefit. If and when trade secret protection is used, it is necessary to clarify these opaque limits.

V. COMPETITION LAW

Competition law (also known as anti-trust law or anti-monopoly law in various other jurisdictions) is a regulatory regime that seeks to maintain equitable market competition and efficiency through the regulation of anti-competitive conduct by companies. Competition law finds application in and influences the shape of other types of data regulation such as sui generis database protection and privacy and data protection. The key issue is the relationship between competition law and consumer data. Consumer data are increasingly relevant to competition assessments. This can manifest in two key ways:

- a) privacy and data protection might be an aspect of quality on which businesses may compete;
- b) the collection and ownership of consumer data, and access to that information, might impact competition. The potential harms that present themselves if left unregulated include mergers and acquisitions, abuse of dominance and cartel cases.

Currently, a number of policies and treaties exist in the African continent which speak directly to the manner in which competition ought to be regulated, albeit in a more general sense and not specific to data. Most of these have been formulated and enforced within established RECs. Examples of these RECs and their governing laws include:

- The Common Market for Eastern and Southern Africa (COMESA)
 - The 2004 COMESA Competition Regulations and Competition Rules
 - The EAC Competition Act (2006)
 - The EAC Common Market Protocol and the Protocol on the Establishment of an EAC Customs Union;
- Economic Community of West African States (ECOWAS)
 - The ECOWAS Supplementary Act on the Adoption of Community Competition Rules and the modalities of their application within ECOWAS
- West African Economic and Monetary Union (WAEMU)
 - The WAEMU Treaty, Regulation No. 2/2002/CM/UEMOA of 23 May 2002 on anti-competitive practices within the WAEMU;
- Southern African Customs Union (SACU)
 - The 2002 Southern African Customs Union (SACU) Agreement;
- Southern African Development Community (SADC)
 - The SADC Protocol on Trade (2006)
 - SADC Declaration on Regional Cooperation in Competition and Consumer Policies (2009);
- Central African Economic and Monetary Community (CEMAC)
 - The Treaty Establishing the Economic Community of Central African States
 - CEMAC Regulation No. 1/99/UEAC-CM-639 of 25 June 1999 on Abuse of Dominance and Monopoly Economic Community of Central African States (ECCAS)
 - The Treaty Establishing the Economic Community of Central African States (1992);

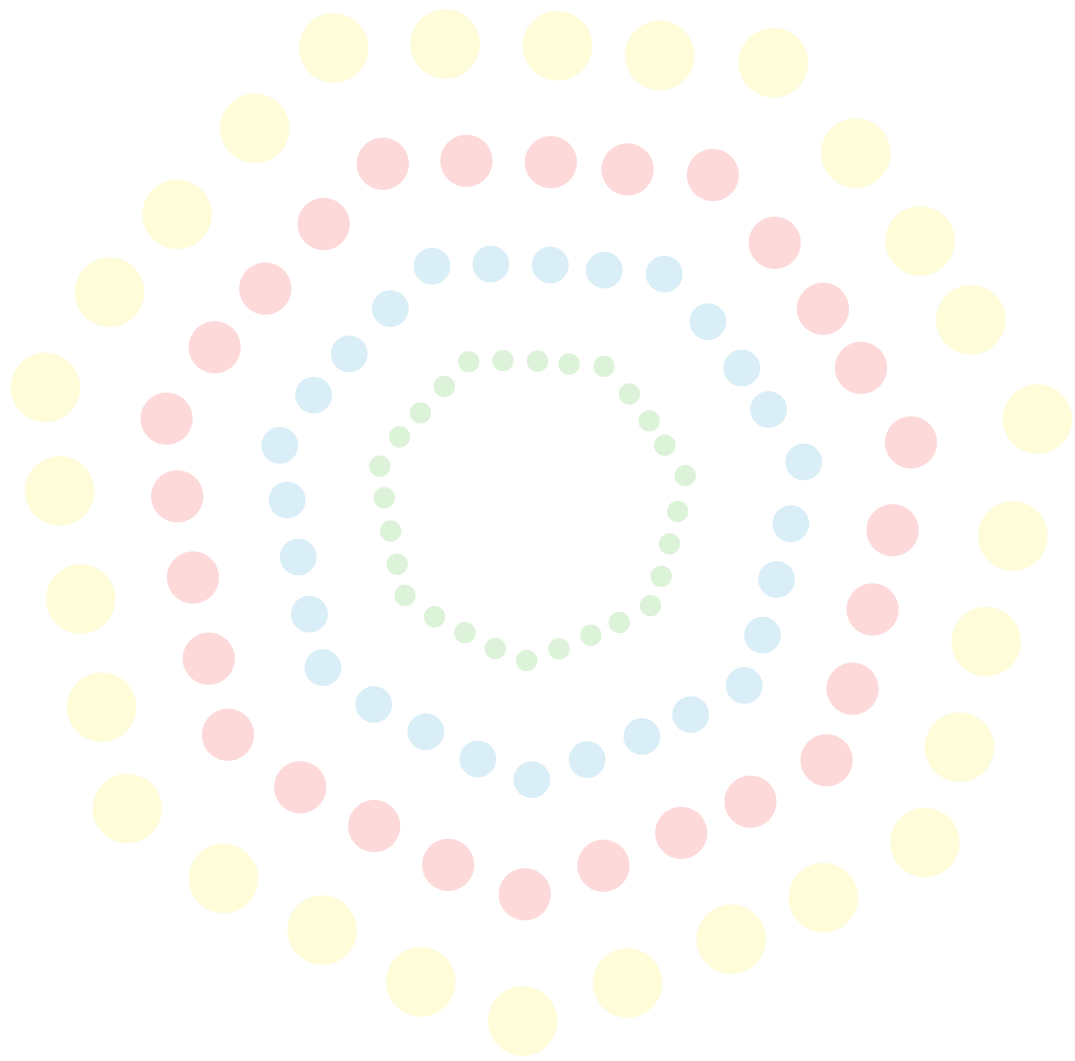
Harmonizing competition rules is becoming more and more crucial, especially in light of the data era. For instance, mergers involving companies that utilize customer data may impair competition in two ways:

a) by lowering the standard of data security and privacy services offered in the relevant market; or

b) by combining consumer data to raise expenses for competitors or raise entry barriers.

Additionally, there is a chance for an exclusionary abuse of power when it is not controlled or monitored. In such a case, a dominating company practices exclusionary behavior to deny rivals access to customer data. As an alternative, a dominant company that has exclusive access to consumer data may use tying or bundling to increase the prices or entry barriers for competitors. Abuse of power is a major danger to the equitable distribution and use of data in a continent as unequal as Africa and with little existing infrastructure.

From the above analysis, and in the absence of one umbrella data policy framework that takes into account all legal avenues that may be concerned with data, the existence of divergent regulatory approaches may result in disproportionate levels of protection between jurisdictions and unnecessary restrictions on the cross-border movement of data. There is increasing need to establish legal controls over the collection, processing, and movement of data in addition to the necessity for data to be a legal certainty. This should be done while keeping in mind all relevant data regulation and keeping in mind that if data protection requirements are overly strict, they may have a negative influence on the goals of this policy intervention.



2. TOPICAL TRENDS IN AFRICA

One of the most viable means of maximizing Africa's digital economy is by ensuring strong and effective cross-border digital policies. This is due to the fact that today, commercial activities need to thrive beyond borders and data as the lifeblood of any digital economy is of little value when it is inert i.e. data as a resource cannot self-actualize. Rather it needs to be acted on to generate real value. The real value of data is often realized when it flows freely to generate new insights. However, such free flow of data, especially across African borders requires consideration of key digital policy trends. These considerations are necessary because as data flows, so do risks and obligations that require common standards especially in Africa. Therefore, this chapter documents overarching and topical cross-border digital policy trends. Two major issues that emerged from the conversations held are the need for coordination and harmonization on digital policy and external influence on African data policy. Part I of this chapter focuses on African trends around trusted environments, data governance and internet shutdowns. It is followed by Part II, which borders on e-commerce and inclusive economies (digital trade, competition, taxation). Part III briefly highlights the infrastructure challenges and brings attention to the status of some of the foundational infrastructure for the digital and data economy such as digital identity and data centers.

I. TRUSTED ENVIRONMENTS

a. INTERNET SHUTDOWNS

Recent years have seen the 'increasing scope and scale of Internet shutdowns' across the world³¹ ([Marchant and Stremiau 2020, 4216](#)). Despite the United Nations Human Rights Council having [condemned](#) actions to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, especially "... when this act of censorship takes place during an election period, a critical moment in democratic life", Information Security Operations Center (ISOC) recorded 49 government-mandated shutdowns in the 2019, with a significant number of these in Africa.³²

There were 25 cases of Internet shutdowns in Africa recorded in 2019, a rise from 20 in 2018 and 12 in 2017. There were major Internet shutdowns in at least five African countries since the start of the pandemic, mostly around elections, usually in the name of protecting national security. Many countries having put in place misinformation regulations or simply unrestrained emergency powers that enabled governments to do so to fight against the spread of fake news and hate speech. Intermittent and extended Internet shutdowns have occurred in Chad, Sudan, Gabon and Zimbabwe. Ethiopia has had at least seven internet shutdowns during the pandemic and as the Tigrayan conflict has escalated. Internet shutdowns are blunt instruments used by governments to both censor political expression and disrupt coordination activities among the citizenry.

²⁹ UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *Digital Economy Report 2021: Cross-Border Data Flows and Development*. (S.I.: UNITED NATIONS, 2021), <https://unctad.org/webflyer/digital-economy-report-2021>.

³⁰ African Union, 'AU Data Policy Framework'. <https://au.int/en/documents/20220728/au-data-policy-framework>

³¹ Eleanor Marchant and Nicole Stremiau, 'Internet Shutdowns in Africa | The Changing Landscape of Internet Shutdowns in Africa — Introduction', *International Journal of Communication* 14, no. 0 (13 August 2020): 8.

³² While there are more Internet shutdowns and interruptions recorded in Africa's 54 countries than in other regions, the country with the most single reported shutdowns is the world's largest democracy, India. With over 550 internet suspensions in various states over the past decade, more the half have occurred since 2019, with shutdowns in Kashmir lasting for more than a year and a half.

<https://indianexpress.com/article/technology/tech-news-technology/india-ranks-highest-in-internet-suspensions-7654773/#:~:text=India%20leads%20the%20global%20tally,instances%20of%20shutdowns%20being%20enforced.>

The African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression and Access to Information in Africa³³ has expressed grave concern about the growing trend of Internet shutdowns. The Rapporteur also characterizes shutdowns as a violation of the right to freedom of expression and more broadly contrary to Article 9 of the African Charter on Human and Peoples' Rights.

Subsequently, there were major Internet shutdowns in at least five African countries since the start of the pandemic, mostly around elections, usually in the name of "protecting national security". But with many countries having put in place misinformation regulations or simply unrestrained emergency powers that enabled governments to do so to "fight against the spread of fake news and hate speech" dissent has been limited to an extent. Uganda shutdown the Internet for five days at the height of the pandemic and during the 2021 elections. Ostensibly the shutdown was in retaliation to Facebook's takedown notifications on Government websites.³⁴ In Africa's most populated country Nigeria, the government banned Twitter after it deleted a tweet by President Muhammadu Buhari which warned separatists against causing by the civil war in Nigeria.³⁵

Circumstances vary, but some commonalities of Internet shutdowns in Africa are identifiable, including the targeting of social media platforms during demonstrations for reform and shutdowns occurring in the run up to elections or during polling and during military coups.³⁶ Generally African Internet shutdowns are done in an ad-hoc manner with weak legal reasoning³⁷ (De Gregorio and Stremlau 2020). There have been some judicial checks of executive breaches. For example, in January 2019, the Zimbabwean High Court in Harare ruled that Internet shutdowns were unconstitutional. More research is required on why private telecommunications operators comply with government orders on shutdowns. Mare's 2020 study on Zimbabwe's setting aside any potential elective affinities among shareholders, managers and state officials³⁸ draws attention to the way that telecommunications operators juggle an array of pressures, including telecommunications regulatory authorities that are staffed by officials purposefully deployed by hegemonic interests.

As a tactic of last resort, there is some indication that in the medium term government's ordered Internet shutdowns may backfire. The limited research on the subject in Africa suggests that this tactic is not very effective in limiting protest movements. Moreover, shutdowns may in fact help galvanize new groups to join the protests especially when dissenters have built parallel organization tools in anticipation of a shutdown (Rydzak, Karanja and Opiyo 2020). Researchers are also increasingly discussing 'slow shutdowns' (Parks and Thompson 2020), where, over the course of a decade the steady passage of restrictive laws combined with an under-investment into technical infrastructure and general resource starvation of institutions results in a practical shutdown. Tanzania from 2010 to 2018 is one such example. Compounding these issues is how dissent is being criminalized through cyber-crime legislation, as is also the case in Tanzania (Cross 2021).

³³ 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (The African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression and Access to Information in Africa, 2019), <https://www.achpr.org/presspublic/publication?id=80>.

³⁴ <https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effect>

³⁵ <https://www.rfi.fr/en/africa/20220113-free-as-a-bird-nigeria-ends-twitter-ban-after-seven-months>

³⁶ Access Now, 'The return of digital authoritarianism: internet shutdowns in 2021'. <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>

³⁷ Giovanni De Gregorio and Nicole Stremlau, 'Internet Shutdowns in Africa | Internet Shutdowns and the Limits of Law', *International Journal of Communication* 14, no. 0 (13 August 2020): 20.

³⁸ Admire Mare, 'Internet Shutdowns in Africa | State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe', *International Journal of Communication* 14, no. 0 (13 August 2020): 20. <https://ijoc.org/index.php/ijoc/article/view/11494>

b. DISINFORMATION

As new technologies come to market it seems that shutdowns may be replaced with more sophisticated ways to curtail the digital dissemination of information³⁹ ([Marchant and Stremlau 2020](#)). The effects of social media trolls—both paid and unpaid—and bots to hound dissidents, which distort the discourse, and create more information than can be parsed by the public, can cumulatively disempower activists and opponents. Seemingly the goal is to use disinformation practices to dilute the quality of information, and attempt to redirect the attention of citizens. Due to the lack of resources for civil society actors, states have greater incentives, with which to intervene.

African countries and institutions have had a long history of attending to the causes and consequences of disinformation, being issues that were most acute during the AIDS crisis in the 1980s ([Konotey-Ahulu 1987](#)). This policy experience can be leveraged by policy-makers and advocates to address digitally mediated disinformation, even if topics have changed. In contrast to fake news (see below), the problem of disinformation in African domestic politics is somewhat similar to experiences in American and European domestic politics, insofar that it is anchored on nationalist sentiments with disinformation practices themselves appearing too closely connected to electioneering (see [Nkabane and Mutereko 2021](#)). For example, an active disinformation operation using Twitter bots was discovered to be active during the 2019 South African election ([Baldassaro 2019](#)). Furthermore there are forms of extreme speech and incitement around racism, religion, misogyny, and xenophobia, and that groups purposefully use social media to amplify (see [Chenzi 2020](#)). There is some evidence that when using their closed networks transnational African elites do attempt to intervene so as to curtail the spread of disinformation ([Timcke 2022](#)), but there is less knowledge about the size of the effect of these interventions.

As platform companies give fewer resources to content moderation in African markets, ‘African countries appear to have shifted their focus towards state-centric approaches to regulating content’ ([Garbe, Selvik, and Lemaire 2021](#)). The result is that the character of disinformation practices becomes ‘regime-specific’ ([Garbe, Selvik, and Lemaire 2021](#)). With the unevenness of African countries ‘coming online’, some of the continent’s political contests are not fully digitally mediated and so maintain some traditional characteristics. At the same time, the lack of dedicated African research teams does mean that disinformation operations are harder to detect, while their scope and scale have yet to be regularly tracked. Debates about the character of disinformation in the African continent are complicated by long standing Global North agencies’ due criticism of news media coverage of African politics ([Hawk 2002](#)). The absence of local and international press coverage does give a distorted picture of what is occurring, as well as the consequences for external efforts to support local democratization projects.

Paralleling the first Russia-Africa Summit in Sochi 2019 Russia’s renewed diplomatic bilateral relations with African countries has been labeled as a disinformation project ([Akinola and Ogunnubi 2021](#)). This term has stuck, even if terms like corruption may be more suited for opening up markets for armaments, security provision, as well as access to minerals and energy ([Neethling 2019](#)). But much more research is required to reach more secure conclusions about the nature of these projects, the effectiveness of any detectable disinformation efforts, and what the wider consequences are for the societies in which these projects are in operation.

Together with the concept of ‘fake news’ disinformation can be understood as ‘information disorder’. The resources available to address disinformation disorder in Africa exhibit the same inequalities as the other aspects of digital globalization ([Wasserman et al, 2022](#)).

³⁹ Marchant and Stremlau, ‘Internet Shutdowns in Africa| The Changing Landscape of Internet Shutdowns in Africa — Introduction’. <https://ijoc.org/index.php/ijoc/article/view/11490/3182>

c. FAKE NEWS

In the European or American context, fake news is perceived as a social problem with significant political weight as it sways the opinion of populations, thereby reinforcing polarization and causing dysfunction across a whole range of issues. For this reason persons actively and knowingly promoting fake news are deemed deviant, and subsequently the cause of moral indignation and anxiety for institutional actors. The result is a media environment in which trust deteriorates giving way to growing frustration with the sheer technical and social task to curb extreme speech and incitement online, while platform companies themselves seem reluctant to directly address these issues lest they be perceived to be ‘choosing a side’. By contrast, as a general rule fake news does not have this weight in African countries, at least right now. Studies on Kenya, Nigeria, and South Africa show that people living in these countries frequently encounter misinformation and fake news ([Wasserman and Madrid-Morales 2018](#)), especially on platforms like WhatsApp ([Madrid-Morales et al 2021](#)). However, a study on fears of disinformation and associated risks drawing upon 154,195 respondents from 142 countries found that African respondents tended to worry much less about disinformation, fraud and harassment online than their counterparts did in other regions ([Knuutila, Neudert, Howard 2020](#)). With less than a fifth of respondents giving these issues much worry, African ‘people rarely perceive technology-related risks as being worrisome’ ([Knuutila, Neudert, Howard 2020, 3](#)). By contrast, around 60% of Americans and 45% of Europeans fear these developments. So while the fake news phenomenon is not exclusive to the Global North, in Africa it is closer to the ‘light-hearted approach to politics and everyday life’ ([Wasserman 2017](#)). If anything, larger issues of media trust are led by demographic considerations. Audience research in South Africa, for example, finds out that youth do not doubt the general truthfulness of commercial or community news ([Wasserman 2017](#)). Rather, they believe the topics do not align with the events and forces that shape their lives. While their interest in news and politics remains high, youth do choose to disengage from existing sources ([Van Gyampo and Anyidoho 2019](#)).

The expression of fake news works in concert with tastes of local audiences, much like the use of clickbait journalistic practices in the continent ([Wanda et al 2021](#)). Along another dimension, African mediascapes are tied to global internet culture through the African diaspora or participating in social media communities ([Royston 2014](#)). Due to these kinds of connections fake news produced in the Global North to sway Global North audiences may be, and often is, circulated by networks in the continent. Even so, the circulation of fake news images, for instance, does not signify that the meaning or message is the same: different backgrounds and local circumstances purport different audience understandings.

There is value in appreciating how the phenomenon of ‘fake news’ in local African countries’ specific contexts emerges from their dynamics of cultural production, circulation, and consumption ([Wasserman 2017](#)), which themselves are informed by social forces, some centuries in influence. Another consideration is how African journalists are invested in amplifying discussions about the impending harms of fake news, in part because they have a direct interest in protecting their vocation, professional standing and credibility ([Wasserman 2017](#)). Journalists are keen to use the label of ‘fake news’ to discredit emerging entrepreneurial competitors who are experimenting with models that might be called community or alternative digital media in the Global North ([Grätz 2013](#)).

Related to professional journalist practice, during the coronavirus pandemic, a study on notable fact checking organizations in Southern Africa found that these organizations believed that they did a good job of curtailing fake news and disinformation ([Mare and Munoriyarwa 2022](#)). At best the interventions were a partial success due to the sheer volume of information as well as the algorithmic promotion of content on platforms rewarding ‘engaging’ material, regardless of its truthfulness (see [Timcke 2021](#)). Given these structural elements, fact checking organizations have limited scope to ‘frame information’. Indeed, fact checkers compete with a ‘number of actors including the state, the Church, civil society and the public, all fighting for legitimacy’ (Ogoal 2020).

Governments have used fake news to imprison critics, with authorities using the label to discredit opponents for mainstream investigative reporting. They frame reports as biased regardless of the evidence included. But this does not stand up to scrutiny. For example, in 2018, Economic Community of West African States (ECOWAS) Regional Court of Justice ruled that The Gambia's laws on sedition, false news and criminal defamation violate the right to freedom of expression ([Amnesty 2018](#)). Contravention of these laws had been used by state intelligence officers as a pretext to torture journalists. Much like how, prior to 2016, fake news did not have pejorative connotations in the Global North, that same understanding applies to Africa at the moment. In a fairly neutral fashion, the term encompasses genres like satire which are deployed to lampoon the powerful by the powerless as a proverbial weapon of the weak (see [Scott 1985](#)). These tactics are deemed useful in contexts where internet shutdowns are more common than desirable (see below).

Addressing these state politics to curtail dissent, in 2017 the African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression and Access to Information co-signed the [Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda](#) issued by the UN Special Rapporteur for Freedom of Opinion and Expression, and supported by the OSCE's Representative on Freedom of the Media, the Organization of American States' Special Rapporteur on Freedom of Expression. In part the statement reads:

"[We are] Alarmed at instances in which public authorities denigrate, intimidate and threaten the media, including by stating that the media is "the opposition" or is "lying" and has a hidden political agenda, which increases the risk of threats and violence against journalists, undermines public trust and confidence in journalism as a public watchdog, and may mislead the public by blurring the lines between disinformation and media products containing independently verifiable facts."

Legal regulation of information disorder often relies on laws intended to serve other purposes such as press regulation or cybercrime ([Wasserman et al, 2022](#)): "Many laws are unclear on how to determine what is considered a "false rumor" or "false news," or what the threshold is for deciding that information is likely to alarm the public, worry them, or provoke them against "the established powers." Penalties are often excessive and may impinge on the freedom of expression.

d. CYBERCRIME AND CYBER SECURITY

Cybercrime is a feature of emerging economies ([Antonescua and Birăub 2015](#)), in part because it indicates that the digitization of economic activities is occurring. So it is unsurprising that many African economies have become important sources as well as victims of cyber-threats ([Kshetri 2019](#)). Cyberattacks can be attributed to uneven and vulnerable systems combined with lax cybersecurity practices. Still, because of the nature of digital networks, the effects of cybercrime extend beyond national boundaries. Research from 2013 projects that many African organizations spend less than 1% of their budgets on cyber security ([Kshetri, 2013](#)). Without cyber security protocols, vulnerabilities can be exploited, and new vectors for cyber attacks can emerge.

One published estimate is that cybercrimes cost African economies \$3.5 billion in 2017, with Nigeria losing \$649 million, Kenya losing \$210 million and South Africa losing \$157 million to cyber attacks of all kinds ([Kshetri, 2019](#)). INTERPOL ([2021](#)) estimates that, on average, each act of cybercrime in Africa is able to steal \$2.7million. 'In 2016, Ghana's financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails and 280,000 related to botnets' ([Kshetri, 2019](#)). In 2016, 11 of 54 countries had cyber security laws and regulations

([Bada, Von Solms, and Agrafiotis 2019](#)). Cyber security initiatives tend to be ‘mostly led by the private sector,’ ([Signé and Signé 2021](#)) with surveys stating that 70% of core business staffers have attended cyber-awareness training of some sort ([Bada, Von Solms, and Agrafiotis 2019](#)).⁴⁰ At the same time, lack of skilled and professional cyber-security workers hampers implementation, at least in some countries with smaller economies.

Overall, the low investment into cyber security increases the cost of doing business, with many costs also passed unto citizens and consumers ([Eboib 2020](#)). Citizens of African countries tend not to be fully aware of the risks in cyberspace ([Bada, Von Solms, and Agrafiotis 2019](#)). This is indicative of how weak cyber security is restraining the economic growth and social development in Africa. An added complexity is the alleged extensive use of unlicensed or pirated software, often due to prohibitive costs ([Asongu 2014](#)). Without the ability to take advantage of security updates from manufacturers malware can exploit those weaknesses. Internet access is often through mobile platforms, which brings other specific requirements about information security ([Okuku, Renaud and Valeriano 2015](#)). Cybercrime encompasses online scams, digital extortion, business email compromise, ransomware, and Botnets. To help address these variants INTERPOL ([2021](#)) has recently created the African Cybercrime Operations Desk. Given the human factor in cyber security, researchers propose that well-designed public messaging campaigns would be fruitful and economical ([Bada, Von Solms, and Agrafiotis 2019](#)).

African governments have taken steps to address cyber security. At the continental level, for example, the African Union’s Agenda 2063 does address cybersecurity vulnerabilities in their infrastructure and energy development component ([AU, nd.](#)). Furthermore the AU does have a [Convention on Cyber Security and Personal Data Protection](#). As of October 2022, 13 countries have ratified the convention ([AU, 2022](#)). These countries are Angola, Cape Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia. However, the convention is still not in force. The AU Convention on Cyber Security has been aided by periodic information sharing workshops held between the [AU Commission and the Council of Europe](#). Additionally, the AU does have a [Cybersecurity Expert Group](#). In 2020 the International Telecommunication Union’s (ITU) Global Cybersecurity Index ([2020](#)) found out that overall African countries had made gains on passing data protection legislation, with 29 countries having done so, and with 4 countries in the drafting process. At the time of the ITU report 11 had not initiated the legislative process. One area of concern is that the ITU ([2022](#)) found out that less than half of African countries had Computer Security Incident Response Teams (CSIRTs), a central institutional mechanism to reliably deal with cyber incidents. Still, there is room for national and transnational coordination to work toward cyber-resiliency, but this must be undertaken at the technical level to mitigate threats.

⁴⁰The survey was underspecific on which sectors to which this statistic applies.

Policy Pathway for African Governments on Cyber Security

The [Brookings Institute](#) suggests the following policy pathway for African policy makers:

1. Define a medium and long-term cyber security strategy, supported by appropriate legal frameworks.
2. Integrate this cyber security strategy into government initiatives while calculating the costs required.
3. Establish and fund a national authority to implement the strategy.
4. A ‘whole of government’ approach to promote responsible cyber security culture in order to build confidence and credibility in digital services,
5. Promote awareness-raising and training programs in cyber security in the public, private, academic, and civil society sectors so that there is deep knowledge on how to mitigate cyber security risks.
6. Devise response plans to anticipate actions before, during, and after major attacks on key infrastructure, with these plans including plans on how to continue functioning if digital networks were damaged.

African countries have attempted to put in place appropriate legislation, in SADC at least most countries have either passed specific cyber crime or amended existing laws. However, capacity to investigate and successfully prosecute cyber crimes is inadequate ([3SA 2022](#)). Laws protecting personal data are recognized as necessary adjuncts to cyber crime legislation. However specific legislation to protect children online is largely absent. Cyber security, and the investigation of cyber crime is complicated by cross-border issues, since investigating authorities have geographically bounded jurisdictions while malicious actors have no such constraints.

e. SURVEILLANCE

Much attention has been given to the implications of Dragnet US signals intelligence for African states ([Duncan 2018](#)) as well as the direct impact of the US military in Africa with regard to surveillance, development, and governance ([Piombo 2015](#)). More recent scholarship has looked at the reconstitution of the African security cluster (e.g. [Duncan 2015](#)). If it was ever the correct appraisal in the first place, the African state’s apparent lack of bureaucratic capacity to undertake technological surveillance is rapidly diminishing as surveillance capacities are being acquired from multiple vendors. Documentation of these developments are partially incomplete due to secrecy. Some commentators express concern that Chinese based firms are selling surveillance capabilities to authoritarian-leaning governments in Africa ([Gravett 2022](#)) without much due consideration given to the exercise of human rights.

What is known about state procurement of surveillance equipment and the construction of a state surveillance apparatus mostly comes from inferences of state press releases, like when the Ugandan police unveiled its CCTV system ([Independent 2022](#)). Leaks of confidential documents to journalists and human rights organizations supplement this knowledge.

The private security industry not only has an expanding labor force for surveillance activities, but is acquiring similar capabilities as the state ([Diphorn 2016](#)).

f. ONLINE GENDER-BASED VIOLENCE

In 2020, the humanitarian organization [Plan International](#), heard from 14,000 girls and young women from across 31 countries in [surveys](#) based on online experiences from around the world. As many as 58% had experienced online harassment, with half saying they faced more harassment online than in the street. Plan found out that girls are being targeted online “just for being young and female...” and that “it gets worse for women and girls who are politically outspoken, disabled, Black, or identify as Lesbian, Gay, Bisexual, Transgender and Queer (LGBTQ+)”.⁴¹ A particularly disturbing implication of this was the finding that online abuse was pushing women and girls offline and at times when policy objectives are pushing for gender equity and participation in public spaces.

African women are stalked, harassed and targeted on platforms, in some cases leading to gender-based sexual violence ([Makinde et al 2016](#)). Platforms are spaces where the LGBTQ+ population are targeted by hate speech and gender discrimination ([Mkhize, Nunlall and Gopal 2020](#)). In response, Women’s rights groups across the continent are using social media to mobilize against gender-based violence ([Skalli 2015](#), [Wasuna 2018](#), [Oparinde and Matsha 2021](#)), but they are doing so in a vacuum of platform’s own content moderation programs.

The adoption of the Resolution on the [Protection of Women Against Digital Violence in Africa \(ACHPR/Res.522\(LXXII\) 2022\)](#) during the African Commission of Human and People’s Rights (African Commission) is an important legal step in recognizing the extent of online abuse against women, though it fails to acknowledge the intersectionality of those that are most vulnerable in terms of race, class, gender, sexuality, urban or rural location. It identifies online violence as occurring through cyberstalking, unsolicited sexually explicit content, doxing, cyber-bullying, and the non-consensual sharing of intimate images. Importantly the Resolution reiterates the definition of violence in the African Charter on the Rights of Women in Africa (the [Maputo Protocol](#)) as including “...acts that cause psychological or economic harm or threats to undertake arbitrary restrictions on or deprivation of fundamental freedoms”.⁴²

The Resolution calls on Member States to:

- review and adopt legislation that will counteract all forms of violence by including digital violence (cyber-harassment, cyberstalking, sexist hate speech, etc.) in the definition of gender-based violence;
- conduct research on digital violence against women;
- raise awareness through programs targeted at boys and men about the causes of digital violence against women;
- close the digital gender divide by empowering women with digital technology education;
- facilitate the cooperation between law enforcement and service providers to identify perpetrators and gather evidence for online harms;
- protect women journalists from digital violence by repealing overly wide surveillance laws that perpetuate their vulnerability; and
- implement gender-sensitive policies when handling cases of digital violence against women.

g. HUMAN RIGHTS ONLINE

Participation and public confidence in the data driven economy requires the realization of human rights and the rule of

⁴¹ <https://www.globalcitizen.org/en/content/what-is-online-gender-based-violence-2/>

⁴² <https://powersingh.africa/2022/08/15/african-commission-resolution-on-protection-of-women-against-digital-violence/>

law in the digital environment. This would mean that the human rights treaties to which African states are committed need to be implemented in the online environment. Across Africa, there is a general consensus that the laws, rules, and other policies that promote cross-border data policies must support human rights, such as by protecting privacy, as well as socioeconomic rights like the right to work and of equitable access to public services. In addition to effective law, regulation, and enforcement, sentiments also demand that the private sector and governments uphold human rights in order for these rights to be realized, particularly with regard to data privacy and the sharing of public data. To this end, African countries have generally shown willingness and eagerness to have human rights being at the forefront of data and digital governance. This is evidenced by, among other efforts:

- African participation at the Human Rights Council adopted resolution 26/9 by which it decided “to establish an open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights, whose mandate shall be to elaborate an international legally binding instrument to regulate, in international human rights law, the activities of transnational corporations and other business enterprises.”
- The publication of the AU Data Policy Framework, a resource intended to enable African countries to maximize the benefits of a data-driven economy by creating an enabling policy environment and building a positive data economy at the national and regional levels. Central to its attainment, the Framework emphasizes the need for a “consolidated data environment and harmonized digital data governance systems to enable the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits.”

II. INCLUSIVE ECONOMY

a. COMPETITION

Cross-border data flows can have effects on competition. As has been mentioned, the practice of data analytics, among others, means that firms with data collection and storage capabilities are able to gain new insights that other competitors cannot gain. As elsewhere in the world the rise of the digital economy has forced competition authorities around the world to define digital and data markets and review more traditional instrumental regulatory tools, which appear inadequate and may produce negative unintended consequences on these dynamic adaptive international systems. While seeking to prevent anti-competitive practices of dominant or monopoly global corporations, and safeguarding local business, the dynamic and global nature of the data economy requires that regulators look beyond their jurisdictions.

In a continent that is unevenly developed as Africa, being in a relatively weak position in relation to other economic regions, it will be essential that, where cross-border data flows are possible, such flows do not inadvertently favor one competitor at the expense of another and that data extraction by monopoly global platforms in particular does not go unchecked. Continued information asymmetries would go against the “shared prosperity” that cross-border data flows are meant to facilitate.

In light of the above considerations, competition regulation and law reform have been deemed necessary by a number of progressive states. The general consensus has been that competition laws and regulations must first establish a regional and competent competition authority that has the power to regulate cross-border data, make inquiries into continental and regional effects, and cooperate with other competition regulators. Competition regulations will also require updating so that competition regulators are empowered to take into account the systematic risks of

changed market structure, such as increased scale of data breaches in regulation of mergers and acquisitions. Likewise, the legislation that sets the powers of competition authorities must be reviewed to ensure that it gives sufficient flexibility to regulators to adjust their regulatory tool.

Recognizing that digital markets and services have transformed the global economy, a coalition of five African regulators announced their intention to collaborate in dealing with the “considerable challenges for competition law enforcement and policy in terms of the unique competition issues that arise” in these markets. In a [statement](#) earlier this year competition authorities from Egypt, Kenya, Mauritius, Nigeria and South Africa said they would need to collaborate to develop capacity and share knowledge and common strategies with respect to the regulation of digital markets. They noted that it is the regulators’ role to consider how digital markets affect domestic participation in the local and global economy and that, in this regard, they (the five regulators) agreed to collaborate in the regulation of digital markets by:

- scoping the conduct in digital markets that has been the subject of investigation in other jurisdictions, on African consumers, businesses, and economies with the purpose of fair regulation and enforcement in Africa (where applicable);
- researching the barriers to the emergence and expansion of African digital platforms and firms that may contribute to enhanced competition and inclusion in these markets for the benefit of African consumers and economies;
- co-operating in the assessment of global, continental, and regional mergers and acquisitions in digital markets, including harmonizing the notification framework; without prejudice to confidentiality commitments;
- sharing information in accordance with existing laws and applicable protocols; and
- sharing knowledge and building capacity to deal with digital markets.

b. TAXATION

Africa’s economic structure remains largely commodity dependent with a low-income tax base due to high levels of informality. The tax system therefore constitutes a fundamental development policy instrument and opportunity for resource mobilization from trade in the continent, and a central element in the establishment of the AfCFTA. Although the instruments in AfCFTA that have already been agreed do not mention the digital economy and issues of digital trade that have only been put on the agenda recently, the African Union’s [Digital Transformation Strategy](#) highlights the importance of the digital economy for the continent ([RIA, 2022](#)). Several protocols of AfCFTA that are currently negotiated bear on the digital economy.

Currently only around ten African countries, including Angola, South Africa, Cameroon, Nigeria, Algeria, Senegal and Kenya, have proposed some form of tax regime for digital goods and services ahead of the finalization of the proposed Basic Erosion and Profit Shifting (BEPS) measures in taxing their elusive digital economy firms—over and above value added taxes (VAT) to mobilize state revenues. BEPS refers to tax planning strategies used by multinational enterprises that exploit gaps and mismatches in tax rules to avoid paying tax. In addition, countries such as Nigeria, Kenya, Zimbabwe and Tunisia, have implemented or are in the process of implementing digital service taxes (DST). DSTs are aimed at collecting revenue from commercial activity and are distinct from the excise or ‘sin’ taxes on social media and mobile money users that have been counterproductive in raising revenues, as they inhibit use, which further undermines universal access objectives and violates associated human rights. ([RIA, 2020](#)).

However, many of the tax frameworks that have been put in place are basic and do not take into consideration the

full spectrum of the digital economy ([Musgrove, 2020](#)). In addition, quite a number of African countries (including Uganda, Mozambique, Tanzania, Zambia and Benin) are already imposing unilateral tax measures on some digital economy transactions, especially on Foreign Service Providers. These taxes generally comprise excise⁴³ duties on digital transactions, value-added taxes (VAT), social media taxes, and online content license fees, with Over-The-Top (OTT) service fees and profit-targeting equalization levies ([RIA, 2022](#)).

c. FINANCIAL INCLUSION AND MOBILE MONEY

Financial inclusion is an immense challenge in the African continent, where more than 70% of individuals do not have access to formal financial services. The [2018 RIA After Access survey](#) shows that, of the countries surveyed, Kenya leads in financial inclusion, with 87% of the population having access to financial services, followed by South Africa and Ghana with 59% each. For the other countries surveyed, less than 50% of the population are financially included. Furthermore, the survey highlights that African residents who reside in urban areas (57%) are more likely to be financially included than those who live in rural areas (38%). Men are also more likely to be financially active than women, resulting in a 21% gender gap in the surveyed countries.^{44 45} ([RIA, 2019](#)).

A survey by the World Bank, however, shows that financial inclusion has increased from 23% to 43% in Sub-Saharan African countries. This is driven in part by the growth of mobile money usage. The 2017 RIA After Access survey found out that 46% of people in the surveyed countries had access to mobile money services. However, mobile money services were indicated to only be successful in Kenya (85%), Ghana (55%) and Tanzania (45%), but had very little success in South Africa (8%) and Nigeria (4%). The survey further highlighted that the success of mobile money services was dependent on bank account ownership, with countries that had the majority of their population financially included (for instance South Africa) less likely to have a high mobile money penetration rate. The low success rate of mobile money in Nigeria was found to be a result of inhibiting financial regulations ([RIA, 2019](#)).

Interoperable cross-border mobile money is both a challenge and an opportunity for financial integration, regionally and across the continent. However mobile money has had the greatest uptake where there is relatively less regulation. Cross-border mobile money is inhibited by restrictive financial regulation. A key question for the development of regional and continental markets is how to enable cross-border mobile money while regulating the money supply, and guarding against fraud.

d. DIGITAL TRADE

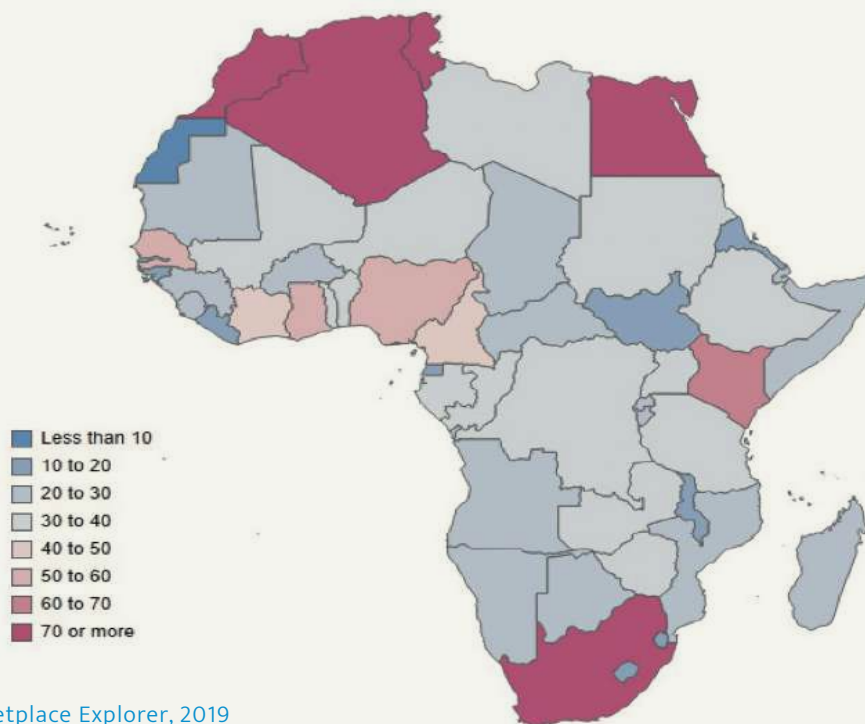
According to [ODI](#) in a report on unlocking Africa's digital trade, Africa still lags behind in terms of retail digital economy when compared to other regions like South America and Asia (ODI, 2022). Only 30% of the African population engaged in the regional Business to Consumer (B2C) e-Commerce model with a generated turnover of USD 22 billion compared to Asia's USD 1,100 billion. In Africa, only 10 countries are responsible for [94% of all online businesses](#) in Africa with Kenya, Nigeria and South Africa generating 45% of the regional online retail sales (International Trade Center, 2020).

⁴³Shamira Ahmed and Alison Gillwald, 'Multifaceted Challenges of Digital Taxation in Africa', Policy Brief 2020, (Cape Town: Research ICT Africa, 30 November 2020), <https://researchictafrica.net/publication/multifaceted-challenges-of-digital-taxation-in-africa/>.

⁴⁴African Union, 'AU Data Policy Framework'.

⁴⁵ Alison Gillwald and Onkokame Mothobi, 'A Demand-Side View Of Mobile Internet From 10 African Countries', After Access Policy Paper, Policy Paper Series 5: After Access-Assessing Digital Inequality in Africa (Research ICT Africa, April 2019), https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf.

Figure 2: e-Marketplaces in Africa



Source: ITC Africa Marketplace Explorer, 2019

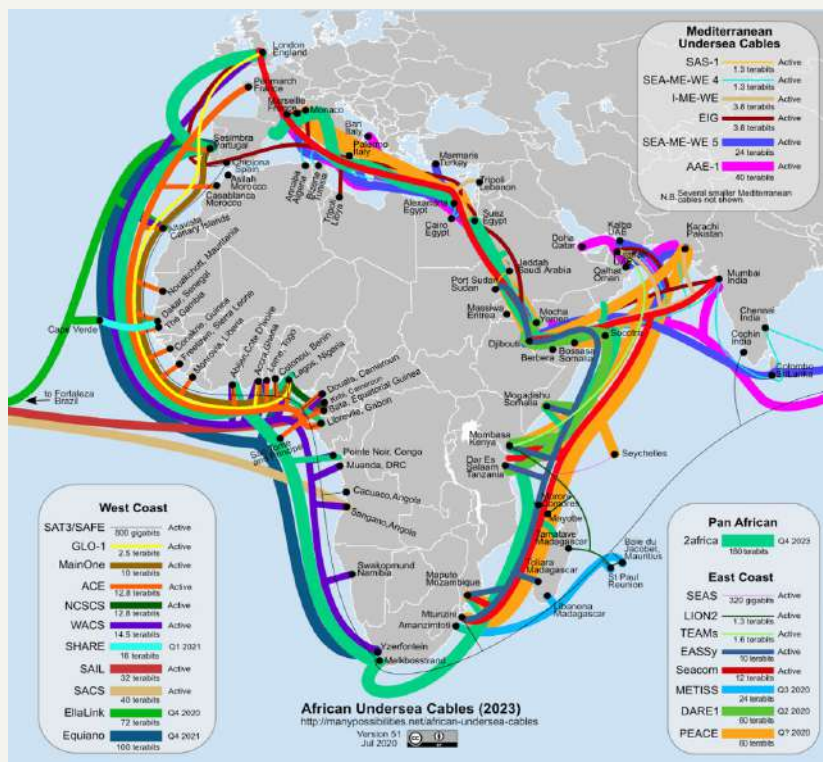
The potential of Africa's digital trade has been mainly inhibited by low intra-African trade, limited Internet connection and access to financial systems (ODI, 2022). As it has been noted earlier, the AfCFTA is critical to realizing the potential of Africa's trade. This potential, especially as it concerns digital trade alone is huge and the AU realizing this, has started to work on an Africa e-Commerce Strategy (ODI, 2022). The Strategy places a lot of emphasis on mobile money payment platforms which are beginning to sprout across the continent. According to the Strategy, these platforms have the opportunities to transform Africa's e-Commerce landscape when they are interconnected across borders. It identifies how the AfCFTA can promote Africa's e-Commerce through digital taxation, data governance that ensures data protection and cross-border data flows and custom duties on electronic trade. The Strategy, by positioning AfCFTA as the main factor in the realization of digital trade in Africa, identifies three areas that are important for harmonization. These include harmonization of custom rules in rapid clearance, (especially with respect to B2C), a pan-African payment settlement system and harmonization of cyber laws that engenders trust and facilitates legal recourse. At the heart of this harmonization strategy also lies the need to address issues such as consumer protection, authentication, data localization, cross-border data flows, cyber security and data protection (ODI, 2022).

e. INFRASTRUCTURE

Digital and data infrastructure is less developed in Africa than in any other part of the world. The current status of infrastructure in Africa can be summarized as follows:

Connectivity: while enormous progress has been made in the past ten or more years with the laying of transoceanic cables and construction of backbone infrastructure, there are still challenges in last mile connectivity in parts of the continent.

Figure 3: Major Internet cables connecting Africa



Connectivity: enormous progress in the past ten or more years with laying of transoceanic cables and construction of backbone infrastructure but there is limited or no connectivity last mile connectivity in much of the continent.

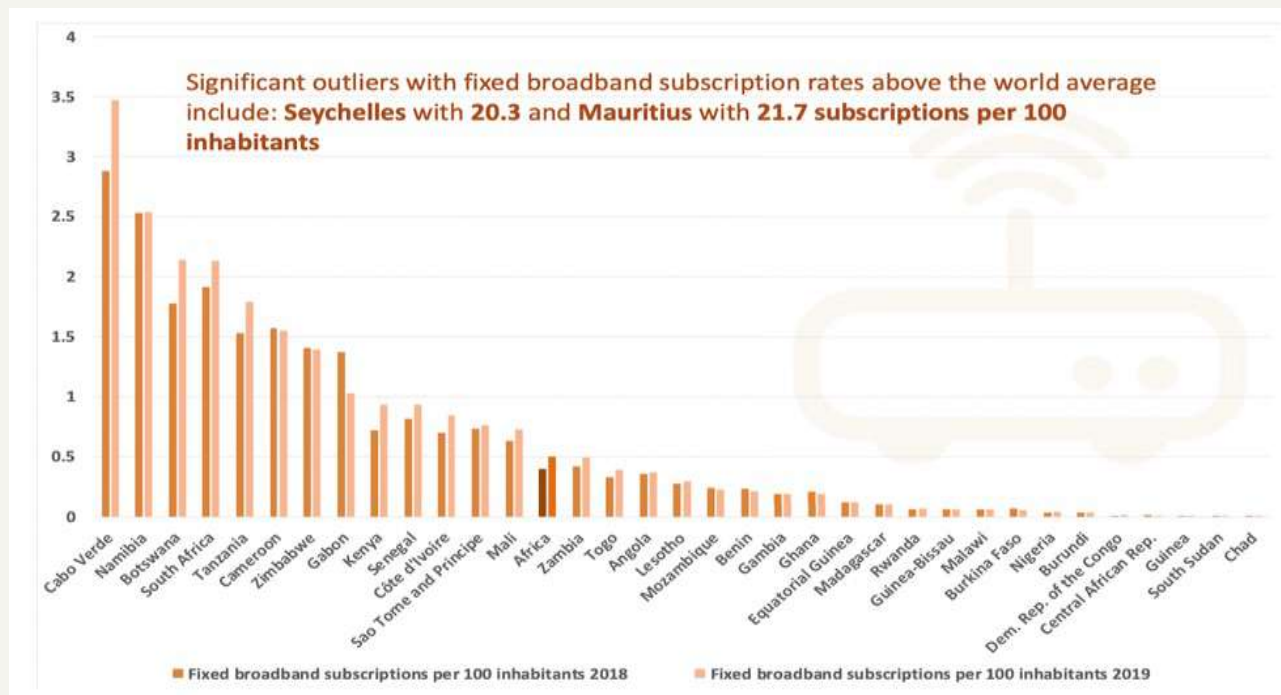
There is a need for a sustained policy to grow infrastructure and regulatory institutions, at the scale required for the continent. Cross-border data flows are essential among African countries but also in and out of Africa to increase network effects. These require the infrastructure upon which data flows and value creation depend.

f. INTERNET CONNECTIVITY

Currently, Africa’s Internet connectivity is among the lowest in the world.⁴⁶ Data infrastructures such as data and collocation centers need quality and affordable internet services (Africa Data Centers Association, 2021). Due to the cloud and remote functions required of these centers in order to store, process and transfer data, high speed and reliable internet connection is necessary. However, currently in African countries, not only is internet connection still low, broadband access and quality is inadequate (UNCTAD, 2021).

⁴⁶ ‘The State of Broadband 2019: Broadband as a Foundation for Sustainable Development’ (Broadband Commission, 2019), <https://www.broadbandcommission.org/publication/the-state-of-broadband-2019/>.

Figure 5: Fixed broadband subscriptions per 100 inhabitants, Africa region



Source: [International Telecommunications Union \(ITU\)](https://www.itu.int), 2021

Whether or not a legislative approach to data flow is restrictive, African countries still need to make deliberate provisions of more quality Internet services as its benefits are not just limited to optimal data storage, processing and transfer but also include dynamic and multiple socioeconomic advantages including increased e-Commerce benefits.

g. DIGITAL ID

The African continent hosts the highest percentage of people without legal identity and are subsequently uncovered by civil registration and denied essential social services offered by states such as healthcare, basic education or food services. The digital economy, however, offers opportunities to redress inequalities such as socio-economic and structural exclusions suffered by minority groups in the continent. Digital forms of (legal) identification are becoming increasingly popular and prevalent in the continent. The COVID-19 pandemic has, similarly to other forms of digitization, increased both the appetite for and potential utility of socio-digital identities (e.g., for vaccine certifications). This underlines the need for critically assessing the design, development, implementation, financing or funding, and governance of digital identities.⁴⁷ Digital ID is facilitative for both private and public sector purposes within a data economy, but demands a robust trust-guided framework to mitigate against the potential harms like personal data abuse, exclusion, or discrimination based on inaccurate (or unfair) data representation, which may accompany such initiatives. A fair and trustworthy digital identification system is a central prerequisite to combining and repurposing public administrative data with other types of data across various use cases. Further, despite several countries introducing digital identification systems, pervasive and interoperable digital identification systems remain a major social and economic challenge in the continent. A study by Research ICT Africa revealed that, while many countries realize the utility of digital ID, colonial histories, which often lead to crowded and disorganized digital ecosystems, opaque

⁴⁷ Anri van der Spuy, 'Conclusion: Assessing Socio-Digital Identity Ecosystems in Africa', Research ICT Africa, 9 November 2021, <https://researchictafrica.net/publication/conclusion-assessing-socio-digital-identity-ecosystems-in-africa/>.

public-private interplays, a frequent lack of institutional capacity (or will), difficult interactions with aid agencies' agendas, and the seemingly unquenchable thirst for digital Kool-aid in the absence of much strategic vision, political will, or institutional capacity, often mar the efforts to effectively embed digital ID systems.⁴⁸

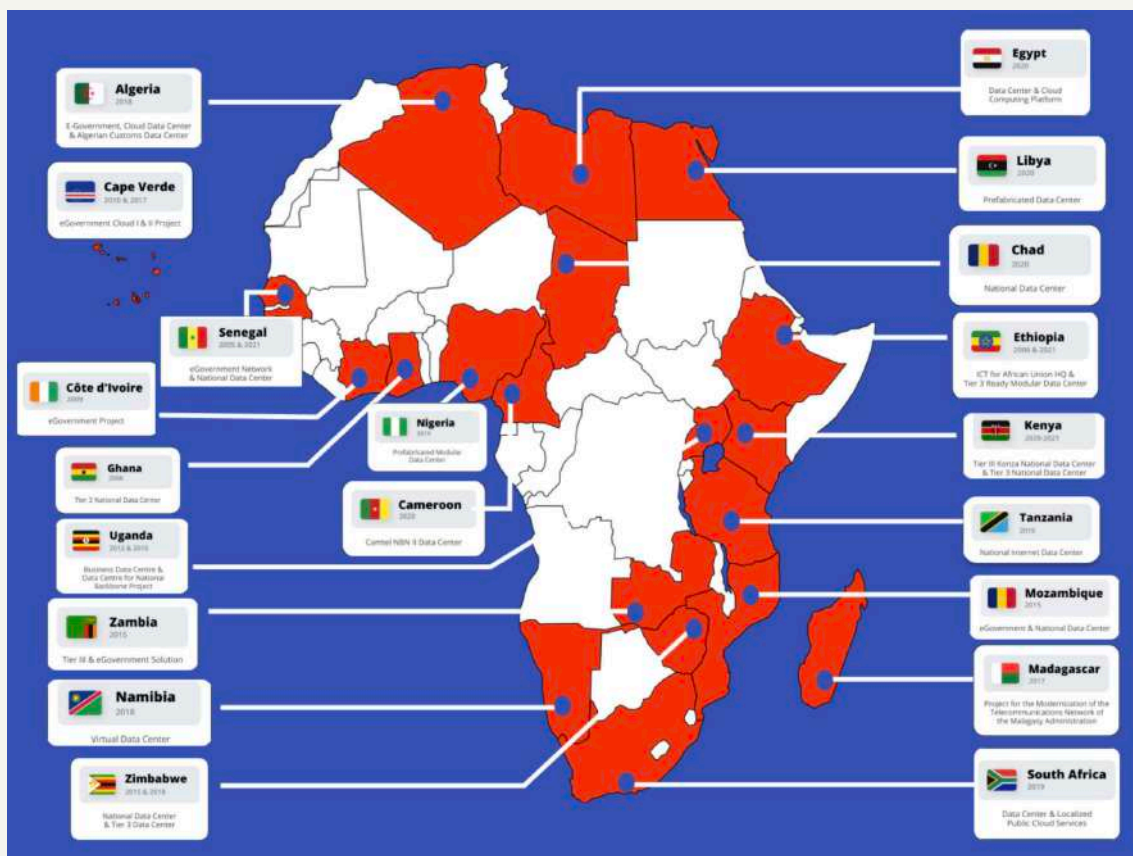
However, it seems the emerging regional frameworks on digital identity are starting to engage with this challenge directly. There are opportunities for decentralized, functional identity to be embedded in data protection frameworks. These may provide functional identity while reducing the risks associated with personal data and encouraging the use of more collaborative and multistakeholder approaches for the design, financing or funding, implementation and governance of digital identity ecosystems.

h. DATA CENTERS

Data centers may be referred to as the remote location where data are stored, processed and distributed (Africa Data Centers Association, 2021). As of mid-2021, Africa accounted for only 1% of the global colocation data center supply according to Xalam Analytics (African Business, 2022). Data center market revenue in Africa is projected to grow by 12% during the period 2019-2025 reaching at least USD3 billion by 2022 ([Data Center Market in Africa Report](#)). Data centers construction in Africa is booming but is still unlikely to meet the demand. One estimate is that seven hundred new data centers are needed in Africa. Most constructions are in a few hubs, especially in South Africa, Kenya and Nigeria ([Profica 2020](#)). Despite high demand, constructing a data center is capital intensive due to the [requirements](#) of data centers. Prerequisites for a data center include space, high bandwidth connectivity, reliable renewable electrical power, cooling, security and skills. Data centers in Africa are thus restricted to locations with high bandwidth connectivity such as landing points of oceanic cables. Reliable energy supply is absent especially in South Africa that has the highest number of data centers in the continent. As a result, data centers will need to self-supply power, raising the capital requirements. Ambient temperature and humidity, and water supply affect which cooling technologies can be used, and are thus a crucial factor in locating data centers. Data centers not only require security but also secure environments due to the vulnerability of fiber and power connections. Thus, data centers require political stability, rule of law and protection from crime. Skilled staffers are required to run the data center, in particular to ensure that consistent temperature, humidity and power are maintained, and that data is backed up to other locations. Together, these constraints militate against every country creating its own data centers.

⁴⁸ Anri van der Spuy et al., 'Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative Analysis of Findings from Ten Country Case Studies', Africa Portal (Research ICT Africa, 11 November 2021), <https://www.africaportal.org/publications/towards-evaluation-socio-digital-id-ecosystems-africa-comparative-analysis-findings-ten-country-case-studies/>.

Figure 6: Location of Data Centers in Africa



Source: TechCabal, 2022

i. E-GOVERNANCE

E-governance, also referred to as electronic governance, is the use of information and communication technologies to solve governance problems. The business of government and governance is complex; however, the ideal goal of any governance system is to improve the lives of people. It can also be defined as government technology directed toward provisioning public services. In African countries, e-governance is fast gaining roots through the use of technologies to implement basic government policies and services. Most e-governance services are grouped into Government-to-Citizen services (G2C), Government-to-Business-and-Citizen (G2BC) and Government-to-Government (G2G) (African Union Development Agency (AUDA-NEPAD), 2022). Some of these basic services include digital IDs, voting, banking, e-immigration services etc. In addition to these services, data has proven more useful beyond the limits of government provisions to include other uses such as civic technology.

Civic technology may be described as the technology that improves citizen engagement in order to demand more transparency and accountability from the government (EDPM, 2022). In a database curated by Civic Tech Innovation Network, there are currently 144 initiatives spread across the various countries like Nigeria, South Africa, Zimbabwe, Burundi and others (Civic Tech Innovation Network, 2020). These initiatives focus on various sectors such as education, justice and human rights and gender. The various technologies used to engage the citizenry include blockchain, chatboxes, geo-coded mapping, OpenStreetMap, etc. In many instances, these initiatives collect government data like budgets, line items, and procurement to engage citizens in demanding more accountability from the government. In some instances, the data collected is used to educate the public on important civic duties such as voting and payment of taxes.

Figure 7: Examples of civic technology initiatives across Africa



Source: Civic Tech Innovation Network, 2020

III. THE NEED FOR COORDINATION AND HARMONIZATION ON DIGITAL POLICY

The DTSA includes an analysis of Strengths, Weaknesses, Opportunities and Threats (SWOT) that laments weak coordination among the continental institutions, which are pursuing the digitization agenda of the continent. Much of this weak coordination is characterized by low cohesion, cooperation, coordination and harmonization among regional and continental actors. This is largely seen in the fragmented approaches to governance in Africa. There are currently 8 different regional economic communities (RECs), each with its own version of data regulations and different developmental goals. Similarly in areas such as intellectual property regulation, Africa has two IP organizations in ARIPO and OAPI which can be construed as lacking unity. In addition, South Africa and Nigeria, two of Africa’s largest economies are not members of either OAPI or ARIPO. This is also evident of the point that Africa lacks a unified purpose or voice.

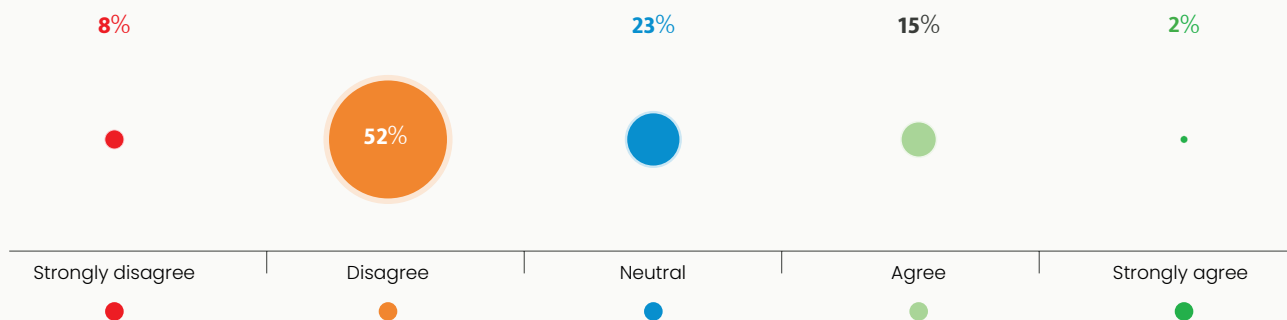
Agenda 2063, among other things, emphasizes the need to build shared prosperity and to integrate in order to build responsive and democratic governance. A particular realization of the need to coordinate and harmonize can be found in paragraph (f) of Goal 66 of Agenda 2063, which, in the context of describing the changing global context, refers to a move toward “multipolarity”.⁴⁹ The AfCFTA is seen as an opportunity to remedy the lack of harmonization and coordination in the continent. The majority of African states have ratified the agreement which is indicative of their willingness to harmonize.

⁴⁹ The text reads: “The changing global context, and in our times the modern information revolution; globalization; changes in technology, production, trade, knowledge and labor markets; the opportunities presented by global demographic trends, urbanization and the growing global middle and working classes in the South; the move towards multi-polarity with strong elements of uni-polarism remaining, global security and the impact of climate change. Humanity today has the capacities, technology and know-how to ensure a decent standard of living and human security for all inhabitants of our earth. And yet children continue to die of preventable diseases; women continue to die whilst giving birth; hunger and malnutrition remain. part of the human experience; and underdevelopment, fragility, marginalization and inequality between regions and countries and within countries persist.”

In the data collection phase of this Report, stakeholders agreed that there is a need to increase coordination among African countries on policy issues. There is, thus, support for the integration envisaged in Agenda 2063, as well as, concern about its achievement.

Figure 8

There is strong coordination among African countries on digital issues



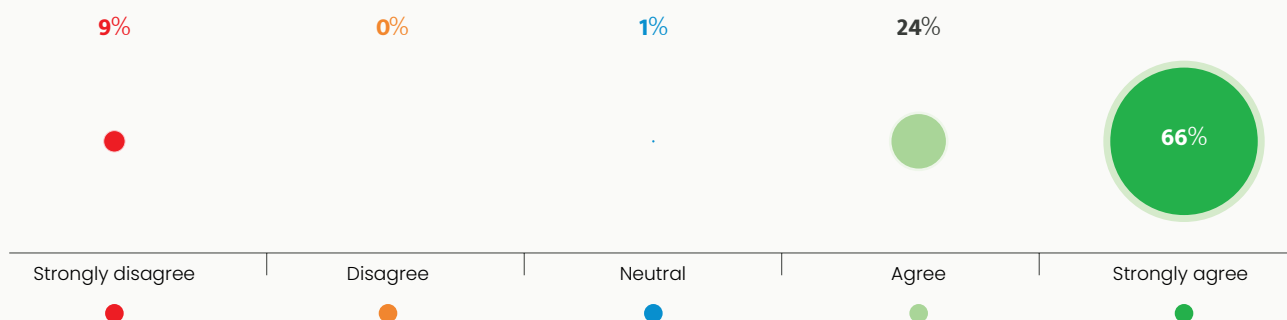
During the data-gathering exercise carried out during the African Internet Governance Forum (AFIGF) in Malawi for this study, respondents addressed the twin questions of coordination and collaboration. The proposition that African countries currently work together on cross-border data policies attracted the lowest average ratings, as most respondents disagreed with the proposition. More than 60% of the respondents rejected the statement that African countries coordinate their actions on data policies.

Conversely, the respondents agreed that African states need to work closer together on policy matters. This agreement reflects the second-highest average rating (after the agreement on Africa’s international participation to further its own vision and agenda), evidencing an undeniable consensus on this question.

Similar sentiments were expressed on the need for African countries to work together more.

Figure 9

African countries need to work more together on digital issues



a. REASONS FOR COOPERATION

Stakeholders who supported cooperation did so for multiple reasons.

Figure 10

The most important reasons for African countries to work together to regulate data are

1. To increase the scale and scope of data markets so that they can be sustainable

2. To create a unified regulatory environment to provide certainty for investment

3. To have sufficient power to regulate multinational digital platforms

4. To influence global policy

Among the reasons advanced for collaboration, mostly by 75% of the online survey respondents, is the fact that such collaboration would increase the scale and scope of digital markets so as to make them sustainable. Another one, as advanced by 71% of the respondents, is that such collaboration would enable the African continent to influence global policy.

The prospect of gaining enough power to regulate multinational digital platforms received the lowest though positive rating. This may reflect the impression that some respondents reasoned that the ability of African countries to regulate digital multinationals does not sound realistic.

Most respondents either lamented a lack of coordination or regarded it as unlikely, given either the capacity or competing policy agendas of national governments. There was none who thought that the combination of cooperation and collaboration was undesirable. But there was no principled opposition to cooperation and collaboration based on claims about the sovereignty of nation states or a perceived need for competition between Member States.

“The success of any data flows strategy in Africa will be if it can bring together a coalition of the willing. States are sovereign and cannot be compelled into doing anything; there needs to be willingness to cooperate. We saw this with roaming and mobile money across Africa, where leaders in member states said, “Let’s just make it happen. We will see cross-border flows between countries and regions on the basis of being willing partners.”

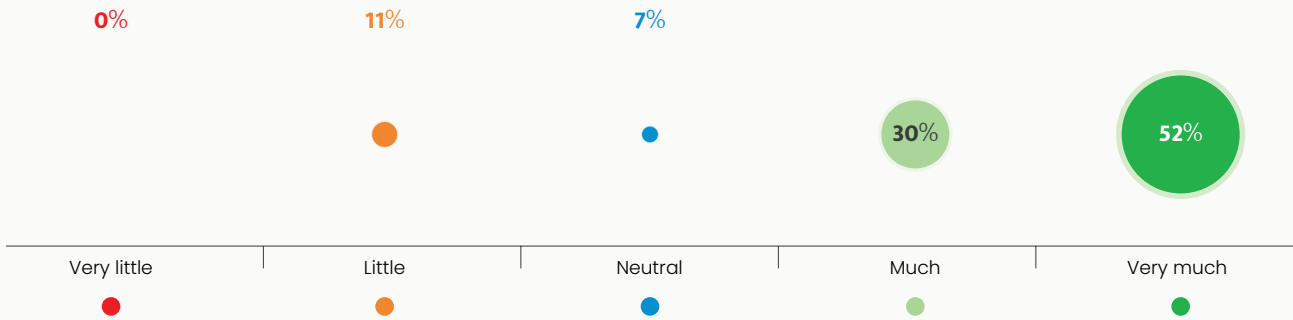
- Senior stakeholder during the interview-based data collection phase of this Report

b. EXTERNAL INFLUENCE ON AFRICAN REGULATION AND POLICY

Another issue raised by stakeholders in research relates to external influence on African regulation and policy. In response to a question posed in the online data collection process, the majority of stakeholders polled believed that there is external influence on digital policy formation in Africa.

Figure 11

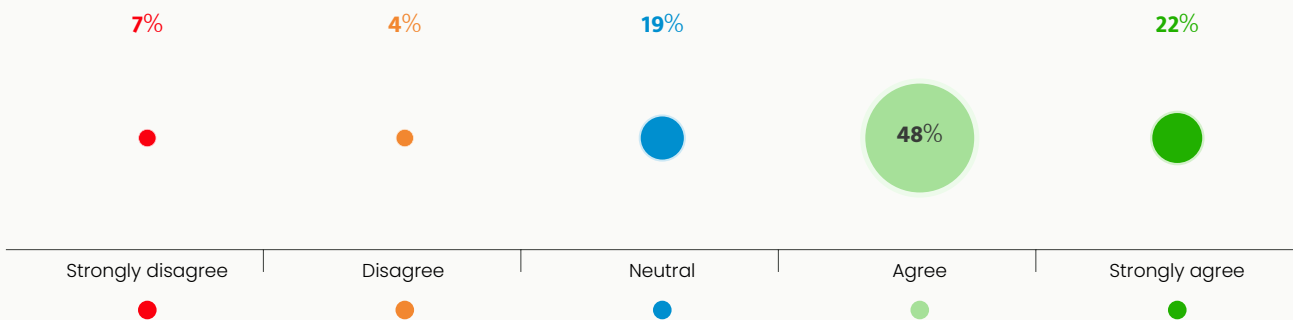
To what extent are African actors subject to regulations adopted elsewhere?



A question specifically asked about external influence on Internet governance and regulation elicited the perception that external influences on African governance and regulation of the Internet are strong.

Figure 12

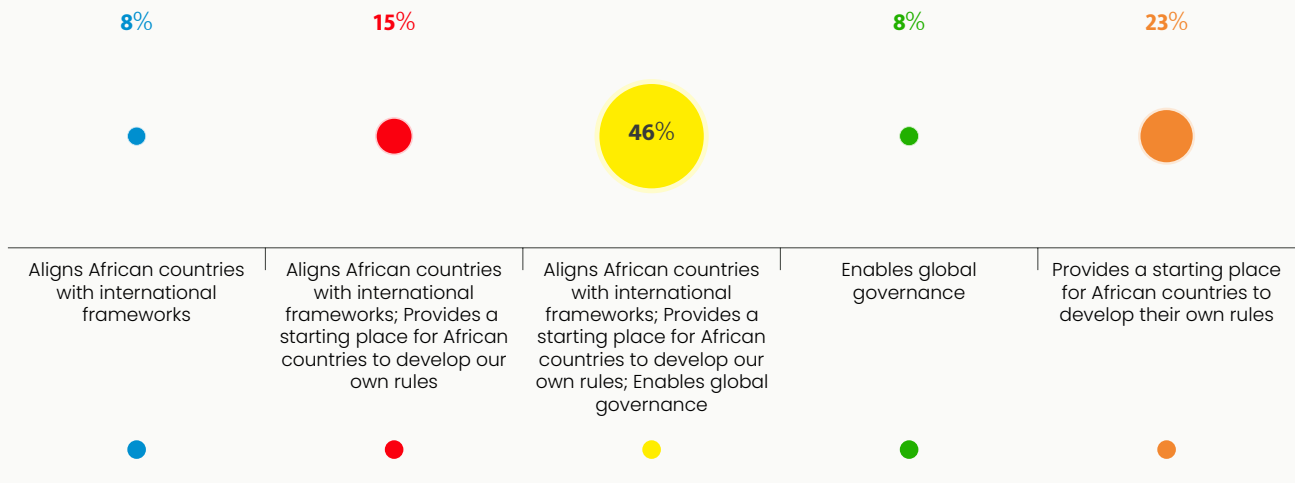
To what extent do regulatory approaches from foreign countries and regions, such as the EU, the United States, or China, influence national initiatives on Internet governance and regulation in Africa?



External influence on African policy and regulation is not necessarily regarded as wholly negative or positive. The positive aspect favored most by respondents is that external influence would result in alignment with international frameworks.

Figure 13

To what extent do regulatory approaches from foreign countries and regions, such as the EU, the United States, or China, influence national initiatives on Internet governance and regulation in Africa positively?



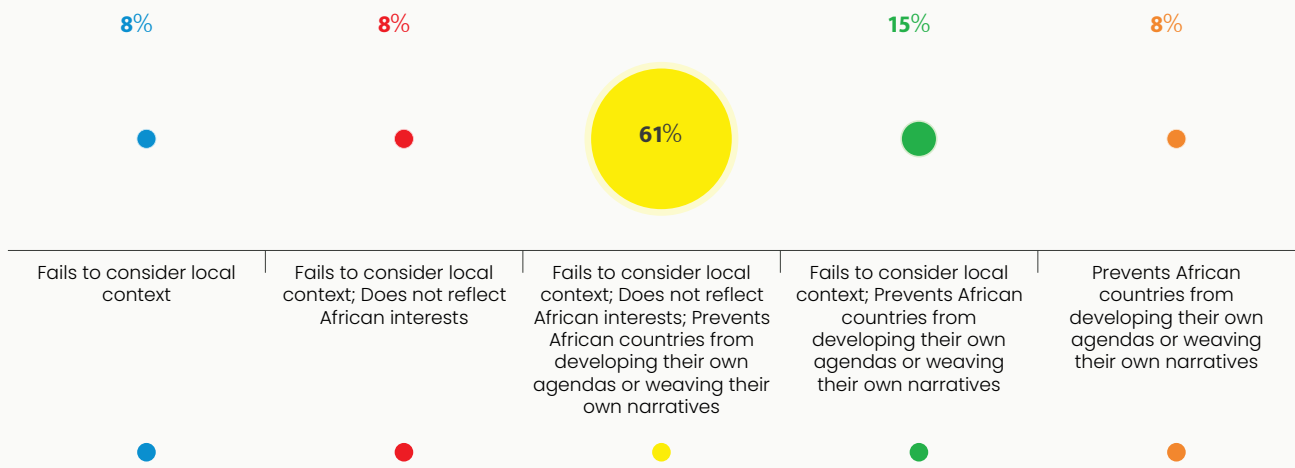
Negative aspects of external influence on African policy and regulation include failing to take local context into account and pre-empting the African countries from developing their own agendas or weaving their own narratives.

One of the biggest risks that I see in relation to the issue of data flows is revenue sharing, as data is money. The multinational tech companies are using this data to generate income; one by developing new inventions, and two by getting income from selling data to other multinational organizations. We in Africa may seem to be in the dark of that at the moment. We don't have African interventions that can store data in the cloud. We must make sure we have discussions and bring other legislators alongside big multinational companies into conversations to address such issues. What are the social responsibility issues of managing and storing our data? What is required is to protect our data?

- Ms Neema Lugangira, Member of Parliament, Tanzania / Chair, African Parliamentary Network on Internet Governance

Figure 14

Reasons why external influence is mostly negative

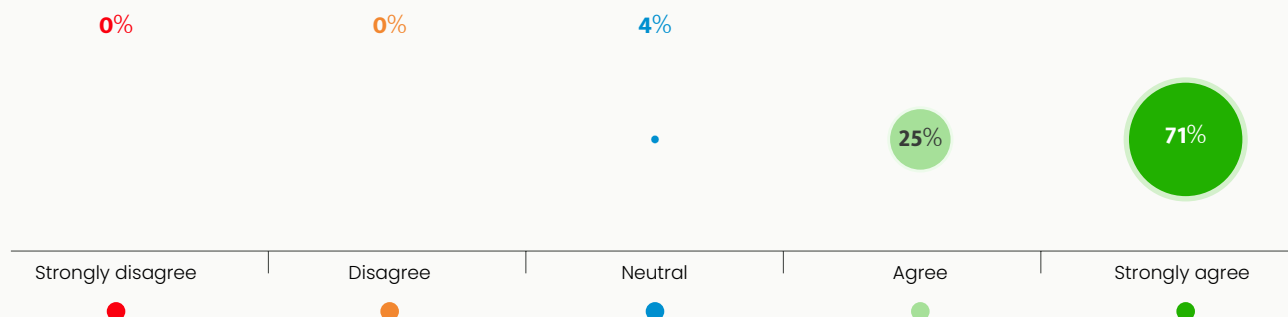


Perhaps to bring it up as a counter to external influence, or at least to play a part in it, many stakeholders expressed a view that African countries should work together to express a common narrative in global policy fora. One aspect of this is participation in standards setting fora. Responses to an online data collection question support this view.

c. SINGLE NARRATIVE IN GLOBAL POLICY FORA

Figure 15

African government delegates should participate more actively in international standard setting forums to improve Africa's ability to formulate or communicate its vision of cross-border data policies.



d. NEED FOR A META-NARRATIVE

Several insights emerged from the workshops and the data collection. In an in-event survey (Menti) conducted during the AfIGF 2022 in Malawi, respondents offered different and sometimes conflicting opinions about whether or not the AU has a paramount narrative. Their position was that if truly the AU does have a paramount narrative, what narrative does it have to tell the world? Nevertheless, three narratives appear most frequently: (1) uplifting the value of data; (2) addressing coordination and implementation; and (3) consolidating Africa's agency in global forums, in that order.

"I believe in the African narrative: Digital technology is bringing an opportunity to Africans to leapfrog. The only way to do so is to work together by removing borders. It is the data economy that allows us to do that. Mobile money innovation success was based on responding to the specific context of Africa. Data flow is the next big thing for Africa. There is so much opportunity, let's just share."

- a senior stakeholder during the interview data collection phase

The knowledge dialogues, while capturing this narrative of strong African voices in global governance fora, also elicited a broader African narrative on forging common policy narratives about Africa as a dynamic, integrated economy offering the scale and scope required for data value creation and an enabling and certain data policy environment for local and foreign investment, trade and innovation. Complementary narratives on the collaboration, coordination and harmonization to achieve these objectives surfaced in all engagements, as did the need for Africans to mobilize around their common interests to provide a coherent voice in matters of global governance.

Crucially, while some responses mirrored the provisions of the policy documents (for example, the 'single market' narrative translates the provisions of the AfCFTA Agreement), only one respondent⁵⁰ relied on the specific provisions that spell out the purposes and vision of those instruments.

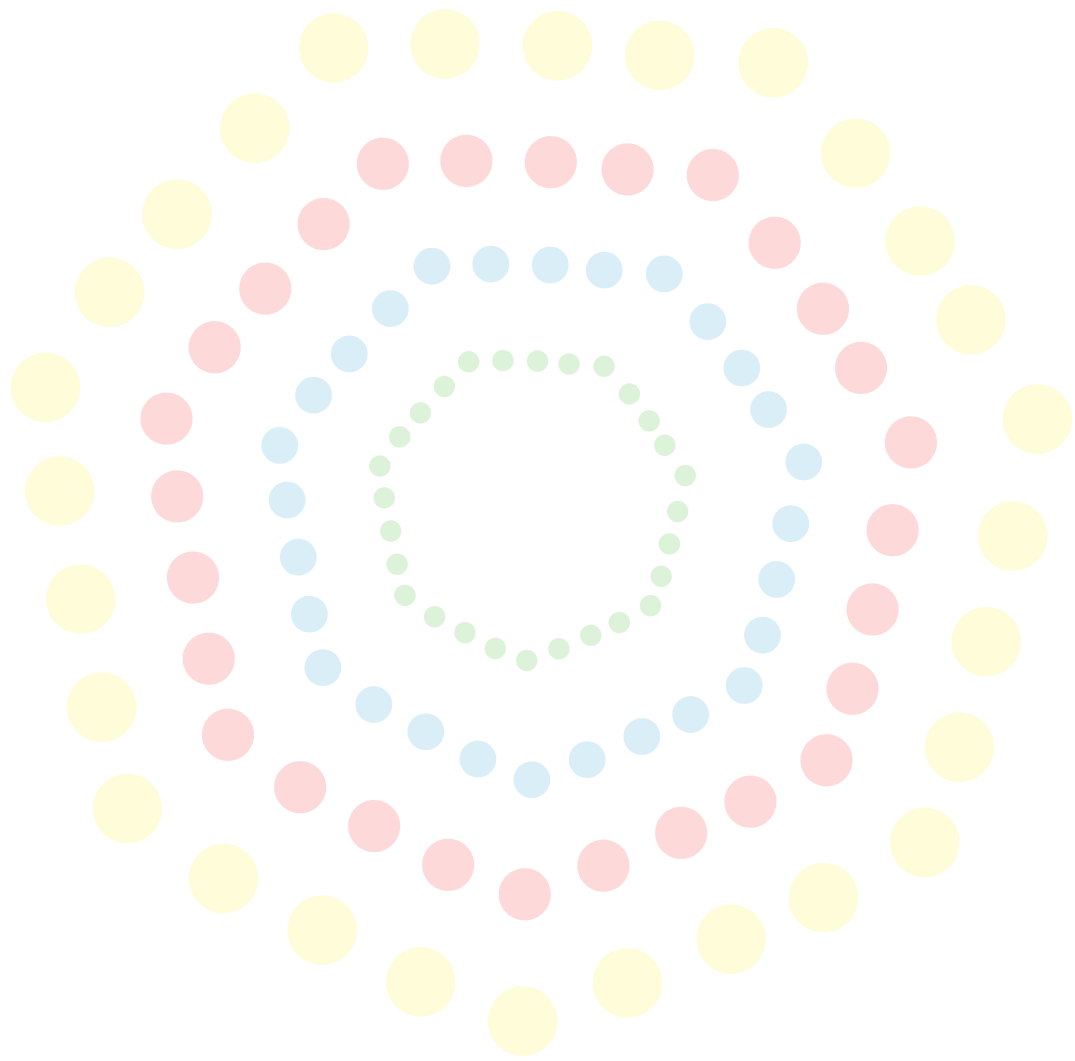
⁵⁰ That respondent described the AU's guiding narrative as an "inclusive and rights based approach".

The top three challenges facing Africa with regard to digital and data policy in our view are:

- *Capacity to implement data governance, to support institutions and to enable data flows - human capacity gap.*
- *Institutional capacity gap - not only competency, but also the existence of the very institutions themselves matters. If there is an institutional vacuum it will be filled and this might present greater challenge in getting the right thing done. Then there are the challenges of institutional silos, which prevent integrated policy and effective implementation*
- *Establishment of trust between states. Even when states have common policies and systems, they don't trust one another to share data. Trust among countries and among stakeholders is important. Regulators establish trust. Trust is essential to inclusive data economy, legitimacy is essential to creating a trusted mechanism, which includes rule of law and protection of rights. How do you establish trust? A big part of the challenge of data governance is, more generally, its governance. That requires legitimacy.*

- Dr Ralph Oyini, Director of Digital Transformation and Services, Smart Africa

To conclude, the overall view is that continental cooperation is recognized as essential for Africa to realize the benefits of the digital economy. A recurring meta-narrative is one that welcomes cross-border data flows as having the potential not only to facilitate economic integration and growth, but also to support progress towards wider achievement of the Sustainable Development Goals.



3. POSSIBLE SOLUTIONS IN AFRICA

Given the discussion on the policy context and African trends mentioned above, this chapter discusses the possible solutions for the continent to frame digital and data policies. Part I examines Africa’s need for a coordinated strategy for data infrastructure. While data center infrastructure is a requisite for successfully using data for development, the continent must also ensure a reliable power supply and high-speed data connection. Part II analyzes the need for harmonized legal standards. The sentiment is that the African Continental Free Trade Area presents the opportunity to create a digital single market through cross-border harmonization, in which data flows will enable economic development. There is also a need to generate harmonization around human rights to create a trusted and functional data environment. While the research has inferred that cross-border data flows are beneficial for sustainable development (although ensuring personal data privacy) data localization was highlighted as a restriction towards free data flow.

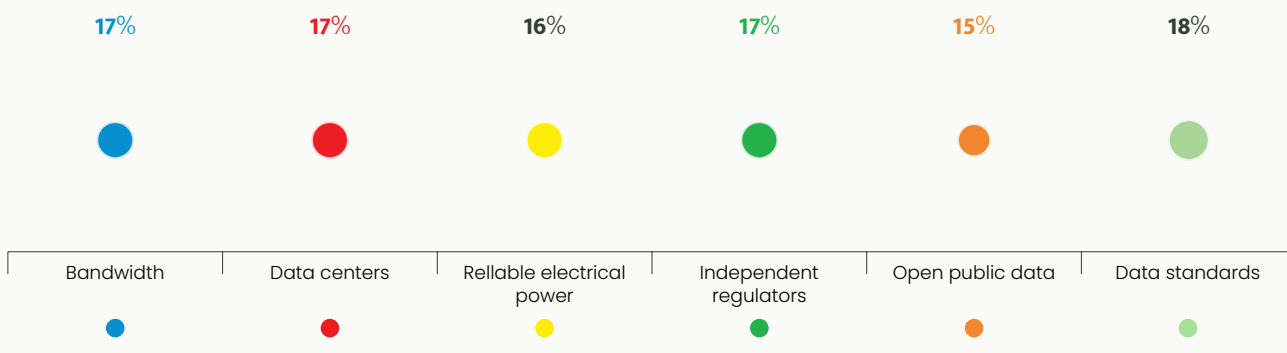
I. DEVELOPING SHARED INFRASTRUCTURE

In Agenda 2063, under Goal number 72 (the adoption clause) paragraph (g), the AU re-emphasizes the commitment to interconnect inland and island states in Africa through world-class infrastructure. To this end, the Agenda pushes to finance and implement infrastructure projects in key areas such as transport, energy and ICT. With emphasis on ICT, the goal is to erect infrastructure, “which will put the continent on equal footing with the rest of the world as an information society, an integrated e-economy where every government, business and citizen has access to reliable and affordable ICT services.”⁵¹

As part of the actionable items listed by the DTSA, the need to establish data center infrastructure is designed to host mission critical servers and computer systems to support the development of a local digital ecosystem, as well as promote infrastructure sharing as mentioned.

Figure 16

What are the factors that must be in place for the successful use of data for development



⁵¹ This will be done by increasing broadband penetration by 10% by 2018, broadband connectivity by 20 percentage points and providing access to ICT to children in schools and venture capital to young ICT entrepreneurs and innovators and migration to digital TV broadcasting by 2016. Progress towards these goals across the continent has been uneven.

Figure 17

Countries without the prerequisites for data centres such as capital, suitable climate, reliable electrical power, high-speed data connections and the like should partner with other African countries to efficiently create a continental data infrastructure.

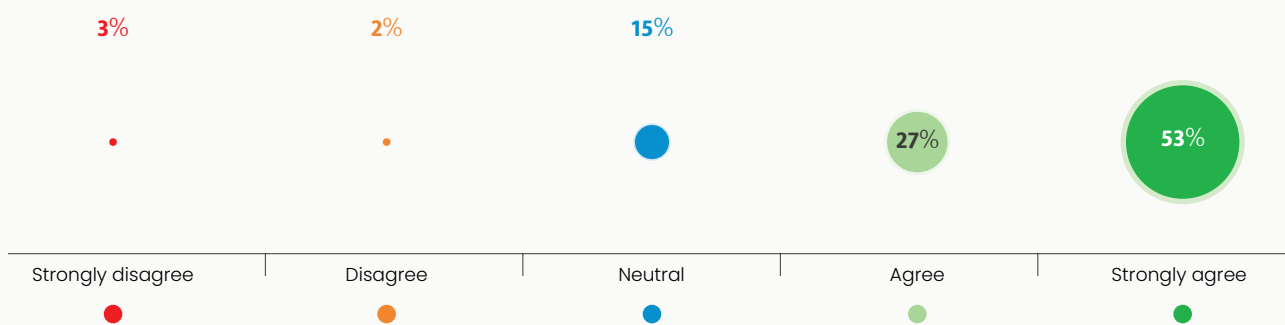
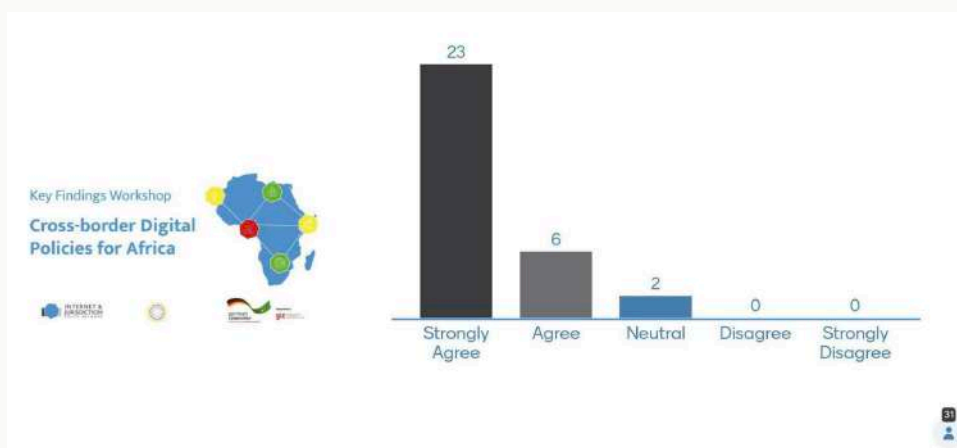


Figure 18

Africa needs a coordinated strategy around its data infrastructure (in particular data centers) / Menti poll



II. HARMONIZED LEGAL STANDARDS

Section C of the DTSA addresses the specific objectives necessary to drive digital transformation. It states that, by 2030, the DTSA aims to build a secured Digital Single Market in Africa where free movement of persons, services and capital is ensured and individuals and businesses can seamlessly access and engage in online activities in line with AfCFTA. To this end, the strategy emphasizes the need to harmonize policies, legislation and regulations, and establish and improve digital networks and services with a view to strengthening intra-Africa trade, intra-investment and capital flows and the socio-economic integration of the continent, while maintaining a relational balance with other continents in the context of networked economies. The DTSA, under the auspices of developing an enabling environment, emphasizes the need to develop a framework with Implementing Acts for interoperability and levels of assurance guided by principles of technology neutrality for cross-border service provision.

The AU Data Policy Framework encourages:

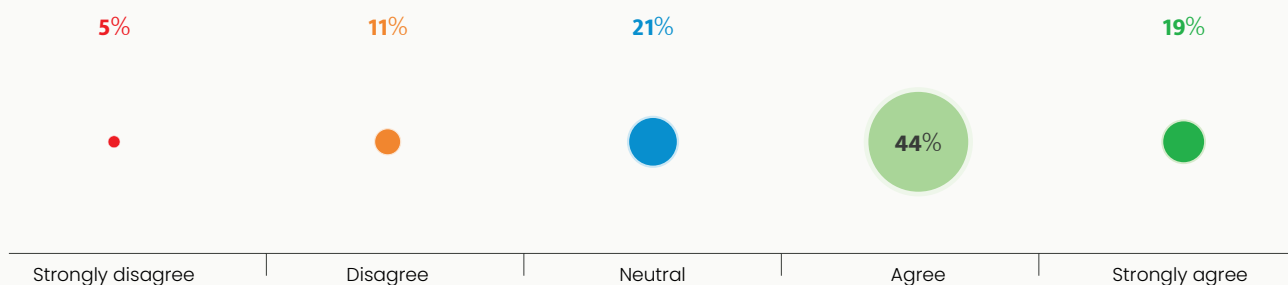
- creating co-jurisdictional frameworks for the coordination of autonomous competition, sector, and data regulators to regulate the data society and economy effectively, and to formulate, implement, and review data policy in a dynamic, forward-looking and experimental way;
- developing national legislations on personal data protection and adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment.

a. The opportunity for coordination offered by the African Continental Free Trade Area

The AfCFTA is an important potential mechanism for coordinating data policy. The following graph shows the opinions of respondents on whether the AfCFTA will lead to a digital single market.

Figure 19

African Continental Free Trade Area enables the achievement of a common digital single market in Africa.



There is optimism that a single digital market, enabled through cross-border harmonization, or at least coordination, and accompanying data flow, will enable economic development.

The majority of respondents to the online survey said that the AfCFTA would enable the continent to create a digital single market. However, some might have expected a better score for the AfCFTA and far more optimism as to the potential that the AfCFTA holds in fostering the digital single market. The AfCFTA is likely to attract cross-border investment by eliminating tariff and non-tariff barriers as well as replacing the existing patchwork of bilateral and regional trade deals with a single, unified market. However, the AfCFTA will require countries to cooperate on simplifying and harmonizing trade and transit procedures and to establish institutional structures and processes to monitor the elimination of trade barriers. A report by the World Bank forecasts that income gains from trade facilitation measures alone could amount to USD 292 billion by 2035. The same report simulates that additional income gains of up to 9% are to be reaped by 2035 if members expand the agreement to harmonize policies on digital trade, investment, competition, and IP rights. Deeper integration across these policy areas would help to build fair and efficient markets, improve competitiveness, and attract further foreign direct investment flows by reducing political and regulatory risk and raising investor confidence.⁵²

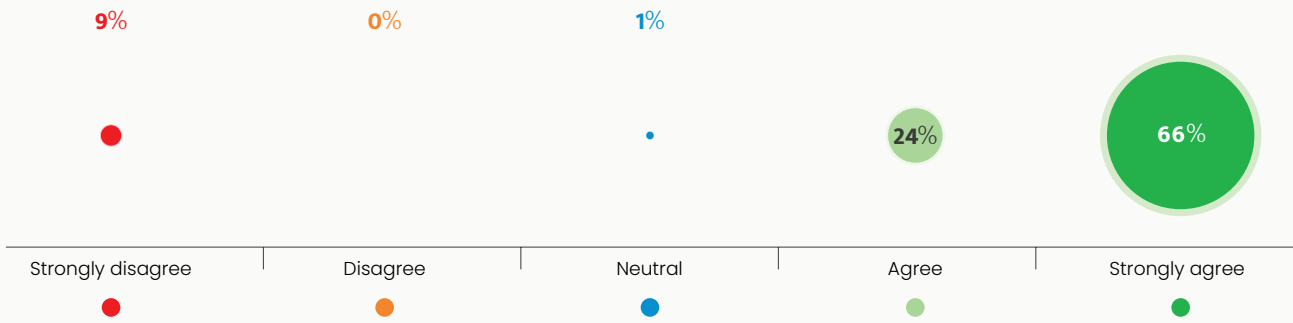
In response to a question in the online data question survey respondents supported the necessity of human rights to a trusted data environment.

⁵²World Bank, 'World Development Report 2021: Data for Better Lives'. <https://www.worldbank.org/en/publication/wdr2021>

b. NEED FOR AFRICAN COUNTRIES TO COOPERATE

Figure 20

Do African countries need to work more together on digital issues?



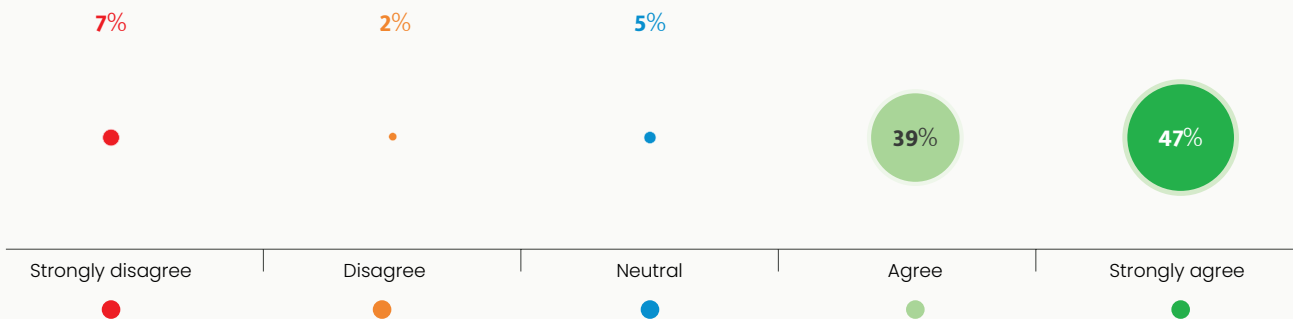
“It is important to understand that even though several countries had data protection laws as a continent today, all 54 countries are not all at the same level. They may also not be in alignment in terms of understanding or have the capacity to implement. A second issue is to understand the challenges of this for cross-border data. How can we talk about free flow of information when each country has its own data protection act?”

When we are talking about data we need to think about data sovereignty. It is unfortunately the case that most of the digital platforms that we use are private sector only and even more so foreign-based companies, and there are issues of the social responsibility of those companies. There is a need for African states to be capacitated to understand how they can govern data to make sure that all the data stored by these companies is not abused. Government officials need to be capacitated at a level where they are able to understand the loopholes, especially because of the issues of data ownership and data sovereignty. The people themselves need to be aware and know that when they give out data how it is going to be used.”

- Senior governmental representative during the interview-based data collection phase of this Report

Figure 21

African countries need to work together to regulate data.



⁵³ In the Menti poll, 18 out of 26 respondents “disagreed”, including 4 who “strongly disagreed” with the proposition that African states strongly coordinated their actions on data policy issues. In other words, 69% of the respondents disagreed with that proposition.

Fourteen respondents agreed with the proposition; the remaining 17 deciding to remain “neutral”. Of the 14 who agreed with the proposition, two “strongly agreed”. One respondent pointed to the IGF as a place where people hold conferences to talk about Internet governance, but the respondent did not identify or provide examples of solutions or coordinated actions. Similarly, four respondents⁵⁵ referred to sub-regional and regional institutions (for instance, the regional IGF) as places where states do or could engage in “some coordination”⁵⁶ by workshopping or discussing common issues. One member of that group went as far as claiming that coordination only occurs in digital policy seminars and forums such as the AfIGF.

In fact, the majority of those who agreed with the proposition relied on regional or sub-regional institutions, especially the AfIGF, as convincing evidence of coordination among countries in Africa. One of the respondents who “strongly agreed” with the proposition presented this coordination in glowing terms:

“ Looking at the organization of the IGF one can strongly see how the African countries are coming together in order to harmonize the digital policies. Networking that is taking place in terms of digitization is marvelous. The countries have organized themselves to harmonize Internet governance in their respective countries.”

In praising inter-African coordination, this respondent described it as involving “marvelous” networking and organized harmonization of Internet governance in national jurisdictions.

Another respondent agreed with the proposition by mentioning the many references to vision 2063 and in the many conferences that aim at “making Africa talk the same language on digital policy issues”. Another respondent said that African countries coordinated their actions since they can trade in ICTs and they often follow the same principles on, for example, the use of fiber transmissions, security and networks.

Interestingly, while agreeing with the proposition in the question one respondent affirmed that “just a few countries” were involved in coordination. Some respondents provided reasons for disagreeing with the proposition. Among others, they explained that they disagreed because the ability of people to access digital services across and within countries in Africa varies greatly. One respondent said that people access digital services at a higher cost and only the top 20% of the population of Malawi can access it, as in affording to pay for those services.

⁵⁴ Note that although it indicated 54 questions, the Zoho online platform only displayed 50 questions, including three questions with no substance.

⁵⁵ This respondent nuanced this coordination by clarifying that regional organizations (for example, EACO, CRASA, and WATRA) focus on different aspects of digital policy issues.

⁵⁶ One of those respondents also notes that coordination needs to be reinforced.

c. CROSS-BORDER DATA FLOW

The aforementioned AU Data Policy Framework sets a number of objectives to create the most value from data for sustainable development:

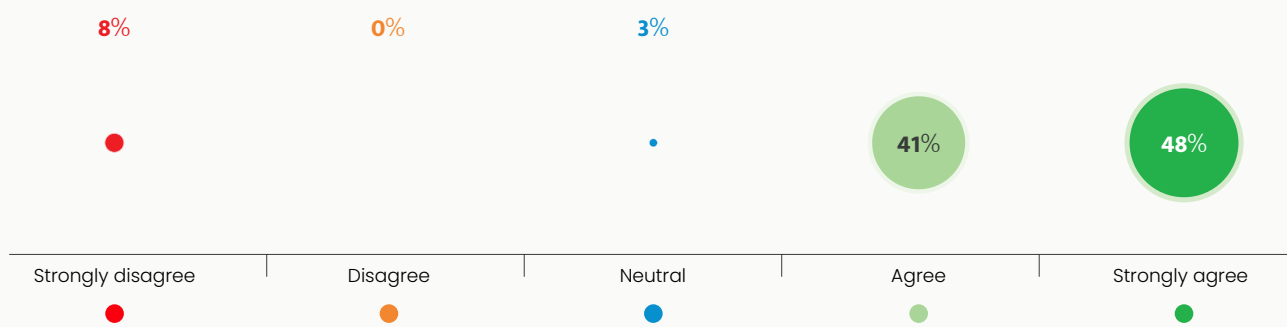
- foster and facilitate cross-border data flows and increase business opportunities while ensuring an adequate level of personal data and privacy;
- establish collaborative trust mechanisms to allow for data to circulate as freely as possible between Member States while preserving the sovereignty of Member States and their ability to regulate the digital economy. [This to] enable states, the private sector, civil society and intergovernmental organizations to coordinate their efforts on data issues across the continent to realize a single digital market and compete more effectively in the global economy;
- cooperatively enable data to flow on the continent while safeguarding human rights;
- promote data portability so that data subjects are not locked into a single provider and, in so doing, promote competition and consumer choice and enable gig workers to move between platforms.

The Framework further recommends that the African Union Commission, RECs and Regional Institutions promote and facilitate data flows within and among AU Member States by developing a Cross-Border Data Flows Mechanism that takes into account the different levels of digital readiness, data maturity, and the legal and regulatory environments of countries. Facilitating data circulation across sectors and across borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security is also necessary.

The vast majority of respondents to the online data collection process agreed that data flow is beneficial.

Figure 22

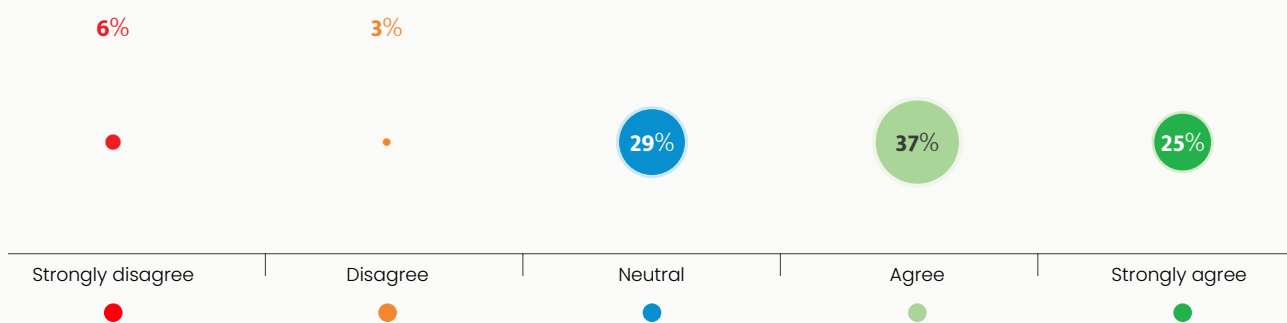
Data flows are beneficial



The majority of respondents who found data flow beneficial also regarded data localization as inhibiting data flow. Somewhat surprisingly several respondents disagreed with the trite proposition, as shown in the following graph.

Figure 23

Data localization lacks support

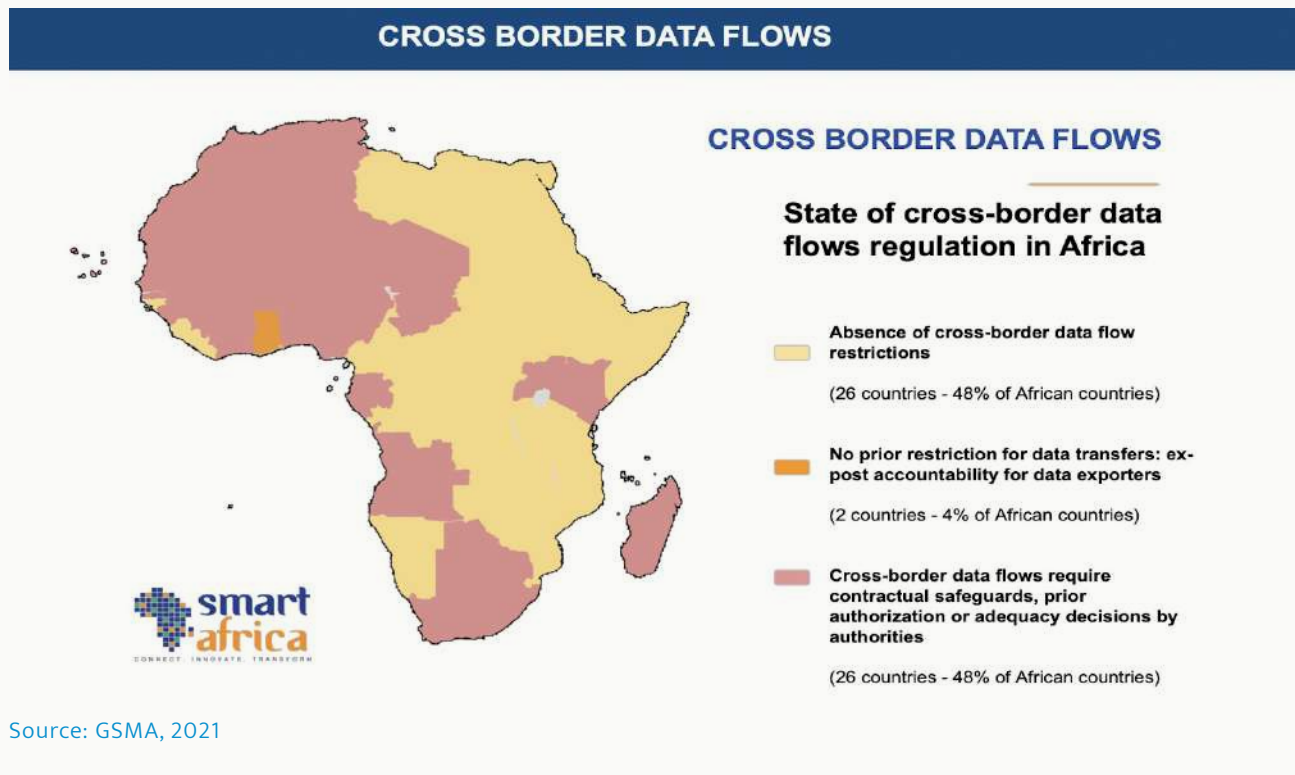


With respect to sub-regional standards on cross-border data flows, Article 36 of the ECOWAS Supplementary Act provides for similar conditional requirements for data transfers like the Convention. The ECOWAS is currently made up of fifteen member countries. However, while the Convention, in referring to cross-border data transfers, means non-African countries, the ECOWAS Supplementary Act, when also referring to cross-border transfers, points to non-ECOWAS countries that include African countries.

The SADC is made up of sixteen member countries and it has a Model Law on data protection. The SADC Model Law also provides for cross-border data transfers and it is not binding on member states. The Model Law divides cross-border data transfers into two categories of countries, that is, those who adopt the Law and those who do not. Article 43(1) of the Law provides for cross-border data transfers for countries that adopt the Law and such data will only be transferred to the recipient in compliance with the local laws in the applicable national jurisdiction. Article 44 provides for cross-border data transfers for countries that do not have a national data protection. It further states that such transfer must ensure adequate level of protection of freedoms. Articles 44(1)(b) and 45 provide for what would qualify as adequate levels of protection and what would not.

At the national level, according to [GSMA](#), 26 African countries do not have any form of data transfer regimes when it comes to cross-border data flows while 26 countries have some form of conditional transfer regimes that range between requirements for contractual safeguards, prior authorization or adequacy decisions by national data protection authorities. Only two countries have an open data transfer regime in the region (GSMA, 2021).

Figure 24



d. MUTUAL PROTECTION OF PERSONAL DATA

Instruments such as the DTSA emphasize the necessity to design and put into effect data protection and privacy policy and regulations in accordance with the Malabo Convention, keeping with the notion of creating an enabling environment.

The AU Data Policy Framework, on the other hand, makes recommendations and emphasizes the need to ensure data protection, upholding security and ensuring equitable sharing of the benefits. Data protection frameworks should also provide minimum standards for cross-border data flows. The establishment of norms and standards should expressly ensure reciprocity as a central principle for permitting cross-border flows.

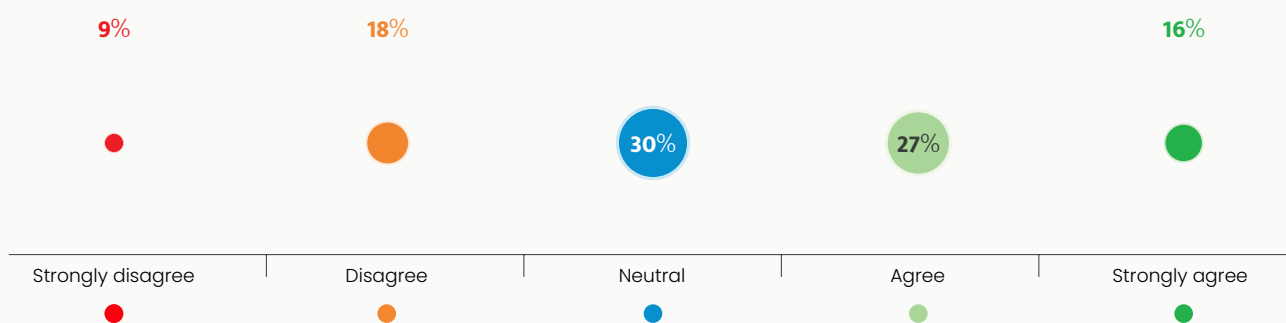
e. AFRICA-WIDE STANDARDS FOR NON-PERSONAL DATA

The DTSA also notes that it is necessary to develop regulation aimed at enabling the free flow of non-personal data. The AU Data Policy Framework deals in more detail with non-personal data. According to the Framework, data governance should include data portability rights for non-personal data to facilitate switching by customers of cloud services and digital platforms. It also recommends that “the negotiation of the competition chapter of the AfCFTA should set minimum standards to ensure that putatively proprietary non-personal data become accessible to innovators, entrepreneurs, and others in the value chain to encourage competition across the continent.”

The survey respondents overwhelmingly agreed (upwards of 80%) that African countries need to work together to regulate data, with a substantial minority of the respondents strongly endorsing this statement. The respondents accepted several reasons for such collaboration, but the one reason most preferred was its (the collaboration) capability to yield economic benefits to all countries, or rather, Africa as a continent. Seven out of ten respondents said that this collaboration would also create a unified regulatory environment to provide certainty for investment.

Figure 25

Africa has the right continental institutions to address cross-border legal challenges on the Internet.



f. OPEN DATA

The concept of ‘open data’ can best be understood to encompass instances in which anyone can freely access, use, modify, and share data for any purpose. Such access is subject, at most, to requirements that preserve provenance and openness.⁵⁷ Often, open data is necessitated by the use of open standards which are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus-driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T).

The adoption of open data regimes ought to be complemented by the capacity to collect, store and move data securely and efficiently. Derivative documents of Agenda 2063 such as the AU Continental Education Strategy for Africa (CESA) emphasize this. CESA aims to reorient Africa’s education and training systems to meet the knowledge, competencies, skills, innovation and creativity required to nurture Africa's core values and promote sustainable development at the national, sub-regional and continental levels.⁵⁸ The key strategic objective (SO) of CESA that is of relevance in this context is SO 11, which emphasizes:

The need to build and enhance capacity for data collection, management, analysis, communication, and improve the management of the education system as well as the statistical tool, through capacity building for data collection, management, analysis, communication, and usage.

g. COMMUNAL DATA GOVERNANCE

Contemporary technological advancements often outpace relevant regulations. In the African context, the same is true. But in addition to having out-of-date laws, Africa also has a widespread issue with digital illiteracy, and the lack of local language instructions and terms and conditions online. Together, these two indicate that new methods of digital governance are required. The adoption of two approaches has come to the fore to address these issues: data communities and data trusts.

⁵⁷ ‘The Open Definition - Open Definition - Defining Open in Open Data, Open Content and Open Knowledge’, 14 May 2014, <https://opendefinition.org/>.

⁵⁸ ‘CESA | AU Education’, accessed 29 September 2022, <https://www.edu-au.org/cesa/>.

While in certain contexts the above-mentioned terms are used interchangeably, they, for the purpose of this Report, share little but distinct difference.

Data trust or stewardship in this context refers to a legally enforced governance structure wherein members pool their personal data and entrust a data trustee or trustees. Such a trustee must have a fiduciary responsibility to act in the best interests of the members of the trust, so as to determine how this data is to be used and managed.⁵⁹ With significant numbers of people digitally and otherwise illiterate in Africa, digital mechanisms of informed consent may not be sufficient to protect the rights of people. There is a risk that the digital means of obtaining consent, such as selecting a button linked to a lengthy legal set of terms, does not actually amount to informed consent. This is because the action that is meant to constitute consent may not be an informed act or understood at all by the person doing it. Thus, data trusts are emerging globally and ensure that the rights of people over their data are upheld with the underlying idea being to promote the management of data in ways that benefit those from whom data is collected.⁶⁰

On the other hand, data communities in this context refer to a situation where communities gather people with varying degrees of digital literacy, to collaborate around common interests and goals that involve using, manipulating, or processing data in some way. The members can discuss projects, request or provide help, exchange ideas or share resources in real-time. Thus, in light of the unique socio-economic conditions in Africa, data trusts have been gaining popularity, especially among the less digitally literate populace. In the same vein, data communities have gained traction largely owing to the different levels of digital infrastructure development across the continent. Data communities in particular have been cited as instrumental vehicles to aid in the achievement of a number of Agenda 2063 goals where collaboration and data sharing are important for shared prosperity.

In light of the above, there has been a call to prioritize community data governance in innovation policy. These communities and trusts require domestic policy incentives and support, including the active promotion of data hubs and other forms of community innovation that can help engender data competencies and data cultures, as civil society actors should do more broadly.

However, there are also certain contextual limitations when it comes to the efficacy of communal based governance. For instance, in Africa, a number of communities live under customary legal systems, where disputes and grievances are handled by traditional community-led processes while the legal system of data protection and trust laws is neither the proffered nor common means by which many African individuals and communities seek refuge from the exploitation of power or to resolve their issues. Furthermore, the ties with historical colonialism where local and indigenous populations were exploited under the pretense of the colonial trustees of their land and personage acting in their best interest cannot be forgotten. Neither can the role of the legal order in legitimizing these practices and forms of governance be forgotten.⁶¹ Thus, building trust in these communal based forms of data governance is also currently a priority.

⁵⁹ Rachel Adams and Nokuthula Olorunju, 'African Data Trusts: New Tools Towards Collective Data Governance?', Research ICT Africa, 31 August 2022, <https://researchictafrica.net/publication/african-data-trusts-new-tools-towards-collective-data-governance/>.

⁶⁰ Adams and Olorunju.

⁶¹ Adams and Olorunju.

h. EXPERIMENTATION THROUGH CROSS-BORDER SANDBOXES FOR DATA

The framing question on what concrete paths could be undertaken toward policy harmonization also calls for flexible approaches toward progressive convergence. One such approach could be to explore innovative ways to encourage responsible data sharing and to leverage the expertise and know-how of existing local communities and communities of practice. As previously laid out in this Report, the complex challenges brought by data require innovative, collaborative and agile governance mechanisms to address them. The emerging concept of cross-border sandboxes for data can be such mechanisms and could allow for a way to “test the waters”.

Data is created, collected, stored, processed, accessed, used, shared, and destroyed in numerous geographic locations. Yet, discourse about data tends to focus on only a few of these components: its storage location, processing, and sharing. In a context where cloud services have proliferated worldwide, the actual location of data can be hard to determine, sometimes by design. Indeed, not only is data moved almost at the speed of light (at least in fiber) along its processing workflow, but also it can be replicated in diverse locations for reasons of security (e.g., geo-redundancy and infrastructure resilience) or efficiency (e.g., speed of delivery and specialization of networks, such as content delivery networks). It can also be split into many different and distributed pieces (e.g., sharding) to facilitate processing.⁶² The rapid and complex movement of data between countries, and the growth of innovative business models that take advantage of this, can bring regulatory complexity. Innovators may face many overlapping applicable laws, creating uncertainty about compliance. Governments may respond to concerns about the rapid movement and international processing of data with measures, such as data localization, which can unnecessarily curtail data’s broad social and economic benefits.

Sandboxes vary according to the flexibility or leeway permitted by regulators, how directly the findings are used to shape or inform future laws, and if any incentives are offered to innovators to participate. These differences are shaped by each national regulator’s legal and cultural environment. Sandboxes also vary in goals, scope, and scale. Due to the varying goals, scope, and scale (as well as degrees of regulatory leeway, the direct impact of regulatory discovery, and availability of incentives for firms to participate), it follows then that costs, benefits, and risks vary along with different types of regulatory sandboxes.

Sandboxes are not physical spaces. They are a collaborative process through which technological innovations, new business processes and models, and the impact of regulations are explored with regulators working with various interested stakeholders. There are two core types of sandboxes:

Regulatory sandboxes are time-limited collaborative endeavors involving regulators, service providers and other relevant stakeholders to test innovative technology and data practices against regulatory frameworks. They have a potential use anywhere innovation is hampered by uncertainty about how regulation applies or where regulation is emerging, and risks are not fully understood. These sandboxes may even help to level the playing field between established and emerging players, by providing a structured and low-risk way to test out challenging new ideas that would otherwise need significant institutional backing before they could even contemplate market entry. They were first used by financial regulators that adapted the software testing environment of sandboxes to create closed environments where new ‘fintech’ is tested, both to check compliance with regulations and, in some jurisdictions,

⁶² De La Chapelle, B. and L. Porciuncula (2021), We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty, Internet & Jurisdiction Policy Network

to investigate if the regulations themselves needed to be updated. The sandbox settings ensure that the risks are contained to consumers or the financial system.

Operational sandboxes are secure, collaborative data-spaces that pool data sets and resources together. They are hosted by one entity and accessed by several others, to serve new combinations and uses of data. They can be created by regulators or government agencies to test capabilities on actual data sets or by a coalition of actors to pool resources together, sometimes through technologically enabled decentralized approaches (e.g., data collaboratives, fiduciaries, and commons), in order to explore or encourage their use.

Thus, broadly speaking, for data, **operational sandboxes** are testing environments where hosted data can be accessed and used, while **regulatory sandboxes** are collaborative processes where regulators and firms evaluate new technologies within a regulatory framework. More succinctly, operational sandboxes actually handle data, and regulatory sandboxes provide dialogue and guidance on how data are handled.⁶³

Regulatory sandboxes for data have been used by regulators in the United Kingdom, Norway, Canada, Singapore, Colombia, and several other countries. So far, they have all focused on applying national regulations within each regulator's jurisdiction. While several issues need to be resolved to make them work, cross-border regulatory sandboxes have significant potential to address barriers to international data flows, particularly regulatory uncertainty between jurisdictions and challenges that require multi-disciplinary collaboration.⁶⁴

African cross-border sandboxes could have the potential to improve regulatory capacity-building and cooperation across borders, increase innovation, competition and choice in many markets, enhance compliance and reduce regulatory arbitrage, and make data more available and accessible across borders and sectors. They can enable data flows, innovation and trade for various sectors, including health, mobility and biodiversity genomics, where sandboxes could be used to tackle friction and bottlenecks. Cross-border sandboxes for data can address challenges by using careful design and issue identification and definition, choice of regulatory partners, stakeholder engagement and active management of information asymmetry and risk. Cross-sectoral innovations – emerging intermediaries, privacy enhancing technologies (PETs) and browser-based consent management – can support cross-border sandboxes so that this mechanism responsibly unlocks the value of data and helps to accelerate the SDG implementation by governments and any other non-state actors.

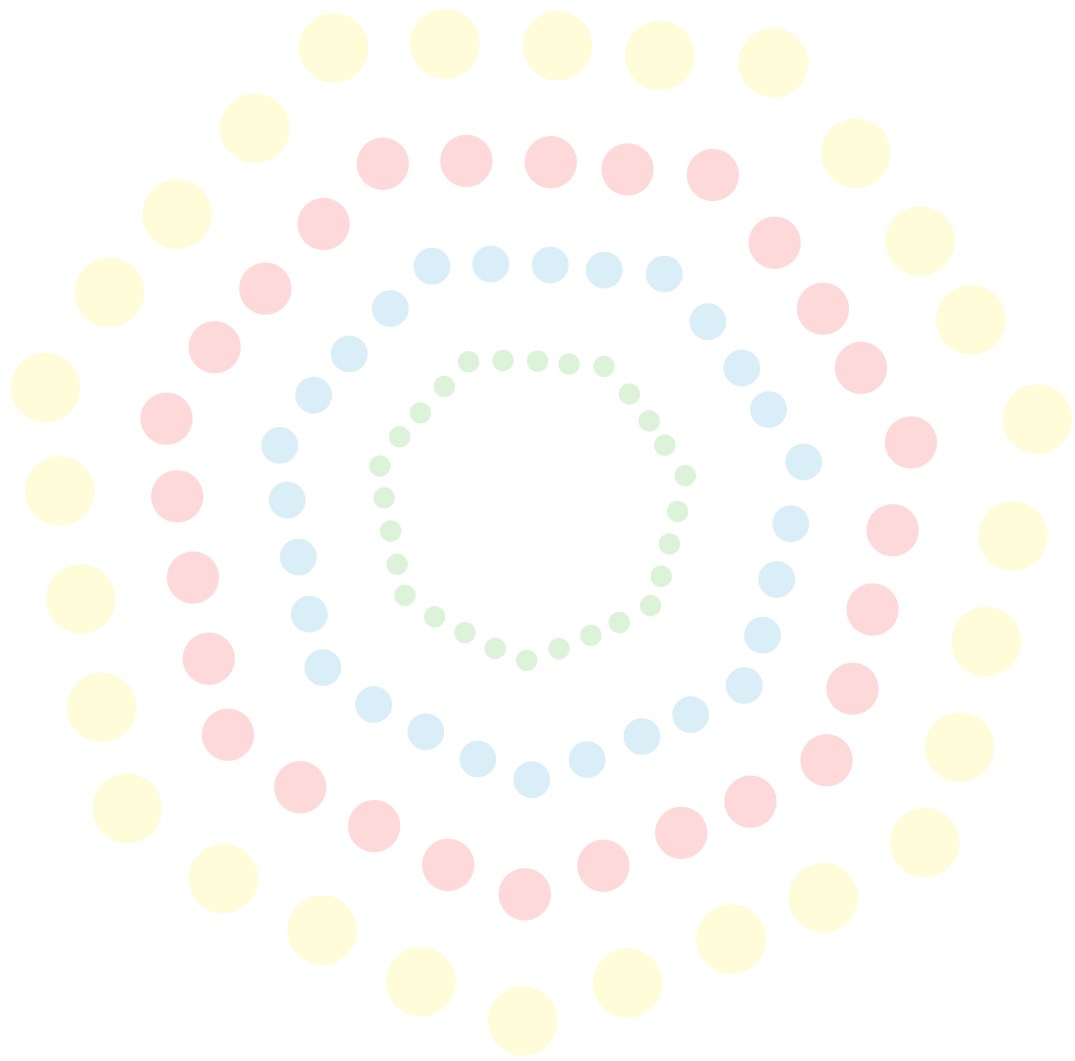
⁶³ Datasphere Initiative (2022), 'Sandboxes for data: creating spaces for agile solutions across borders', <https://www.thedatasphere.org/>

⁶⁴ BMWi (2019), 'Making Space for Innovation: The handbook for regulatory sandboxes', Federal Ministry for Economic Affairs and Energy, Germany.

For a who's who of some of the key organizations working on global data governance solutions in Africa, the Datasphere Governance Atlas (April 2022) provides an important preliminary mapping of the landscape, supporting the identification of silos and the work towards bridging those silos to better understand the dynamics and interdependencies of numerous initiatives working on data policy. In this exercise, the Datasphere Initiative identified various organizations that work with some aspect of data governance that are either headquartered in Africa or elsewhere with specific missions and projects focused on African challenges. In addition to the 28 organizations identified, the Atlas mapped 113 global organizations that, despite not having a specific focus on African challenges, might somehow impact the discussions in the region through their work.

The Atlas also mapped 41 international multilateral organizations. While the main focus of most intergovernmental organizations (IGOs) – organizations composed of governments and created by treaties – is not on data or data governance, IGOs are increasingly understanding the power of data to support better real-world interventions to advance their missions and commitments to the SDGs. Because of their nature and agenda, IGOs work in regions such as Africa and their work can directly impact the region. They could thus be considered as part of the relevant organizations working on data governance in the region.

Examples of organizations from the Datasphere Governance Atlas headquartered or working in Africa are listed – in a non-exhaustive manner – in the Annex B: Key organizations working on global data governance solutions in Africa.



MOVING FORWARD

The investigation of this Report took us through the African Policy Context, current Topical Trends on the continent, and possible solutions to cooperate on digital policy across borders. It is important to note that the findings of this Report are non-exhaustive, notwithstanding the observed complexity and interdependencies of the challenges described.

A recurring observation during the consultation process in preparation for this Report was the perceived underrepresentation of African stakeholders in many global governance or international negotiation fora, certainly from agenda setting and generally, from the perspective of leadership at the member state level. Within the context of the Agenda 2063, the Digital Transformation Strategy and the commitment to a digital single market, the African Continental Free Trade Area, and the recognition of the need for harmonization in these foundational frameworks, a coherent and recognizable African position will need to emerge. Such African position will be one that reflects the diverse interests of unevenly developed countries, whose strength lay in unity and collective action and the creation of policy and regulatory conditions that contribute to the integration of African (data) markets and digital systems that would enable them to operate and compete internationally as a more effective bloc.

As stated in its Digital Economy Report 2021, UNCTAD recommends that ‘Developing countries need to find the optimal balance between promoting domestic economic development, protecting public policy interests and integrating into the global digital ecosystem.’ In this context, African countries have, through the African Union policy documents, already expressed the intention of working together to identify common challenges and opportunities to be able to leverage their strengths in and outside Africa.

Focused international coordination of actors at different levels will be required, and leveraging of shared infrastructure and innovative solutions ways to further harmonize legal standards will be of utmost importance. This brings us back to the structuring questions put forward at the beginning of this Report as a contribution to the ongoing debate on cross-border digital policies in Africa:

- What path towards harmonization?
- What digital infrastructure strategy?
- How to leverage data sharing for development?
- How to strengthen the voice of Africa in the global data governance fora?

By using them to frame cross-border digital challenges with a focus on cross-border data issues, the following pathways for action and areas for further research have emerged:

EVIDENCE-BASED POLICY DEVELOPMENT

Africa needs more research to be able to influence its digital policy outlook. One of the ways of achieving such optimal balance is for the AU to coordinate and collaborate with African stakeholders on evidence-based policy development for cross-border data flows. This will include rigorous and in-depth research on topical policy issues that impact cross-border data flow in the region.

For example, it will be useful to have country-by-country and regional analyses of the legal and economic landscape of digital taxation in Africa. Not only does this have the potential to examine digital taxation as one of the issues involved with ensuring effective cross-border data flows, but also it could assist African stakeholders to see the potential of the digital economy and the need to harmonize their policies on digital taxation for regional prosperity.

IMPLEMENTING THE AU DATA POLICY FRAMEWORK INTO NATIONAL STRATEGIES

Another way of contributing to optimal balance is to implement the current AU Data Policy Framework, which addresses some of the digital policy trends highlighted above into national contexts. To implement the Framework, the AU Member States will develop national data policy plans or strategies that draw directly from the Framework, revise their existing data policies in response to the Framework, and facilitate a common front not only for Africa but also outside Africa. These strategies or plans will articulate the AU Member States' national approach to data, data use, regulation, and future while also keying into the regional needs for a vibrant digital economy.⁶⁵

Continental cooperation is increasingly recognized as essential for Africa to realize the benefits of the digital economy. Cross-border data flows have the potential not only to enable economic integration, but also to support development in other ways. Together with interoperable data standards, cross-border digital policies are the basis for cooperation, enabling coordinated action and progress toward harmonization of digital policy. Datafication (to which data flows have become increasingly important), together with the analysis and use of large volumes of data, has also been recognized as a key factor in the development of Africa.

The task that lies ahead for Africa is to build a common understanding of these evolving issues and enable further knowledge sharing and stakeholder cooperation. Africa is in the process of actively shaping its digital future, and the hope is that this Report can offer a useful baseline to conduct further research and actions to support evidence-based policy-making. In this complex landscape, many different issues need attention; Data governance is the next, most important frontier of digital policies – because it underpins everything – and it is becoming a major theme within cross-border digital policymaking.

A FRAMEWORK FOR FURTHER DEVELOPMENT

Based on the knowledge curated in this Report and the African community engaged through the collaborative methodology utilized by the Internet & Jurisdiction Policy Network, the following overview shares examples of required investigation and steps that could be used as a framework for further development. Intended to assist policymakers, they align with existing policy priorities expressed in the African Union policy documents, but also talk to the imperative of global governance to responsibly unlock the value of data for all:

⁶⁵ Rwanda currently has a [National Data Revolution Policy](#) that predates the Framework but Nigeria is currently working towards such a [policy](#) and it lists the Framework as one of its Guides.

- Should other regions carry out Impact assessments of the extraterritorial impact of their regulations to prevent unintended consequences, including for Africa?
- What interfaces with global processes are most helpful for Africa to develop further?
- Increased coordination of African countries on digital policy should be achieved through policies that can be adapted to national and regional contexts and that address cross-border issues while taking into account differences;
- Member States should progressively realize the rights-preserving enabling environment proposed in the AU Data Policy Framework to build the levels of trust needed within and among states for data to flow across the continent in support of the AfCFTA and a digital single market in Africa;
- States should develop their data standards to align with those developed through the AU to develop integrated data systems that are interoperable and that enable the flow of data across the continent;
- African countries need to cooperate to develop standards for data, and create shared public datasets for research on key issues such as urbanization, land and water use, and others that are essential for sustainable development;
- Data sovereignty, personal and national, in Africa should be realized through the reciprocal protection of personal data and continental policies to enable data flows and economic regulation that ensure the benefits of responsible data sharing for all;
- Data policies must derive from legitimate institutions and be rights-preserving in order to create a trusted environment;
- Shared data infrastructure, including data centers, should be appropriately developed where the necessary physical conditions and demand exist;
- Africa-driven peer-to-peer and internationally supported institutional capacity building and the development of specialized competencies should be sought to create, maintain and adapt institutional requirements to the dynamic and fast-changing digital environment;
- African countries should cooperate in international fora to have a common African voice, reflecting shared interests and advocating data policies that support inclusive development and that uphold both individual and collective rights.

REFERENCES

- Adams, R., & Olorunju, N. (2022, August 31). African Data Trusts: New Tools Towards Collective Data Governance? Research ICT Africa. <https://researchictafrica.net/publication/african-data-trusts-new-tools-towards-collective-data-governance/>
- African Continental Free Trade Area (AfCFTA) Legal Texts and Policy Documents—Tralac trade law centre. (n.d.). Retrieved 18 January 2022, from <https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html>
- African Union. (2019). The Digital Transformation Strategy for Africa (2020 -2030). <https://www.tralac.org/documents/resources/african-union/3013-the-digital-transformation-strategy-for-africa-2020-2030/file.html>
- African Union Commission. (2015). Agenda 2063 The Africa We Want. African Union Commission. https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf
- AU Data Policy Framework. (2022). African Union. <https://au.int/en/documents/20220728/au-data-policy-framework>
- CESA | AU Education. (n.d.). Retrieved 29 September 2022, from <https://www.edu-au.org/cesa/>
- Data Protection and Privacy Legislation Worldwide. (n.d.). UNCTAD. Retrieved 17 October 2022, from <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- Digital Economy Report 2019 | UNCTAD. (n.d.). Retrieved 6 September 2022, from <https://unctad.org/webflyer/digital-economy-report-2019>
- Nations, U. (n.d.). Big Data for Sustainable Development. United Nations; United Nations. Retrieved 28 October 2022, from <https://www.un.org/en/global-issues/big-data-for-sustainable-development>
- Spuy, A. van der. (2021, November 9). Conclusion: Assessing socio-digital identity ecosystems in Africa. Research ICT Africa. <https://researchictafrica.net/publication/conclusion-assessing-socio-digital-identity-ecosystems-in-africa/>
- Spuy, A. van der, Bhandari, V., Trikanad, S., & Paul, Y. T. (2021, November 11). Towards the Evaluation of Socio-digital ID Ecosystems in Africa: Comparative Analysis of Findings from Ten Country Case Studies. Africa Portal; Research ICT Africa. <https://www.africaportal.org/publications/towards-evaluation-socio-digital-id-ecosystems-africa-comparative-analysis-findings-ten-country-case-studies/>
- The Open Definition—Open Definition—Defining Open in Open Data, Open Content and Open Knowledge. (2014). <https://opendefinition.org/>
- UNCTAD. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].
- World Bank. (2021). World Development Report 2021: Data for Better Lives [Text/HTML]. World Bank. <https://www.worldbank.org/en/publication/wdr2021>
- World Bank, & Nations, U. (2017). Combating Cybercrime: Tools and Capacity Building for Emerging Economies [Handbook]. World Bank. <https://doi.org/10.1596/30306>
- World Development Report 2020: Trading for Development in the Age of Global Value Chains. (n.d.). [Text/HTML]. World Bank. Retrieved 20 October 2022, from <https://www.worldbank.org/en/publication/wdr2020>

ANNEX A: THE RESEARCH PROCESS

Methods

In a consultative process that gathered the expertise and insights of multiple stakeholders, the research that underpins this report proceeded in five stages:

- desk research (to review the literature, documents, and policy instruments on Africa’s cross-border data);
- knowledge dialogue workshops (to identify challenges, opinions and trends regarding cross-border data policies for Africa);
- data collection (to gather data on those challenges, opinions, and trends);
- data analysis and interpretation; and
- report writing.

I. THE KNOWLEDGE DIALOGUE WORKSHOPS

In the first stage of the process, two knowledge-sharing workshops gathered data from stakeholders about what the major cross-border data policy trends and challenges within the context of the digital economy are, and what important questions policymakers should frame and answer. The first workshop in December 2021 featured a dialogue among African stakeholders, while the second workshop, held on 22 February 2022, involved a conversation between African stakeholders and experts from Europe, the United States, and Asia. The knowledge dialogue workshops investigated fundamental issues:

- What is the status of cross-border data flows on the continent?
- In the absence of a common narrative on the data economy can a common narrative on cross-border policies be forged in the context of the new AU Data Policy Framework?
- What needs to happen to enable African governments to navigate the increasingly dynamic, complex and adaptive global communication systems so as to address our specific challenges, and respond to the growing significance of data within the context of the digital economy?

Are there any other emerging trend related to cross-border digital policies for Africa from your perspective?



Strengthening African wide institutions as AU, ECOWAS, as well as civil society

From my point of view, everything has been listed.

Copyright exceptions for data mining

I existe des tendances émergentes liées aux politiques numériques transfrontalières. Ces dernières sont tirées par les pays ayant ratifié la Convention 108 sur la protection des données.

The entrepreneurial insight is needed given the lack of inclusion of this sector towards informing digital policies

Digital infrastructure and skills.

Yes. The trend on how Africans can improve the value of their data in the global data ecosystem.

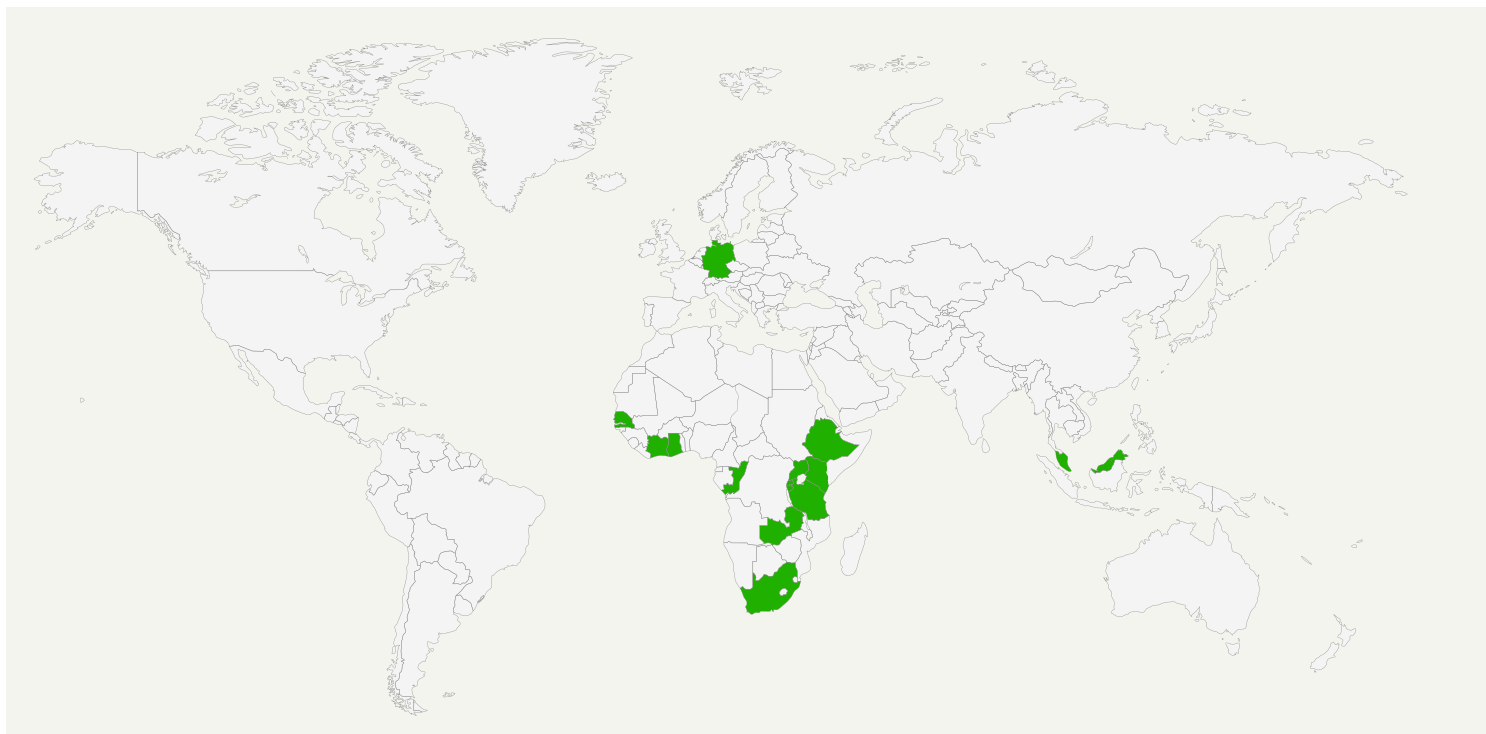
Data sovereignty

Preparing university curricula for the 4th Industrial Revolution

The impact of automation and the 4th Industrial Revolution on employment

Over 35 registrations from 14 countries (December 2021)

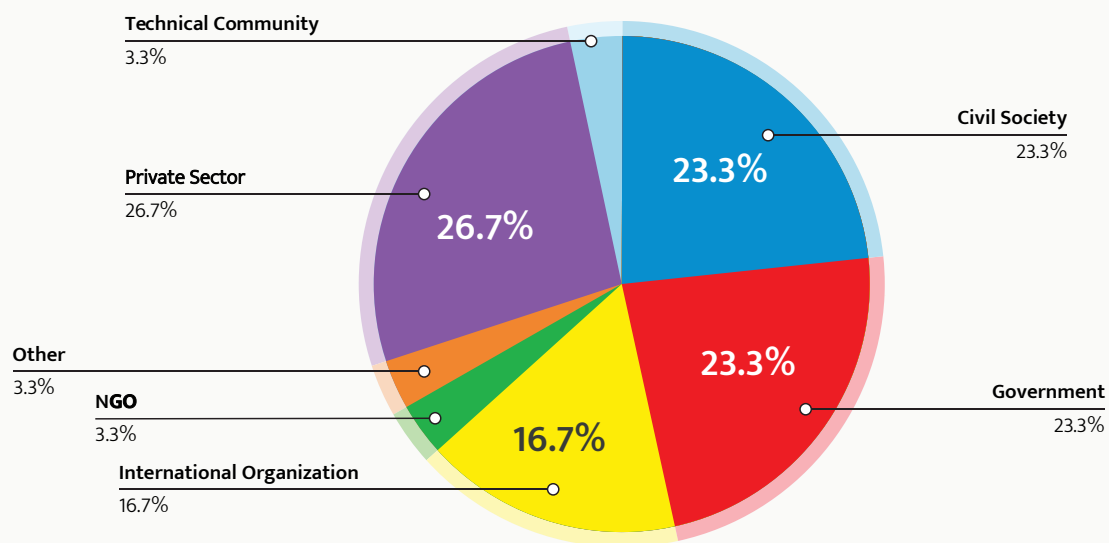
The 35 registrants for the first knowledge dialogue (December 2021) were from the countries shown in the graphic below. The bulk of people that registered were from Africa, mostly from East Africa, with a smaller number coming from Southern Africa. There were also a few European and Asian registrants.



Distribution of participants at the first knowledge dialogue workshop based on location

Stakeholder groups (December 2021 Knowledge Dialogue Workshops)

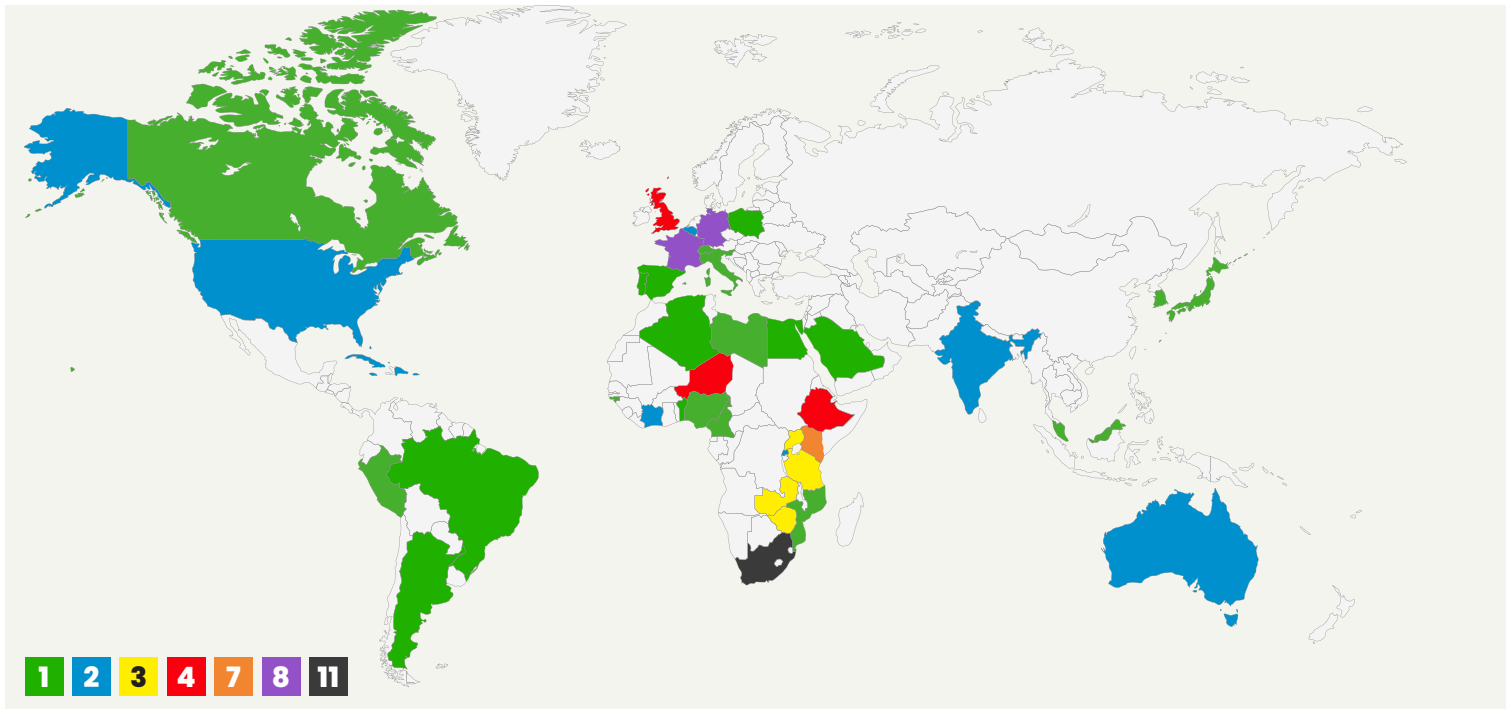
The infographic below shows the distribution of stakeholder groups present at the first knowledge dialogue in December 2021. Participants from the private sector made up the largest stakeholder group making up 26.7% of the participants while the technical community, non-profit organisations and other unspecified stakeholders had the least representation with 3.3% each.



Distribution of stakeholder groups present at the first Knowledge Dialogue Workshop

Over 100 registrations from 40 countries

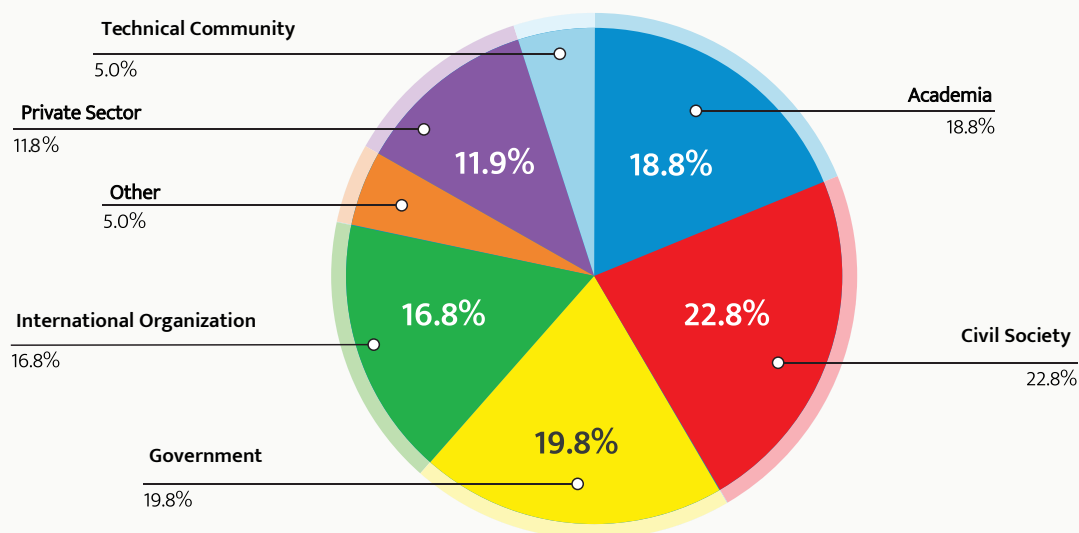
At the second knowledge dialogue workshop, over 100 registrations were recorded from over 40 countries. The second knowledge workshop saw greater participation from countries outside of Africa with North America, South America, Western Europe and Australia being present at the workshop. Likewise, participation from North and Southern Africa also improved.



Distribution of participants at the second knowledge dialogue workshop based on location

Breakdown per stakeholder group

At the second knowledge dialogue workshop, the stakeholders came from more diverse backgrounds. At this workshop, the majority of participants were from civil society organisations (22.8%). A noticeable uptake was also noted with stakeholders from academia who were the third most active participants behind civil society and government respectively. Regrettably though, the technical community and others remained underrepresented making up only 5% of present participants.



Distribution of stakeholder groups present at the second Knowledge Dialogue Workshop

II. THE LAUNCH OF THE DATA COLLECTION PHASE

a. THE MENTI ONLINE POLL AT THE AFIGF IN MALAWI

The 24 respondents who took part in the Menti online poll conducted during the AfIGF in Malawi were divided on whether or not the African continent had any narratives for its data policy instruments. The majority suggested that there are important narratives. The minority view (i.e., two respondents out of 24)⁶⁶ maintained that the continent has no such narrative. Three respondents attributed this absence of narrative to (a lack of) coordination or implementation.⁶⁷ Two other respondents singled out shortcomings, one lamenting the lack of political will in endorsing data policy instruments; the other the lack of necessary legal framework. But it was not clear whether the respondents simply deplored the low degree of policy-making or political commitment, or whether the lack of policies or political will itself constituted a key narrative.

On the other hand, most respondents identified master narratives, ranging from data through national priorities to continent-wide goals. First, some respondents linked the key narratives behind the data policy instruments of the AU to data. Thus, they used phrases such as “data justice”, “data for development”, “data protection”, data localization,⁶⁸ “data integrity”, (more equitable) data flows, data collection, and “datafication processes”. With regard to the latter concept, the respondent in question spoke about “harvesting the potential of datafication processes while avoiding their pitfalls. In sum, for this group, the narratives behind the AU’s data policies consist of recognizing and raising the value of data.

⁶⁶ Whereas the one respondent made it clear that Africa does not have any key data-policy narrative because of lacking coordination, the other respondent simply said that the continent has not yet built the “necessary legal framework”. We could not therefore tell for sure whether two respondents or only one respondent maintained that the AU lacks a guiding data-policy narrative.

⁶⁷ One of them called for (more) coordination. More importantly, note that four respondents invoked coordination or implementation, though one of them nonetheless expressed his idea of the AU’s chief narrative, despite his comments on inadequate implementation.

⁶⁸ Two respondents put forth this concept.

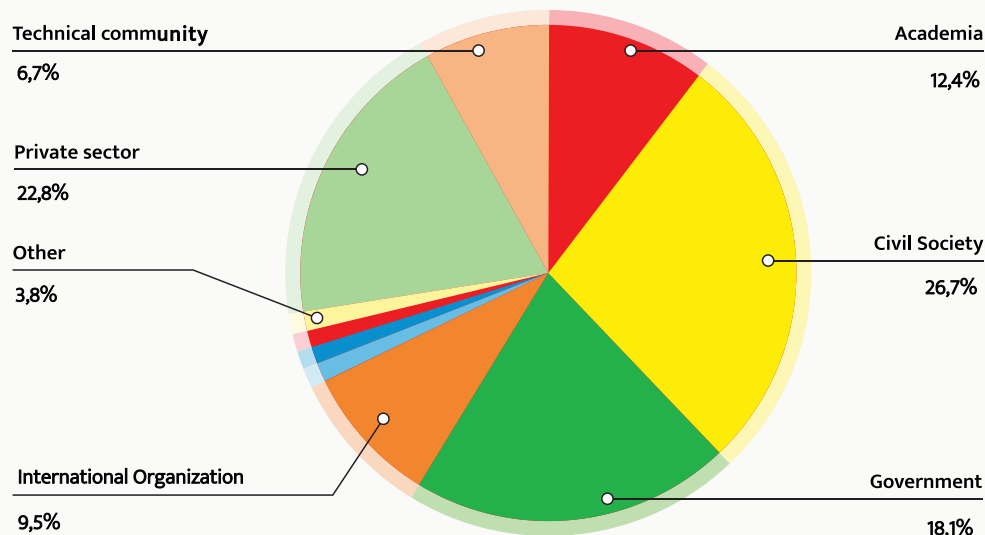
Others defined these narratives by (the extent to which they align with) national priorities, such as upskilling, infrastructure development or “incountry [sic] bureaucracy”, though it is not clear as to how the latter priority (i.e., bureaucracy) pertains to cross-border data policies. (Also unclear, respondents did not specify whether or not they intended to classify the priorities of upskilling and infrastructure development as either domestic or cross-border goals, or both.

More importantly, a number of respondents related the data-policy narratives to continental goals. For example, one respondent stated that the key narrative behind the AU’s data policy instruments was the African single market as a long-term goal. Others cited the harmonization of laws, economic integration, and the promotion of e-commerce and digital trade. One emphasized African-centeredness whereas two respondents perceived the AU’s data-policy narrative as consolidating the continent’s voice and influencing global data governance.

Apart from these distinct groups, three respondents criticized the key narratives. Notably, they qualified the narratives as “disjointed” and “tick box exercises” while decrying “too much influence of EU regulations” on data policy.

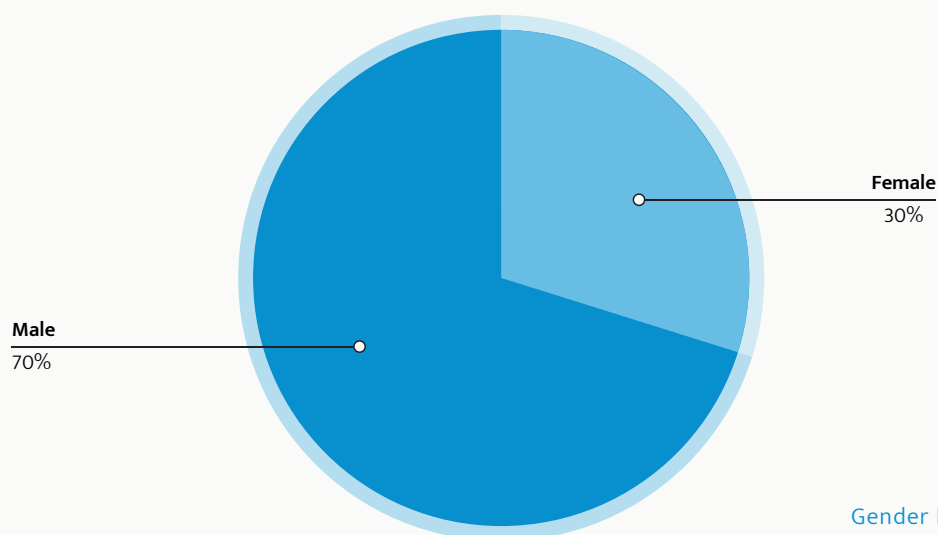
III. DATA COLLECTION

The next stage involved an online data-gathering process. This stage employed two quantitative methods: questionnaires and structured interviews. The online questionnaire sought to capture the concerns of stakeholders on data policy, the benefits and challenges of cross-border coordination, and how these issues fit into an emerging continental narrative. The online data collection included questions that could be represented graphically and open ended questions.



Stakeholder Representation

A large proportion of the respondents were male. While the respondents were self selecting so that the ratio is not indicative of the demographics of any particular community the gender imbalance is cause for concern.



Gender Representation

a. DESK RESEARCH

The knowledge dialogue workshops, data collection and high level interviews were combined with desk research focused on policy instruments, and government and intergovernmental reports to inform a report designed to be immediately useful to policy makers.

b. HIGH-LEVEL INTERVIEWS

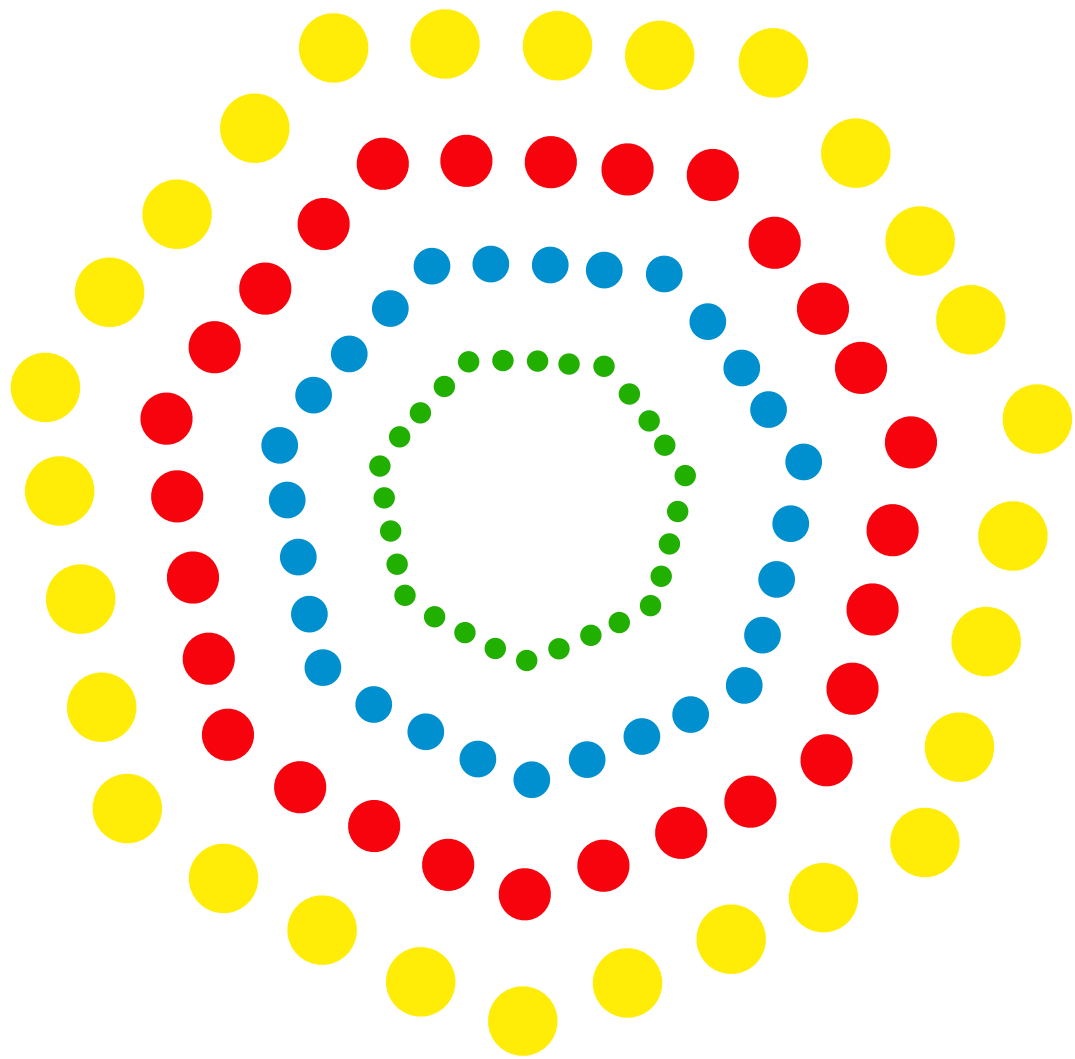
Interviews with government, intergovernmental and non-profit leaders yielded important insights. They were complemented by observations made during the Key Findings Workshop in October 2022.

Key Findings Workshop

Key findings of the research were presented in an online workshop on 25 October 2022. Seventy-five **participants** discussed the findings and participated in an online poll.

Timeline	
November 4, 2021	Internet and Jurisdiction Virtual Event launched project.
December 13, 2021	The first knowledge dialogue workshop brought African stakeholders together to identify important issues of digital policy.
February 22, 2022	The second knowledge dialogue workshop with African and global stakeholders discussed important issues of digital policy and identified the demand for a common African narrative on cross-border data issues.
July 4, 2022	Report on the findings of the knowledge dialogue workshops.
July 19, 2022	A special panel at the African Internet Governance Forum discussed cross-border digital issues, including data flow, and launched the data collection process.
July - August 2022	Online data collection process.
August - October 2022	High level interviews.
October 25, 2022	Key findings workshop.

An important part of the methodology, therefore, included recurring outreach and consultation with stakeholders to gather diverse inputs and provide interim feedback on the report’s research questions and themes of focus.








ANNEX B: KEY ORGANIZATIONS WORKING ON GLOBAL DATA GOVERNANCE SOLUTIONS IN AFRICA.

Access Now

www.accessnow.org

Access Now is a global non-governmental organization that defends users' digital rights, including those of civil society groups, journalists, activists and human rights defenders. Through research, advocacy and coalition building with partners globally, this civic group advocates a human rights perspective on data issues and defends the right to privacy and data security to ensure that online activities are private, safe, and secure. It also provides comprehensive, real-time technical assistance to users.

Sample publications: ["The Future of Data Protection: What We Expect in 2021"](#)

Geographic scope:	Global	
Country/Headquarters:	Various	
Type:	Non-governmental	
Objectives:	Trust	
Outcomes:	Knowledge and community building, Advocacy	
Sector:	Justice	

African Francophone Open Data Community (CAFDO)

www.cafdo.africa

CAFDO is a non-governmental organization in Sub-Saharan Africa with a mission to create the conditions for a greater impact of open data in French-speaking African countries. Through networking, community building, and developing data-driven innovations to improve services and delivery in agriculture, transportation, gender equality and public service, CAFDO provides leadership in regional public, personal and corporate data governance. CAFDO also hosts training via the [Africa Data Academy](#).

Sample publications: ["Assessment of the Open Data ecosystem in Tunisia"](#); [Blog](#).







Geographic scope:	Sub-Saharan Africa	
Country/Headquarters:	Burkina Faso	
Type:	Non-governmental	
Objectives:	Data governance	
Outcomes:	Community building, Advocacy	
Sector:	Non-specific	

African Open Data Network (AODN)

www.developlocal.org/tagg/aodn

AODN is a non-governmental organization in Sub-Saharan Africa. It is a regional hub of Open Data for Development Network and Open Knowledge and Global Partnership for Sustainable Development Data. Its mission is to generate research insights to support open data initiatives and contribute to improvements in data for development in Africa. It focuses on research, networking, capacity development, and facilitating technical assistance to governments for successful open data initiatives in the region. AODN is part of the [Local Development Research Institute](#).

Sample publications: [Blog](#)

Geographic scope:	Sub-Saharan Africa	
Country/Headquarters:	Kenya	
Type:	Non-governmental	
Objectives:	Data governance	
Outcomes:	Knowledge and community building, Advocacy	
Sector:	Non-specific	

Big Data for Migration Alliance

<https://data4migration.org>

Big Data for Migration Alliance is a coalition seeking to improve the evidence base on migration and human mobility globally through research, community building, and advocacy. It aims to provide guidance and capacity building support on ethical and responsible data innovation.

Sample publications: [“Designing Data Collaboratives to Better Understand Human Mobility and Migration in West Africa”](#); [“The 100 Questions The Migration Data Agenda”](#); [“Big Data for Migration Alliance \(BD4M\) Harnessing the Potential of New Data Sources and Innovative Methodologies for Migration”](#); [“Designing Data Collaboratives to Better Understand Human Mobility and Migration in West Africa”](#); [“Big Data and Alternative Data Sources on Migration: From Case-Studies to Policy Support - Summary Report”](#); [“Big Data and Alternative Data Sources on Migration: From Case-Studies to Policy Support”](#); [“Can Big Data Help Us Achieve a ‘Migration Data Revolution?’”](#); [“IOM Migration Data Strategy”](#); [“Data Innovation for Migration: Why Now and How?”](#); [Blog](#)

Geographic scope:	Global
Country/Headquarters:	Ghana
Type:	Coalition
Objectives:	Socio-economic development
Outcomes:	Knowledge and community building, Advocacy
Sector:	Justice, Health, Transportation & mobility

Coalition for Digital Environment Sustainability (CODES)

www.sparkblue.org/CODES

CODES is part of the broader follow-up to the U.N. Secretary-General’s Roadmap on Digital Cooperation. Launched in March 2021, it will lead a global multistakeholder process and convene a series of events to anchor environmental sustainability needs within the Digital Cooperation Roadmap and catalyze a digital planet for sustainability. It seems to focus on energy and climate topics. It executes its mission by mobilizing the research community planning for digitizing environmental sustainability.

Geographic scope:	Global
Country/Headquarters:	Various
Type:	Coalition
Objectives:	Data governance
Outcomes:	Community building, Advocacy
Sector:	Environment

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

<https://cipesa.org>

CIPESA is a non-governmental organization in Uganda that focuses on the use of ICT in support of development and poverty reduction. It works across the continent informing policy making and encouraging debate by publishing commentaries, briefing papers and newsletters. Through research and networking, CIPESA supports the role ICT can play in achieving the key objective of open government. A member of [Global Knowledge Partnership \(GKP\)](#) and [Association for Progressive Communications \(APC\)](#), it is one of the two programs established under the [Catalyzing Access to Information and Communications Technologies in Africa \(CATIA\)](#) initiative. It supports the mission of the [Open Government Partnership \(OGP\)](#).

Geographic scope:	Sub-Saharan Africa
Country/Headquarters:	Uganda
Type:	Non-governmental
Objectives:	Data governance
Outcomes:	Community building, Advocacy
Sector:	Non-specific

Sample publications: [“New Law Holds Promise for Improved Data Governance in Kenya”](#); [“Uganda is a Ripe State for Open Governance Data”](#)

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

<https://cipesa.org>

CIPESA is a non-governmental organization in Uganda that focuses on the use of ICT in support of development and poverty reduction. It works across the continent informing policy making and encouraging debate by publishing commentaries, briefing papers and newsletters. Through research and networking, CIPESA supports the role ICT can play in achieving the key objective of open government. A member of [Global Knowledge Partnership \(GKP\)](#) and [Association for Progressive Communications \(APC\)](#), it is one of the two programs established under the [Catalyzing Access to Information and Communications Technologies in Africa \(CATIA\)](#) initiative. It supports the mission of the [Open Government Partnership \(OGP\)](#).

Sample publications: "[New Law Holds Promise for Improved Data Governance in Kenya](#)"; "[Uganda is a Ripe State for Open Governance Data](#)"

Committee on Data (CODATA)

<https://codata.org>

CODATA of the [International Science Council](#) was established as the International Council for Science Committee on Data for Science and Technology in 1966. CODATA promotes global collaboration to advance open science and to improve the availability and usability of data for all areas of research. It works with regional organizations, such as the European Commission and the EU Member states with their major leading initiative for the [European Open Science Cloud](#), which has an increasing number of partner initiatives in other regions. In order that high-throughput data generation instruments and computers may effectively support the scientific and innovation process, both data and workflow components need to be machine-actionable. Building on and refining many earlier efforts, in 2014 the [FAIR principles](#) were formulated. The CODATA [International Data Policy Committee \(IDPC\)](#) is the key instrument by which CODATA pursues its mission of promoting effective and appropriate policies for Open Science and FAIR data. [Task Groups](#) are groups of scientists, researchers and data experts who work together on a specific problem or theme to advance the state of data management and to advance science. CODATA collaborates on major data conferences such as [SciDataCon](#) and [International Data Week](#).

Sample publications: "[Data Science Journal](#)"; "[The Future of Science and Science of the Future: Vision and Strategy for the African Open Science Platform \(v02\)](#)"; "[CODATA History](#)"; [Blog](#)

Geographic scope:

Sub-Saharan Africa

Country/Headquarters:

Uganda

Type:

Non-governmental

Objectives:

Data governance

Outcomes:

Community building, Advocacy

Sector:

Non-specific

Geographic scope:

Global

Country/Headquarters:

France

Type:

Non-governmental

Objectives:

Data governance

Outcomes:

Knowledge, capacity and community building, Advocacy

Sector:

Non-specific

Dalberg Data Global Insights

<https://dalberg.com/what-we-do/dalberg-data-insights/>

Dalberg Data Global Insights is a global non-governmental organization with a purpose of building inclusive data ecosystems to address international development challenges. The group works in sectors of public health, food security, financial inclusion, gender, poverty alleviation, and energy access to develop data solutions in collaboration with stakeholders. By leveraging AI, the group adopts a human-centered approach to empower local and global communities based on their set of needs to better target, implement, and evaluate their programs and initiatives.

Sample publications: [“Dalberg Data Insights’ Mobile Money Dashboards Promote Financial Inclusion in Uganda”](#); [“What Are Hidden Data Treasures and How Can They Help Development Outcomes?”](#)

Geographic scope:
Global

Country/Headquarters:
Multinational

Type:
Non-governmental

Objectives:
Socio-economic development

Outcomes:
Data aggregator, Knowledge building, Advocacy

Sector:
Environment, Health, Gender, Economy, development, trade & finance, Food security

Data Collaboratives for Local Impact (DLCI)

<https://dcli.co/>

DLCI is a non-governmental organization that empowers individuals and communities in Africa with the data skills they need to solve health, education, gender inequality, and economic growth challenges. DLCI uses a systems-approach to unlock the power of data, advance country leadership in improving lives, and build the skills that youth and women need to access opportunities within the global digital economy. Relevant programs include [Tanzania Data Lab](#), a world class data and innovation lab that harnesses the potential of the data in solving local, regional, and global sustainable challenges through data and innovation. It offers [public resources](#) and [projects](#) to improve data-informed decision-making.

Sample publications: [“Assessing Data Readiness of Sub-National Institutions Using the Data Compass”](#); [“The Tanzanian Youth Data Engagement Strategy 2018-2023”](#)

Geographic scope:
Sub-Saharan Africa

Country/Headquarters:
United States

Type:
Non-governmental

Objectives:
Socio-economic development

Outcomes:
Knowledge and capacity building

Sector:
Non-specific

Data Policy Center

https://cipit.strathmore.edu/?page_id=9355

Data Policy Center at Strathmore University is a research center to study, create and share knowledge on the development of intellectual property and information technology. The long-term goal of the DPC is to contribute to the body of evidence available for those influencing policy in the areas of data protection, data bias, open data, and other issues pertaining to data governance with a focus on issues relevant to the Global South.

Sample publications: [“The Gap in Kenyan Based International Personal Data Transfers: Adequacy Considerations”](#), [“Data Protection in the Kenyan Banking Sector”](#)

Geographic scope:
Sub-Saharan Africa

Country/Headquarters:
Kenya

Type:
Research institution

Objectives:
Data governance

Outcomes:
Knowledge building

Sector:
Health, Economy, development, trade & finance

Data for Development Network (D4D.net)

<https://www.d4d.net>

D4D.net is a global research cooperative that works to strengthen collaboration across a broad network of stakeholders by developing and mobilizing the knowledge needed to advance the use of data to address critical development challenges across the Global South. Programs include the Global Index on Responsible AI, Global Data Barometer, Open Data for Development, and Data for Gender Equality. It starts with a simple premise – The responsible use of data can help us to achieve the Sustainable Development Goals (SDGs), understand the impact of the COVID crisis, or identify key priority areas for development programming to be addressed in the future. However, we need to know more, share what we know, and be willing to work together for the public good.

Sample publications: [“Global Data Barometer”](#); [“Designing a Rights-based Global Index on Responsible AI”](#); [“The State of Open Data”](#)

Digital Council Africa

www.digitalcouncil.africa

Digital Council Africa is an independent, not-for-profit organization with a business membership composition that seeks dialogue with all stakeholders on how to maximize the societal benefits of digital and data-driven technologies to increase equality and inclusivity, well-being and digital adoption in Africa. Established in 2010 under the banner of the FTTx Council Africa, the Digital Council supports and educates governments, policy makers and political leaders on technology and data issues facing the continent.

Sample publications: [Conext Newsletter](#)

Feminist Open Government (FOGO)

<https://fogo.od4d.net>

FOGO is a non-governmental initiative in Canada that aims to advance gender equality and better governance through increased transparency, participation, accountability, and government responsiveness. The initiative’s research will be action-oriented, informed by evidence, and produced in such a way that government reformers and civil society partners in Open Government Partnership countries can use it.

Sample publications: [“Feminist Open Government: Addressing Gender Equity Challenges in Open Government Co-Creation Processes. Case Studies from Latin America, Africa and Asia”](#)

Geographic scope:
Global



Country/Headquarters:
Canada



Type:
Non-governmental



Objectives:
Socio-economic development



Outcomes:
Knowledge, capacity and community building, Advocacy



Sector:
Non-specific



Geographic scope:
Sub-Saharan Africa



Country/Headquarters:
South Africa



Type:
Coalition



Objectives:
Socio-economic development



Outcomes:
Knowledge and community building, Advocacy



Sector:
Non-specific



Geographic scope:
Global



Country/Headquarters:
Canada



Type:
Non-governmental



Objectives:
Socio-economic development



Outcomes:
Data aggregator, Community building, Advocacy





Sector:
Gender



Ghana Open Data Initiative

<https://data.gov.gh>

Ghana Open Data Initiative is a non-governmental platform to ensure public accessibility of data collected by the group on topics of [agriculture](#), [business](#), [city data](#), [education](#), [elections](#), [energy](#), [environment](#), [health](#), and [local government](#). The Initiative supports (i) better governance and delivery of public services attributable to more evidence-based decision-making, higher levels of information sharing, and increased transparency; and (ii) socio-economic development attributable to reuse of open data and innovation, insights gained by harvesting open data with other data sources. Programs include [Hackathon](#) and [Open Data for Academic Outreach](#) with the ultimate goal to set up Open Data clubs in universities to engage continuously with the Ghana Open Data Initiative.


Geographic scope:	 National
Country/Headquarters:	 Ghana
Type:	 Non-governmental
Objectives:	 Data repository
Outcomes:	 Data aggregator, Capacity and community building, Advocacy
Sector:	 Agriculture, Economy, development, trade & finance, Education, Environment, Health,

Global Data Justice

<https://globaldatajustice.org>

Global Data Justice is an academic project, based in the Netherlands, that focuses on the diverse debates and processes occurring around data governance in different regions to draw out overarching principles and needs that can push data technologies' governance in the direction of social justice.

Sample publications: [“What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally”](#); [“Constructing Commercial Data Ethics”](#); [“Global Data Justice”](#); [“What is Responsible and sustainable Data Justice?”](#); [“A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk”](#)

Geographic scope:	 Europe & Central Asia, South Asia, Sub-Saharan Africa
Country/Headquarters:	 The Netherlands
Type:	 Research institution
Objectives:	 Data governance
Outcomes:	 Knowledge and community building, Advocacy
Sector:	 Business, Justice, Media, Health

Global Partnership for Sustainable Development Data

www.data4sdgs.org

Global Partnership for Sustainable Development Data (Global Partnership) is a global network, headquartered in Washington, D.C. with a distributed team working from eight countries, with fiduciary hosting by the United Nations Foundation (501c3). The network works together to ensure the new opportunities of the data revolution are used to achieve the Sustainable Development Goals to improve lives, fight inequality, and promote environmental sustainability. It bridges divides between sectors as a connector, a facilitator, a broker, and an advocate. The Global Partnership brings together 600 partner organizations to put the power of data behind delivering the Sustainable Development Goals. Based on its [Five-Year Strategy](#) and its 2021-2023 [Country Engagement Strategy](#), it does this by: (i) Building a global movement advocating on data for development; (ii) Influencing and shaping global policies and frameworks on data; (iii) Getting data to where it is needed, in the hands of decision-makers and governments. The Global Partnership works through advocacy campaigns, like the [Data Values Project](#), and various initiatives, like the [Inclusive Data Charter](#) and [Data for Now](#). It offers [learning resources](#) for communities to build from others' experiences and to help develop common mechanisms and approaches toward more coherent and inclusive data ecosystems.

Geographic scope:	 Global
Country/Headquarters:	 United States
Type:	 Coalition
Objectives:	 Socio-economic development
Outcomes:	 Knowledge, capacity and community building, Advocacy
Sector:	 Agriculture, Economy, development, trade & finance, Education, Environment, Health, Justice, Gender, Food security, Media, Transportation & mobility

Sample publications: [“Data for a Resilient Africa”](#); [“Advancing Dialogue on Data Governance in Latin America and the Caribbean”](#); [“Four Recommendations for Building Trust in Multistakeholder Governance of the Data Economy”](#); [“Improved Data Governance Leads to Better Economic Outcomes for Philippine Citizens”](#); [“Four Approaches to Align Data Values Across Communities of Practice”](#); [“Toward a Common Understanding of Data Governance”](#); [News](#)

Health Data Collaborative

www.healthdatacollaborative.org

Health Data Collaborative is a non-governmental organization that provides a collaborative platform that leverages and aligns technical and financial resources to country owned strategies and plans for collecting, storing, analyzing and using data to improve health outcomes, with specific focus on SDG targets and communities that are left behind. The group executes its mission through partnering with global [health stakeholders](#) and [building knowledge](#) through its [working groups](#) and tools they produce.

Sample publications: [“Data and Digital Governance Working Group: Terms of Reference”](#)

Geographic scope:
Sub-Saharan Africa

Country/Headquarters:
Various

Type:
Non-governmental

Objectives:
Data governance

Outcomes:
Capacity and community building, Advocacy

Sector:
Health



Innovation for Poverty Action

www.poverty-action.org

Innovation for Poverty Action is a research and policy non-profit organization that creates and shares evidence, while equipping decision-makers to use evidence to reduce poverty. With a long-term presence in 22 countries in [Africa, Asia, and Latin America](#), IPA leads the field of development in cutting-edge research quality, innovation, and impact. Its program areas include [agriculture](#), [education](#), [financial inclusion](#), [governance](#), [health](#), [peace and recovery](#), [entrepreneurship](#), and [social protection](#). IPA values research transparency, thus data-sharing is a key component of [transparent research](#).

Sample publications: [“2020-2021 IPA Annual Report”](#); [“Report: Measuring Fees and Transparency in Nigeria’s Digital Financial Services”](#); [Blog](#)

Geographic scope:
Global

Country/Headquarters:
Various

Type:
Coalition

Objectives:
Data governance

Outcomes:
Community and capacity building

Sector:
Non-specific



Internet Society (ISOC)

www.internetsociety.org

ISOC is a global non-profit organization that supports and promotes the development of the internet as an open, secure and trustworthy global technical infrastructure, a resource to enrich people’s lives, and a force for good in society. People are at the heart of the [Society’s mission](#). The group seeks collaboration with all who share these goals. It executes its mission by offering [programs](#) and [projects](#) to close the digital divide and to strengthen the internet, and by [advocacy](#).

Sample publications: [“Internet Way of Networking Use Case: Data Localization”](#); [“Action Plan 2022”](#)

Geographic scope:
Global

Country/Headquarters:
United States

Type:
Non-governmental

Objectives:
Trust

Outcomes:
Knowledge and community building, Advocacy

Sector:
Non-specific



Open Institute

<https://openinstitute.africa>

Open Institute is a non-profit organization based in Nairobi, Kenya, that collaborates with governments, civil society organizations, citizen groups and the private sector to find innovative ways to achieve sustainable development. The Institute with stakeholders aims to promote responsive governments that have the necessary capacity to listen and engage fruitfully with citizens. Through its work it wants to see open and proactive governments that ensure all the relevant information concerning development is disclosed to the public to give value to citizen voices. Its programs include responsive government and active citizenship.

Sample publications: "[Data Governance](#)"; [Blog](#)

Geographic scope:
National

Country/Headquarters:
Kenya

Type:
Non-governmental

Objectives:
Data governance

Outcomes:
Knowledge, capacity and community building, Advocacy

Sector:
Non-specific

OpenUp

<https://openup.org.za>

OpenUp is a global non-governmental organization that partners with government, organizations, industry leaders and civil society to identify, gather, and make accessible information that supports open communities and an empowered citizenry. It executes its mission through partnerships and projects and tools.

Sample publications: "[Simple Tech Tool Helps to Expose Huge Lottery Corruption](#)"; "[How to Measure the Impact of OpenUp's Civic Tech Tools](#)"; [Blog](#)

Geographic scope:
Global

Country/Headquarters:
South Africa

Type:
Non-governmental

Objectives:
Data governance

Outcomes:
Capacity building, Advocacy

Sector:
Non-specific

Partnership in Statistics for Development (PARIS21)

<https://paris21.org/about-paris21>

PARIS21 is an international non-governmental organization promoting the better use and production of statistics throughout the developing world. PARIS21's goal is to develop a culture of Management for Development Results (MfDR). PARIS21 pursues this goal primarily by encouraging and assisting low-income and lower middle-income countries to design, implement, and monitor a National Strategy for the Development of Statistics (NSDS). The group executes its mission through engaging international initiatives, knowledge building, advocating, developing innovative solutions for statistics, and strengthening statistical systems. Gender Data Network is a joint initiative between PARIS21, Data2X, the U.N. Economic Commission for Africa (ECA), and Open Data Watch.

Sample publications: "[New policy brief: Participatory Data Ecosystems to Close COVID-19 Data Trust Deficit](#)"; [Newsletter](#)

Geographic scope:
Global

Country/Headquarters:
France

Type:
Non-governmental

Objectives:
Socio-economic development

Outcomes:
Knowledge, capacity and community building

Sector:
Non-specific

Research ICT Africa

<https://researchictafrica.net>

Research ICT Africa, with a vision of digital equality in Africa, accelerates economic inclusion and social justice by undertaking rigorous research and data surveys to inform digital policy and data governance. It conducts multidisciplinary research on digital governance, policy and regulation, through various projects, to facilitate evidence-based and informed policy making for improved access, use and application of digital technologies for social and economic development in Africa. Its ICT Africa Mobile Pricing Index is a database of the lowest data and voice prices collected quarterly for each mobile operator in Africa. Its public-interest research on the digital economy and society responds to national, regional and continental needs. It provides relevant stakeholders with the information and analysis required to develop flexible and adaptive policies and regulation to deal with an increasingly complex and dynamic digital environment. RIA contributes to the gathering and analysis of data and indicators to establish a repository of knowledge for furthering research and digital governance.

Sample publications: [“Designing a Rights-Based Global Index on Responsible AI”](#); [“From Data Protection to Data Justice – redressing the uneven distribution of opportunities and harms in AI”](#); [AI4D – Digital and Biometric Identity Systems](#); [“An African perspective on gender and artificial intelligence needs African data and research”](#); [Blog](#)

Geographic scope:
Sub-Saharan Africa

Country/Headquarters:
South Africa

Type:
Non-governmental

Objectives:
Socio-economic development

Outcomes:
Data aggregator, Knowledge, capacity and community building, Advocacy

Sector:
Business, Economy, development, trade & finance, Education, Transportation & Mobility, Health, Gender, Justice, Media

Slum Dwellers International (SDI)

<https://sdinet.org>

SDI is a network of community-based organizations of the urban poor in 32 countries and hundreds of cities and towns across Africa, Asia and Latin America. SDI is committed to supporting a process that is driven from below. Its partners include academic institutions, international networks and multilateral organizations. Its main project is the Explore Our Data map with city and settlement data. SDI's databases are becoming the largest repositories of informal settlement data in the world and the first port of call for researchers, policy makers, local governments and national governments.

Sample publications: [Videos](#); [Blog](#)

Geographic scope:
Latin America & Caribbean, East Asia & Pacific, South Asia

Country/Headquarters:
South Africa

Type:
Non-governmental

Objectives:
Data repository

Outcomes:
Data aggregator, Advocacy

Sector:
Agriculture, Justice, Environment, Health, Gender, Food security, Education, Economy, development, trade & finance

Tanzania Data Lab

<https://dlab.or.tz>

Tanzania Data Lab is a world class data and innovation lab that harnesses the potential of the data revolution and the fourth industrial revolution in solving local, regional, and global sustainable development challenges through data and innovation. The group envisions an African continent where data is frequently and consistently used to inform policy and decision making at all levels. To accomplish its mission, the group works on several projects: Data Science Solutions, capacity development, community engagement, and innovation. Its resources include data portal, co-working space, and publications.

Sample publications: [“Assessing Data Readiness”](#)

Geographic scope:
National

Country/Headquarters:
Tanzania

Type:
Non-governmental

Objectives:
Socio-economic development

Outcomes:
Capacity and community building

Sector:
Non-specific

Unwanted Witness

www.unwantedwitness.org

Unwanted Witness is a civil society organization in Uganda that was established to respond to the gap in effective communication using various online expression platforms. Its mission is to contribute to good governance through effective and efficient internet/online activism through networking and strengthening capacities of netizens for collective advocacy and synergy. Programs include [Data Protection and Privacy](#), [Digital Identity](#), and [freedom of expression](#).

Sample publications: [“Privacy Scorecard Report 2021”](#); [“Data Protection and Privacy Law Analysis”](#); [“The Data Protection and Privacy Act 2019”](#); [Blog](#)

Geographic scope:
National

Country/Headquarters:
Uganda

Type:
Non-governmental

Objectives:
Trust

Outcomes:
Capacity and community building, Advocacy

Sector:
Justice

World Data Systems

www.worlddatasystem.org

World Data Systems is an Interdisciplinary Body of the [International Science Council](#). Its mission is to support the ISC’s vision by promoting long-term stewardship of, and universal and equitable access to, quality-assured scientific data and data services, products, and information across all disciplines in the natural and social sciences and the humanities. WDS replaced the International Polar Year and the International Geophysical Year to better respond to modern data needs. The Body’s [objectives](#) are: to enable universal and equitable access to quality-assured scientific data, data services, products and information; to ensure long-term data stewardship; to foster compliance to agreed-upon data standards and conventions; and to provide mechanisms to facilitate and improve access to data and data products. Its [working groups](#) and the [Scientific Committee](#) follow [Data Sharing Principles](#) when dealing with large datasets. The [Early Career Researchers and Scientists Network](#) promotes best practices in data management, data analysis, and data sharing among Early Career Researchers (ECRs).

Sample publications: [“Strategic Plan 2019-2023”](#); [“WDS Scientific Committee 2018-2021 Teleconference #21”](#); [“Membership Maturity”](#); [Blog](#)

Geographic scope:
Global, Sub-Saharan Africa

Country/Headquarters:
France

Type:
Research institution

Objectives:
Data governance

Outcomes:
Knowledge, capacity and community building

Sector:
Non-specific

The Internet & Jurisdiction Policy Network is the multistakeholder organization addressing the tension between the cross-border nature of the internet and national jurisdictions.

Its Secretariat facilitates a global policy process between key stakeholders to enable transnational cooperation and policy coherence. Participants in the Policy Network work together to preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from different stakeholder groups around the world, including governments, the world's largest Internet companies, the technical community, civil society groups, leading universities, and international organizations.

