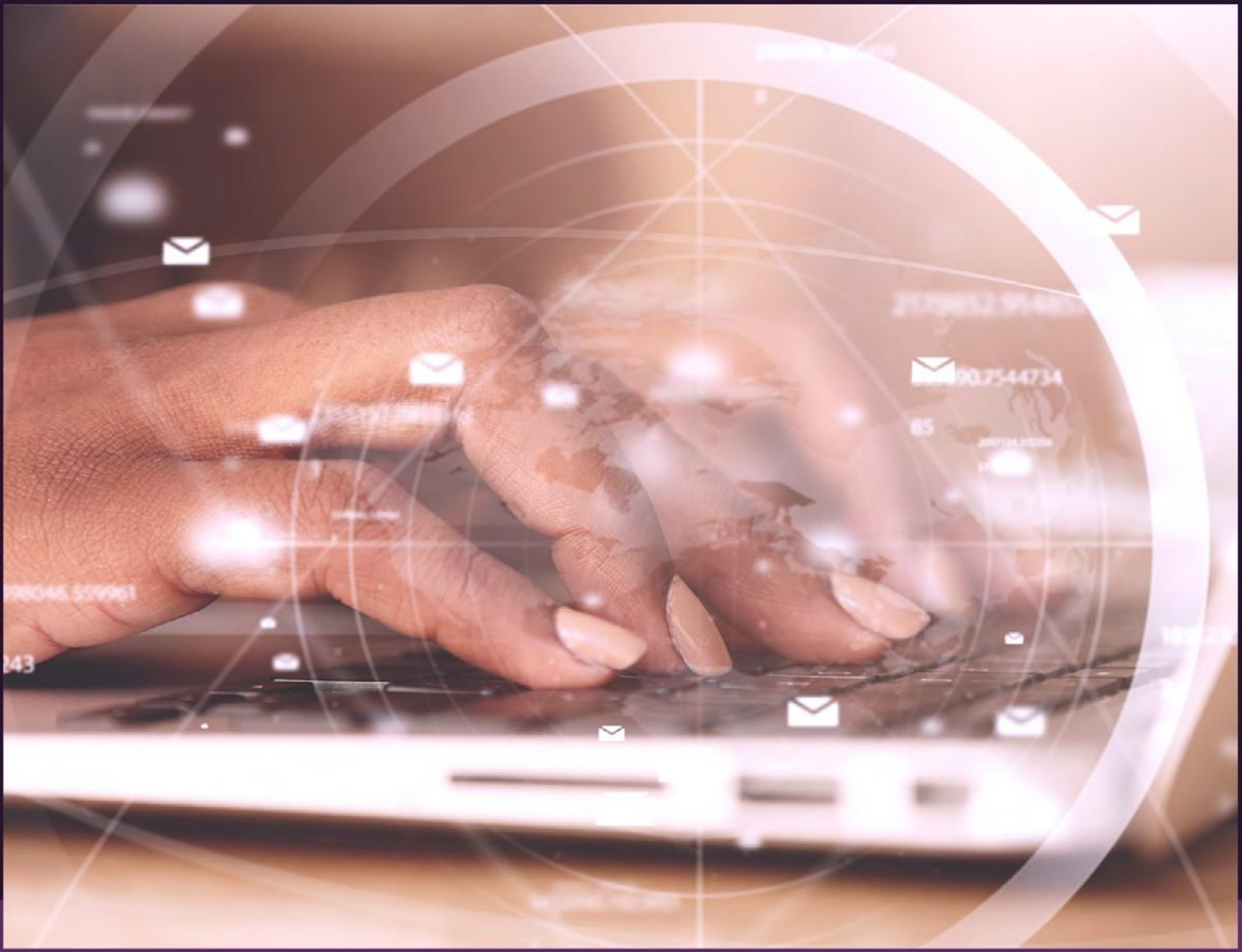


GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA
TECHNICAL BACKGROUND PAPER SERIES

Regulating Digital Data in Africa

WORLD BANK GROUP

DIGITAL
DEVELOPMENT
PARTNERSHIP

GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA

TECHNICAL BACKGROUND PAPER SERIES

Regulating Data Protection and Cybersecurity in Africa: Findings from the Global Data Regulation Diagnostic

THE WORLD BANK
IBRD • IDA

DIGITAL
DEVELOPMENT
PARTNERSHIP

The World Bank

1818 H Street NW

Washington DC 20433

Telephone: 202-473-1000

Internet: www.worldbank.org

Disclaimer

This work is a product of the staff of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

Rights and Permissions

Acknowledgements

This Background Note was prepared by Rong Chen (Economist, Digital Development), Lillyana Daza Jaller (consultant), and Tania Begazo (Senior Economist) with contributions from Ana Ruival (consultant, Digital Development).

The Background Note benefited immensely from the participation, assistance, and insights from other experts. The team is especially grateful for references on cybersecurity assessments in Africa provided by Anat Lewin, Senior Digital Specialist, the peer reviewers David Satola, Lead Counsel, Technology & Innovation, Legal and Anat Lewin, and the prior work conducted for the World Development Report 2021 'Data for Better Lives' that allowed for the development of the survey used to compare the status of data regulation across countries in Africa.

Common Abbreviations and Defined Terms

This section explains the common terms and abbreviations used in this paper.

Abbreviation / Term	Full Terminology / Definition
ARP	Administrative Redress Panel
ATI	Access to Information
CERTs	Computer Emergency Response Teams
CNDP	Morocco's Data Protection National Commission
CSIRTs	Computer Security Incident Response Teams
CSSSI	Morocco's Committee for Information Systems Security
DGSSI	Morocco's Directorate General for Information Systems Security (,
DPC	Kenya's Data Protection Commissioner
ECCAS	Economic Community of Central African States
FRAND	Fair, reasonable and non-discriminatory terms
GCI	Global Cybersecurity Index
IPR	Intellectual property right
maCERT	Moroccan Computer Emergency Response Team
NCS	National cybersecurity strategy
NIN	National Identification Number

Table of Contents

List of Figures

List of Tables

1 The Importance of Data Regulation

Rapid development of digital technologies in recent years has shown its great potential for Africa to promote job creation, improve delivery of public services, and enhance individual welfare. For instance, it is estimated that e-commerce platforms, such as Jumia, could create about three million new jobs in Africa by 2025.[1] Mobile money, exemplified by the global household name—M-Pesa, contributes to poverty reduction in many African countries.[2] The COVID-19 global pandemic led to an accelerated rise in the use of digital technologies around the world, increasing innovation but also leading to various governance challenges and risks.

There is a growing concern on data protection and cybersecurity risks associated with various digital economic activities. Data protection is at the core of this apprehension for individuals around the world. From social media to mobile payments to telehealth appointments, our personal information is stored in databases on an unprecedented scale. While these innovations make our lives easier and keep us connected, unless the data are adequately protected it can be misused for all kinds of purposes, from harassment to fraud.

The increased use of the Internet for both personal and professional needs has created opportunities for dangerous players seeking to take advantage of vulnerabilities for personal gain. In 2020, Kenyan internet users faced 14 million malware attacks between January and August. The number of cyberattacks in Zimbabwe grew five times during the same period.[3] In August 2020, Experian, a global consumer credit reporting company, sold personal data of about 24 million South Africans to a fraudster posing as a legitimate client.[4] In December 2020, personally identifiable information belonging to Absa Bank's customers -who are spread throughout twelve African countries- were leaked. According to the African Union Convention on Cyber Security and Personal Data Protection, cybercrime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa".[5]

Adequate legal and regulatory frameworks are key for countries to be able to fully reap the benefits of emerging technologies while minimizing the associated risks. The international nature of the use and impact of these technologies complicate their regulation. Concerns about how data is acquired, handled, used, shared and reused have led to governments establishing heterogeneous approaches for data governance. Data are the building blocks of these revolutionary technologies and restricting their flow can hamper trade, innovation, and economic growth.[6] Governments have a difficult task: ensuring adequate flow of data across borders and within a country to allow novel technologies to operate adequately while safeguarding individual rights. A rights-based approach can lead to increased trust, which can in turn foster data flows and data-based digital solutions for development.[7] This note focuses on few key regulatory aspects: data protection, cybersecurity and cybercrime to boost digital trust; and rules on the use, transfer and re-use of data to enable new digital technologies. Other aspects of the data ecosystem as described in the Word Development Report 'Data for Better Lives' are not covered in this note.

To maximize the dividends from a booming digital economy, the continent shall be prepared to address risks associated with the variety of digital economy activities, while enabling the use of data for development. A robust data governance environment is essential in promoting the sustainable development of the digital economy. A comprehensive regulatory framework that specifies rights and responsibilities of different stakeholders in collecting, using, and reusing of data, independent authorities to enforce laws and address public complaints on violations, as well as public-private partnership and regional collaboration are all important components of such a robust data governance environment.

This note aims to provide an overview of data governance frameworks in Africa and explore links with engendering public trust and improving accountability and transparency, as well as providing an enabling environment for participating in the digital economy. It exploits data from the Global Data Regulation Diagnostic (GDRD)[8] which collected information on data regulations across 80 countries globally, including 24 Sub-Saharan African countries and three North African countries, as of June 2020.[9] Additional information for selected countries was collected through desk research and interviews to understand challenges in the implementation of rules captured by the GDRD. This complementary information is as of February 2022.

This note is organized as follows. Section 1 covers data protection, while section 2 looks into cybersecurity and cybercrime, both important aspects for digital trust. Section 3 looks at the linkages between data protection and cybersecurity and cybercrime frameworks and broader governance indicators. Section 4 highlights aspects that can affect the use and reuse of data - data collected for public purposes and by the private sector as part of routine business process - for the development of digital technologies.

2 Personal data protection

Personal data protection is a crucial aspect of an effective data governance environment. Personal data refers to data that conveys information that is specific to a known or knowable individual. Lack of trust in the way personal data is managed makes individuals uncomfortable about sharing such data, which could limit the growth of the digital markets.[10] According to the Data Confidence Index,[11] internet users in Africa are particularly concerned about the impact of the internet on “personal privacy”.[12] Consumers in Kenya expressed preferences on digital loan products with more “data privacy” features.[13] In a study conducted in 2019, 96 percent of Egyptians expressed concern about their online privacy, well above the global average of 78 percent.[14] On the other hand, Kenya stood out with the highest level of confidence among all the economies covered (Figure I). Governments can help engender trust by granting data subject rights with regard to their personal information and imposing technical requirements on data controllers and data processors to ensure the adequate protection of the information. The establishment of a capable and effective enforcement authority is also key to ensure adequate implementation of the legislation.[15]

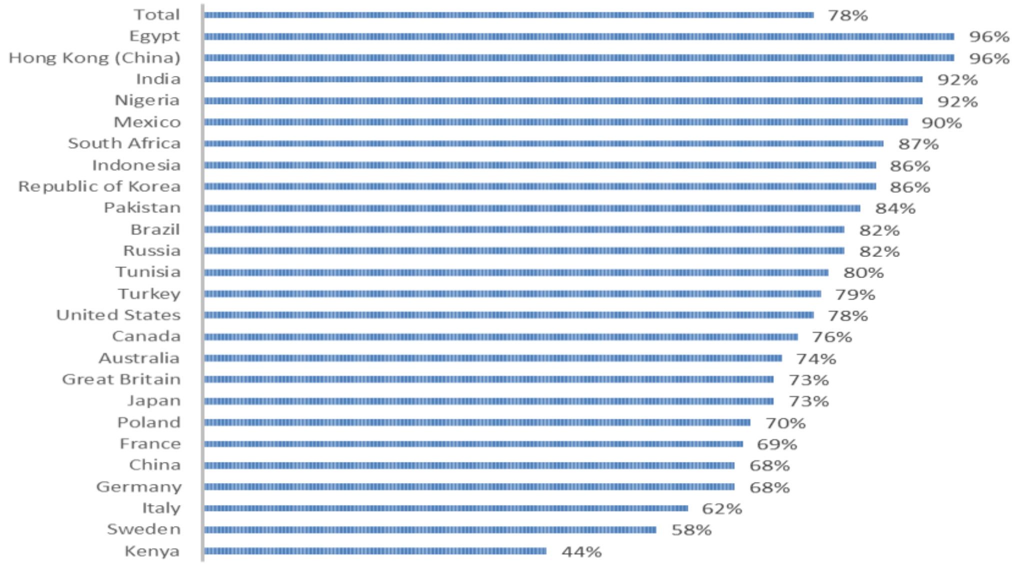
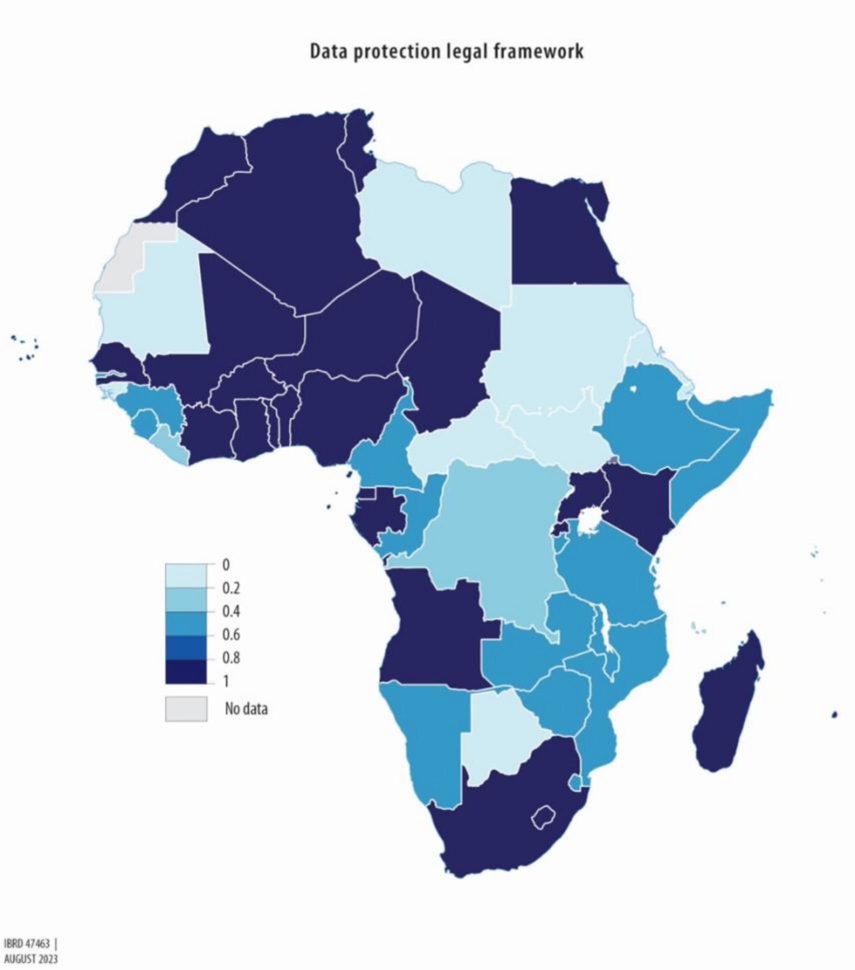


Figure I. Individuals' concern about their online privacy
Source: CIGI-Ipsos (2019)

2.1 Observations of the regulatory landscape on personal data protection in Africa

Over half of the countries in Africa have introduced general data protection legislation, applicable to all sectors (Figure II). Tunisia, Mauritius, and Burkina Faso were regional pioneers in this regard, introducing data protection laws as early as 2004. During the following decade, several countries followed suit, and as of December 2021 twenty-six African countries have adopted general data protection laws. Notably, Mauritius passed its Data Protection Act, which is closely aligned with the EU General Data Protection Regulation (GDPR), five months before the EU regulation was implemented in May 2018. The year 2020 was one of great advances for data protection legislation in Africa. Egypt's Law on the Protection of Personal Data came into force in October 2020. Prior to the approval of this law, Egypt had sector-specific legislation which addressed data protection issues, such as the Labor Law and the Banking Law. In South Africa, although the Protection of Personal Information Act was signed into law in 2013, most of the relevant provisions were not operational until July 2020. Most recently, Rwanda published a data protection law in its Official gazette in October 2021. Other economies have reportedly engaged in discussions to introduce general data protection laws, including Ethiopia, Malawi, and Tanzania; however, no public drafts of those laws were available as of February 2022.

A smaller number of African countries have introduced sector-specific laws, and some rely on constitutional provisions for privacy protection. For example, although Cameroon has no general data protection law, its Law on Cybersecurity and Cybercrime –applicable to electronic communications networks and information systems— includes provisions on data privacy. Although the Democratic Republic of Congo and Liberia have not introduced any laws addressing the issue of data protection, both countries' Constitutions include provisions regarding the individual right to privacy. However, these measures are not sufficient to tackle the situations data subjects and data processors are exposed to in today's world. Finally, eight African countries (denoted in gray in the map below) lack any mention of data protection or privacy in their legal frameworks.



Note: a top score of 1 (dark orange) indicates the existence of a general data protection law, a score of 0.5 indicates the existence of only a sector-specific personal data protection legislation; a score of 0.25 (lightest orange) indicates that there are privacy and/or data protection rights protected in the country's constitution.

Figure II. Data protection legal frameworks in Africa

Source: Authors based on Global Data Regulation Diagnostic and Data Guidance (2021)

After adopting a data protection law of general application, comprehensiveness of such law determines the level of protection provided to different market players. As pointed out in the Global Data Regulation Diagnostic, it is crucial to examine whether the data protection law specifies data subject rights such as redress and the right to challenge the accuracy of data collected, and requirements for collection and processing, such as purpose limitation, data minimization, and storage limitation (Box 1). It is also important to look at whether limitations exist on the ability to make decisions about individuals only on the basis of automated processing, which might lead to social discrimination, and whether a necessity and proportionality test applies to exceptions to limitations on government data collection or processing. Finally, other key information includes whether data subject rights are effectively protected on the technical side through the implementation of measures based on the data protection by design and data protection by default principles, as well as by the monitoring activity of a data protection authority.

Box I. Data processing requirements

Purpose limitation	Data must only be collected for a specified purpose
Data minimization	Data must be adequate, relevant, and limited to what is necessary in relation to the specified purpose
Storage limitation	Data must not be kept longer than is necessary for the specified purpose

Source: ICO (2021)

The existing data protection frameworks in Africa[16] are largely comprehensive (Figure III). Governments that have introduced an overarching data protection law have tended to include what are emerging as common elements of good international practice in this area, such as purpose limitation, data minimization, and data subject rights, which feature in sources ranging from the OECD Principles and GDPR. Kenya and Benin have also included more novel measures, such as data protection by design and data protection by default. Notably, South Africa's data protection law, which came into effect in 2020, leaves out these requirements. Data protection by design means that entities should consider data protection at the initial design stages of their products and systems and throughout the lifecycle of the data collected, and not as an afterthought. The principle of data protection by default entails incorporating the principle of 'data protection by design' by default into its data processing activities. Older data protection laws, which called for 'appropriate technical and organizational measures to protect data', were too broad, allowing controllers to be reactive with regard to data protection instead of implementing preventative measures from the outset. Finally, Privacy Enhancing Technologies (PETs) are technologies designed to allow organizations to extract the full potential of data without putting a data subject's privacy at risk.

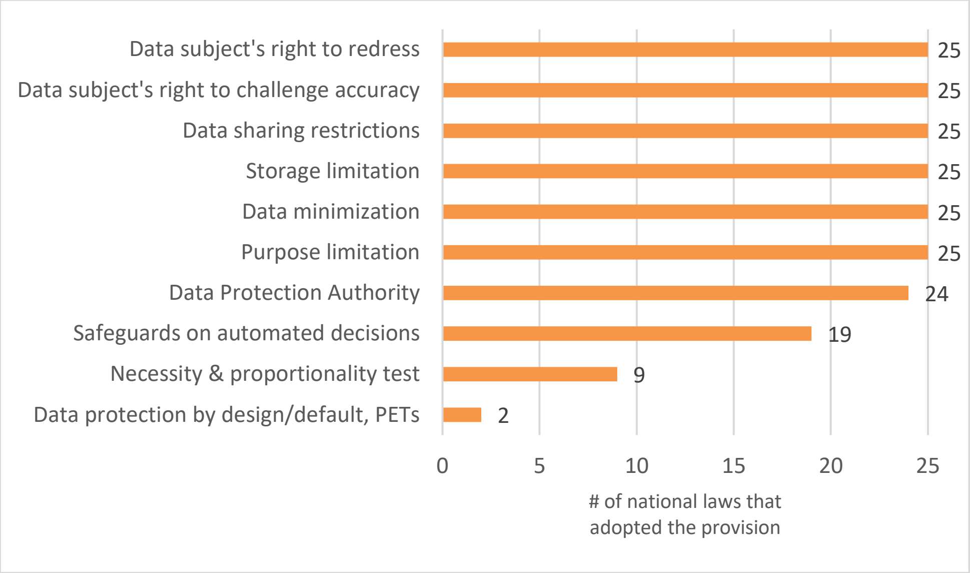


Figure III. Comprehensiveness of African data protection laws

Source: Authors based on Global Data Regulation Diagnostic and desktop research

Every African country in the sample that has adopted a data protection law of general application has buttressed it with the requirement to establish a data protection authority (DPA), but this authority is not always independent or in operation. In several African countries, including Angola and Egypt, although the data protection law requires the establishment of a DPA, it had not been established in practice by February 2022. An independent DPA is regarded as a critical element of an effective data protection regulatory framework[17] and most data protection laws in the continent call for it, however many African countries cannot afford to establish an independent DPA and therefore establish it as part of an existing agency as a first phase. This is the case in Nigeria, Rwanda, and Uganda, for example, where the data protection authorities are not separate from the ministry. Other countries in the region are envisioning an alternative approach, including Burundi and Somalia, where the DPA will be part of the telecommunications regulator. This phased evolution, as part of an existing regulator, can help developing countries set up their DPAs, focusing on building the agency's resources before it becomes fully independent.

Finally, legally mandated DPAs in Africa are tasked mainly with responsibilities such as promoting awareness of the risks, rules, and safeguards of rights pertaining to personal data, providing a redress mechanism, providing guidance on the interpretation of the law or regulation, and enforcing national data protection rights and obligations enshrined under the law or regulation (Figure IV). However, tasks such as publishing activity reports and encouraging the creation of codes of conduct and certifications review are scarcer among DPA mandates in Africa, limiting the agencies' power to ensure compliance. Finally, few African legal protection frameworks require keeping records of sanctions and enforcement, reducing the transparency and accountability of the agencies.

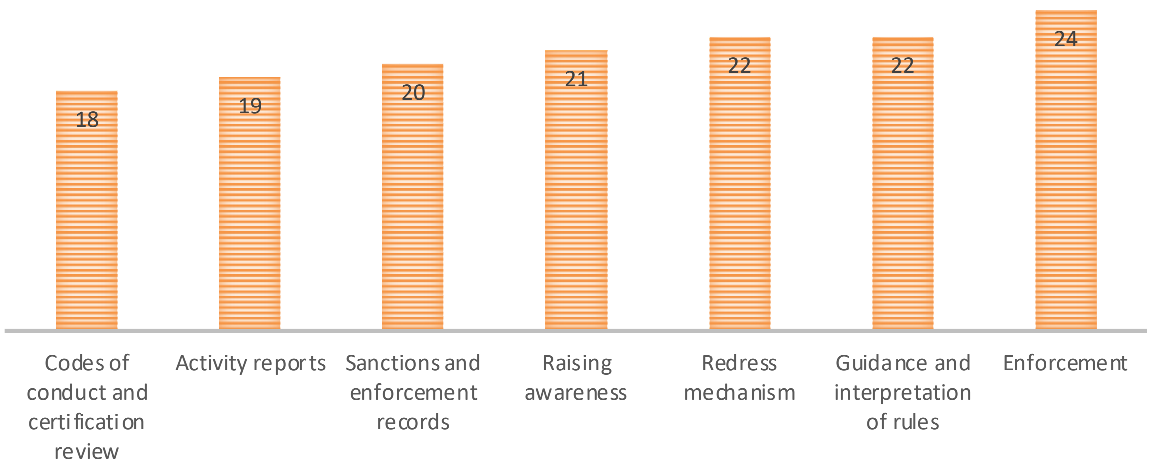


Figure IV. Responsibilities of African Data Protection Agencies
Source: Authors based on Global Data Regulation Diagnostic and desktop research

2.2 Regional collaboration on personal data protection

With the bourgeoning of digital trade, data flows are not bound to national territories. For instance, cross-border remittances or cross-border e-commerce requires consistent rules across countries to provide similar level of consumer protection.[18] Reaching regional consensus on data protection standards is needed to ensure compatibility and avoid fragmentation.[19] Regional collaboration also helps amplify the voice of smaller developing countries in global negotiations related to data governance, especially given the lack of representation in a few ongoing international talks such as the discussion led by the World Trade Organization (WTO) on a data governance framework for cross-border data flows.

A few African regional communities have taken initiatives to promote regional integration on personal data protection. The Economic Community of West African States (ECOWAS) has been working towards region-wide convergence in IT-related standards and the harmonization of regulations. The community adopted the Supplementary Act on Personal Data Protection in 2010. The legally binding act specifies data subject rights, including the right of access and the right of deletion, as well as requirements for controllers, such as confidentiality and security of the personal data. The Act also requires all members to establish an independent data protection authority to ensure compliance. Although implementation was required within two years of the adoption of the Act, one third of the Member States either have no legislation or are still in the process of adopting legislation. Benin, Burkina Faso, and Senegal had already introduced data protection laws prior to the Supplementary Act, and Mali, Ghana, and Cote d’Ivoire are among the countries that incorporated the Act.

Similarly, the African Union (AU) Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention), which seeks to create a pan-African framework to address electronic transactions, personal data protection, and cybercrime, was adopted by the AU in 2014. To date, it has been signed by fourteen countries and ratified by eight countries.[20] However, the Convention must be ratified by fifteen of the fifty-five AU states to enter into force. The chapter on personal data protection addresses automated and non-automated data processing by public and private entities. It imposes an obligation on all state parties to establish a data protection agency, responsible for informing individuals and data processors of their rights and obligations. It also lays out data processing principles, including specific principles for the processing of sensitive data. Given the Convention's deficiencies and lack of traction, recent conversations among the African Union have focused on how to reboot the Malabo Convention. Additionally, in February 2022, the African Union Executive Council endorsed the African Union Data Policy Framework that aims at providing guidance on various areas including data protection.[21]

Finally, Burkina Faso, Cabo Verde, Mauritius, Morocco, Senegal, and Tunisia have ratified the Council of Europe's Convention 108. This is an international human rights treaty focused on data protection, setting out principles that are compatible with the requirements of European Union (EU) regulation. It is the only existing binding international data protection convention. In 2018, 21 states signed a protocol modernizing Convention 108, known as "Convention 108+", which aligns with the EU GDPR. Mauritius and Tunisia later signed the amending protocol, and other parties to Convention 108, such as Morocco, are in the accession process for 108+. At the same time, Morocco is updating its own data protection legislation to seek an adequacy determination from the European Union under the GDPR. This latter approach is also an option for other African countries to facilitate trade and crossborder data flows with key trade partners.

2.3 Africa vs. other income groups on personal data protection frameworks on the book

Compared to other countries included in the sample, the existing data protection legal frameworks of African countries are comprehensive. The continent performs on par with or better than low-and-middle-income economies in other regions on most of the dimensions studied. Adoption of the regulatory practice on data protection by design is lower Africa than in other countries studied across different income groups. However, for the rest of the dimensions, African countries are among the top performers. For example, although only nine African data protection laws include a test of necessity and proportionality to determine whether an exception to limitations on data collection or processing by the government is legitimately applied, the region fares better in this regard than other low- income countries (LICs), and other middle-income countries (MICs) in the sample (Figure V). Furthermore, Africa is in line with or slightly below the adoption rate of high-income countries (HICs) in the sample with regard to data sharing restrictions, data processing requirements, and data subject rights. Finally, the region outperforms all other groups in the sample on few indicators. More than half of the African countries provide rights to limit the making of decisions about individuals solely as a result of automated processing of personal data and 65 percent of the existing data protection laws in the continent mandate the creation of a data protection authority.

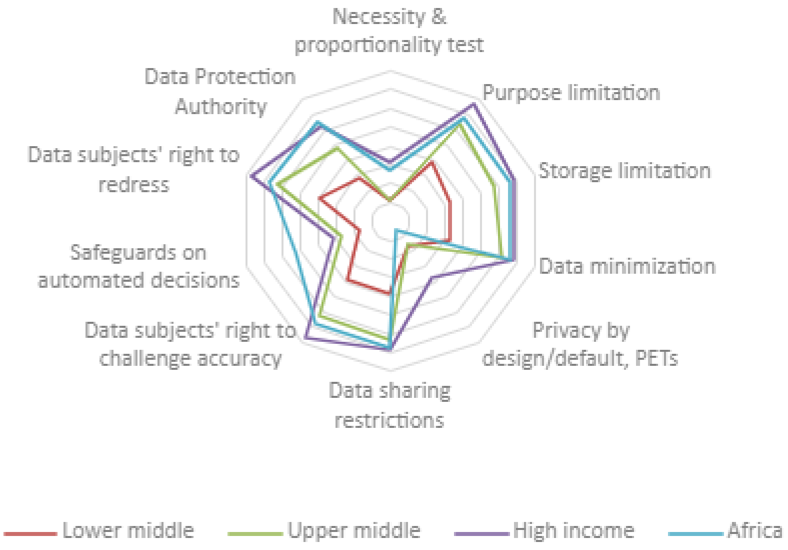


Figure V. Percent of countries per country income group that have adopted good regulatory practices on personal data protection

Source: Authors based on Global Data Regulation Diagnostic and desktop research

Box II. Good regulatory practices in the region

Recently introduced data protection acts in Africa are largely inspired by the GDPR. Compared to older frameworks in the region, they adopt a more flexible approach on data protection. Benin was one of the regional pioneers in the area of data protection, introducing a general law in 2009. In 2018, the government codified several laws related to digital technologies under its Digital Code. This new instrument updates data protection rules to account for the quick development of this area. It applies to controllers located in Benin and ECOWAS as well as those located outside the region who provide goods or services to data subjects located in Benin. Although the data protection rules under the Digital Code are largely inspired by the GDPR, legislators adapted certain provisions according to Benin's needs and capabilities. For instance, the Act leaves out legitimate interest as an alternative to consent in terms legal bases for data processing. This exception was introduced by the EU to address situations where a business may need to process information but cannot justify the need based on a legal or contractual obligation. Although individual rights are largely consistent with the GDPR, the Act provides more detailed timeframes for compliance by controllers.

In 2019, Kenya became one of the latest African countries to introduce data protection legislation. The Data Protection Act establishes individual rights while laying out obligations for data controllers and processors. The Act includes novel provisions on automated individual decision making and data protection by design. It applies to controllers and processors located in Kenya or those processing the data of individuals located in Kenya. Prior to processing personal data, controllers must conduct impact assessments to determine the measures necessary to protect the data. In the case of a breach, controllers must notify the Commissioner within 72 hours of becoming aware of it. Data controllers are required to register with the Data Protection Commissioner and to inform data subjects on the way their data is being treated. However, the Commissioner was not appointed until a year after the enactment of Act, delaying implementation. The newly appointed Commissioner later provided the thresholds required for data controller registration as well as guidelines for the commercial use of personal data.

Nigeria features a comprehensive data protection regime, with the adoption of Nigeria Data Protection Regulation (NDPR) in January 2019. The application scope is broad, including Nigerian citizens and non-Nigerian residents, as well as household activities. However, the NDPR leaves out specific requirements for the processing of sensitive data as well as data breach notifications. The Data Protection Act, passed in June 2023, is expected to fill in these gaps. Among other things, the law seeks to establish a data protection commission and to establish timelines for breach notifications. Before, data protection issues were addressed by the National Information Technology Development Agency (NITDA), which was statutorily mandated in 2007 with a broader regulatory mission, including electronic governance and information technology use. Compliance with the provisions of the NDPR by the private sector was slow, largely due to the lack of guidance by the government. Data Protection Compliance Organizations, meant to provide training and consulting services to aid compliance, were not licensed by the government until July 2019. Lack of skills has also hindered compliance, with data controllers relying on misinformation from non-experts for compliance.[22] Finally, many public bodies were still non-compliant and had not been sanctioned, raising concerns about the NITDA's independence and impartiality. After the approval of the Data Protection Act, NDPR will remain in force until they are updated.

2.4 Implementation and compliance

Although a strong legal and regulatory framework is an important first step toward achieving data governance, adequate implementation is crucial to fully reap the benefits of the digital economy and safeguard individual rights. However, the cost of compliance may lead micro, small, and medium-sized enterprises (MSMEs) with limited monetary resources to risk sanctions rather than making the required upfront expense, thereby endangering their customers' personal data.[23] Companies may also avoid foreign markets with different regulatory requirements.[24] Similarly, small governments with budgetary constraints may not devote adequate attention to this matter, failing to enforce existing data protection rules.[25]

A recent study found that although data protection may be costly for the private sector to implement, it is relatively affordable for governments to enforce.[26] Following an analysis of the costs of compliance and enforcement,[27] experts provided the following suggestions for developing countries:

- Provide clear guidelines for compliance, ensuring a clear distinction between binding law and suggestions for best practices.
- Avoid data localization requirements, as these provide no additional security and raise costs for local firms.
- Seek mutual recognition of data protection laws to reduce firms' costs of complying with several different rules when entering foreign markets.
- Provide flexibilities within the law, such exceptions for certain requirements for MSMEs, or ex post facto liability for certain infringements.

- Provide alternative models for cross-border data transfers, such as self-certification, which allow transfers to countries without an adequacy decision from the European Union subject to certain conditions.

As a result of Africa's heterogeneous data protection regulatory landscape, implementation and compliance with existing protection laws varies across countries. The examples of Morocco, Kenya, and Nigeria (Box 3) illustrate implementation challenges such as limited awareness by businesses, lack of enforcement track record that disincentivizes compliance, burdensome or unclear procedures, and limited resources at data protection entities.

Box 3. Data protection compliance and implementation in Morocco, Kenya, and Nigeria

Morocco

Morocco's Data Protection National Commission (CNDP) is tasked with enforcing compliance of the Law relating to the protection of individuals with regard to the processing of personal data, introduced in 2008. Since the Law's entry into force in 2009, the CNDP has engaged in awareness campaigns to increase compliance among the private sector and to inform the public of their rights under the Law. However, local lawyers note that when local companies hire them for assistance with data protection, the lawyers are obliged to educate company staff on the basics of the Law, including definitions such as data subject and controller. On the other hand, multinational enterprises operating in Morocco have compliance departments in place which are fully aware of the requirements under the Law and have ample experience in this regard.

Contrary to multinationals subject to foreign data protection rules such as the EU GDPR and companies in certain sectors such as finance and health, most local companies are reportedly not in full compliance of the Law. Local law firms attribute this to a lack of data protection culture among Moroccans. Furthermore, although the CNDP has issued warnings advising companies to update their policies and it assists companies with regards to filings, it has not issued any sanctions to date. This has also led to a lack of awareness about the penalties that companies can be subject to for violations of the Law. Finally, firms seeking compliance complain of a burdensome authorization procedure –particularly with regard to sensitive data— which requires time, documentation, and full cooperation of all the parties involved. As a result, most companies are obliged to hire law firms or specialists for this process which can take up to six months. According to the firms, the only cost local companies are faced with is engaging law firm services for compliance advice, as the formalities under the law are free of charge. Additionally, the CNDP allows for online filings to avoid unnecessary travel.

Moroccan enforcement agents are qualified with regard to the requirements under the Law, however they are not legal experts. Lawyers representing local companies must constantly explain legal concepts under insurance or contract law to which the company may be subject and which may shield the company from certain requirements under the data protection law. Additionally, instructions are not always consistent, depending on the agent assigned to the matter. However, as the CNDP's decisions are administrative decisions, individuals may seek review by an administrative court, which may grant legal recourse if necessary.[28] In 2016, the CNDP published its activity report, according to which the agency received 584 complaints, mostly for unwanted SMS (432), video surveillance (45), unsolicited electronic communications (33), disclosure to unauthorized parties or destruction of personal data, and illegal collection of data or reception of unwanted telephone calls. In the first half of 2020, the CNDP reported having received 429 complaints, signaling an increase in awareness of individual rights and available redress.[29]

Kenya

Kenya appointed its first Data Protection Commissioner's (DPC) in November 2020, and since then there has been significant progress towards implementation of the Act. The DPC launched a new official website, which will provide the public with data protection resources and a platform to access important information, report breaches, or seek redress. Additionally, a Taskforce on Development of Data Protection Regulations was created in January 2021, to review the existing data protection legislation and propose an implementation framework, including the Data Protection Regulation. The DPC published several guidelines, open to public participation, on data subject consent and impact assessments. The Regulations of the Office of the Data Protection Commissioner ("ODPC") were gazetted in January 2022 and took effect on 11 February 2022. The Registration Regulations provide a grace period of 6 months for compliance with the Registration Regulations; applications for registration must be submitted by 14 July 2022. However, the Commissioner must still negotiate an annual budget to be able to adequately fulfill the Office's mandate.

While some Kenyan law firms affirm that local companies are ready to comply with the Act, others find that the private sector has inadequate financial, technical, infrastructural, and human capacity, rendering compliance cost prohibitive. For companies already in compliance with other countries' data protection rules, it is almost impossible to separate procedures for specific customers based on their nationality or location. Although compliance with the law will be straightforward for these firms and firms traditionally regulated such as those in the financial sector, it will likely prove more challenging for smaller players that need to adjust their policies. According to local lawyers, companies need a grace period to comply; specific requirements highlighted as challenging for smaller companies are the appointment of a data protection officer, regular updates to the DPC regarding data processing activities, and the data subjects' right to rectification and erasure. Additionally, continuous joint stakeholder meetings between the private sector and the DPC are recommended in the implementation of the Act. Finally, lawyers highlight that rules are vague and ambiguous under the Act, and clarification by the Taskforce is necessary. The DPC recently published three sets of draft regulations and issued a call for comments from the public.[30] The agency will also carry out a set of virtual public hearings to allow stakeholders to voice their views and concerns in this regard.

The Constitution of Kenya provides a mechanism to ensure the transparency, accountability, and independence of all state corporations, including the DPC. Once the Act is implemented, any decisions made by the DPC should be published in the newly launched website, allowing for public participation in the decision-making process. Where an individual feels that a decision by the DPC is inappropriate or unjust, he or she is entitled to appeal to the High Court.

Nigeria

As noted above, Nigeria encountered some issues with its 2019 Data Protection Regulation and the new Data Protection Act is expected to address the shortcomings of the NDPR. Local lawyers are hopeful for a Data Protection Act, which would be stronger than a regulation, thereby improving compliance. They consider that the NDPR is unnecessarily broad, failing to address specific issues, and that enforcement under the Regulation is not sufficiently robust.

According to interviewed lawyers, companies do not have any issues with complying with the formalities of the Law, as there are plenty of experts in the field. They state that Nigerians have been taking data protection more seriously in recent years, and companies are taking the necessary steps to comply with the NDPR with no complaints about costs. However, they point out that there are instances when they begin assisting a company with an annual audit, as required under the NDPR, to find out that the company lacks a framework for compliance with NDPR. Companies do not see compliance with data protection rules as a priority as they were nonexistent in Nigeria prior to 2019. However, a lack of awareness is the likely culprit for this. Filings are free or inexpensive and law firm prices are reportedly very competitive.

Law firms affirm that the NITDA has engaged in data protection awareness campaigns and training. In the wake of the pandemic, NITDA organized capacity building programs to help companies submit their filings and remained responsive to enquiries from concerned stakeholders. Although the NITDA has been in operation since 2007, there have been no visible cases of enforcement due to the new nature of the Law and the implementation framework. Companies are given extended deadlines to comply as well as warnings in certain cases to ease compliance. However, the agency is limited in its enforcement capacity. Unlike other government institutions, it is not very large, and it lacks branches in many regions of the country. In February 2021, a Nigerian company was fined for a violation under NDPR, and the NITDA worked with it to assist in compliance with the NDPR. Following a determination of a breach by the NITDA, a party may approach the Administrative Redress Panel (ARP) to seek redress. However, an ARP has not been established to date. According to the NDPR, a data subject also has the right to seek redress in a court of law. Except otherwise directed by a competent court of law, decisions of the ARP are not a precondition for hearing data breach related issues in the court of law.

Source: Based on interviews carried out in 2021-2022

	Morocco	Kenya	Nigeria
Data protection law	Personal Data Protection Law, 2009	The Data Protection Act, 2019	Data Protection Regulation, 2019
Implementation regulations	Decree for the Application of Law, 2009; The Rules of Procedure of the CNDP, 2011	Data Protection Regulations published in Jan 2022	Draft Data Protection Bill, under consultation in 2022 and approved in June 2023
Data protection authority	CNDP incorporated in 2010	DPC appointed in 2020	Bill envisions DPA. Current regulation is enforced by National Information Technology Development Agency (NITDA)
Complaints received	429 between January and June 2020	No public information on number of decisions	No public information on number of decisions
Enforcement decisions	No public information on number of decisions	No public information on number of decisions	No public information on number of decisions

Table I. Implementation and enforcement of selected data protection laws by 2022

3 Cybersecurity and cybercrime

To ensure digital trust, legal and technical cybersecurity measures must be in place, including to boost the effectiveness of personal data protection regulations. Such measures protect personal data "against accidental or unauthorized destruction of accidental loss as well as against unauthorized access, alteration or dissemination".[31] Misuse or breach of sensitive data can be costly to individuals, firms, and the society. In 2016, malicious cyberactivity in the United States was estimated to result in a loss between $57 billion and $109 billion.[32] Cisco's Amazon Web Services reported that it spent $2.4 million to rectify damage caused by a former employee's illegal access and interference with the company's system. Cyberattacks can be particularly problematic for MSMEs,[33] which are unlikely to survive the financial and reputational impacts of a data breach. Individuals may face social discrimination in case of data leakages about a person's political views or sexual orientation. They also tend to suffer more economic damages than the organization targeted by the breach.[34]

A regulatory framework that imposes cybersecurity requirements on data processors and controllers and criminalizes illegal access or use of infrastructure, systems, and data is needed to address the mounting concerns on data misuse or breaches. Security requirements may include mandatory encryption of personal data, implementation of rigorous internal policies, or the appointment of a data manager. Data breach notification requirements keep data processors and controllers accountable for notifying data subjects and/or authorities of data breaches. Additionally, measures must be in place to criminalize certain online activities such as unauthorized data to a system. The creation of a national cybersecurity strategy (NCS), infrastructure and institutions –such as Computer Emergency Response Teams (CERTs) or

Computer Security Incident Response Teams (CSIRTs)— is also of key importance, as it can help to identify, investigate, and address cyber-security threats and protect key national infrastructure.

3.1 Observations of the regulatory landscape on cybercrime and cybersecurity in Africa

Africa has fallen behind with regard to measures to improve cybersecurity and combat cybercrime (Figure VI). While some countries in the region have shown moderate or high commitment in these areas, most African countries' cybersecurity and cybercrime initiatives are in the early stages.[35]

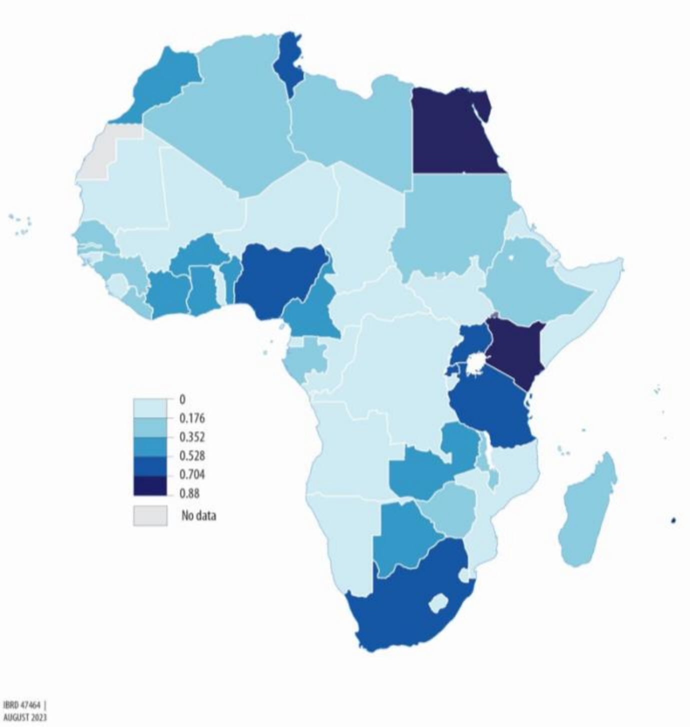


Figure VI. Cybersecurity and cybercrime frameworks in Africa

Source: ITU (2019)

Among the African countries included in the Global Data Regulation Diagnostic, much work remains to be done regarding the cybersecurity obligations of data controllers and processors. Most of the laws include broad requirements in this regard, compelling controllers and processors to ensure the integrity of the data and systems and the confidentiality of personal data (Figure VII). About half of the countries that have a general data protection law require the adoption of an internal policy to establish procedures for preventing and detecting violations and the appointment of a data protection officer. While this is a good start, other measures are recommended to ensure the adequate protection of personal data. These include ongoing assessments of security of systems that use or generate personal data and the ability to restore data and systems after a physical or technical incident. Also, processors and controllers would be advised to perform internal controls and routine risk assessments. Mauritius and Nigeria stand out as the only countries that require encryption of personal data as well as data protection awareness programs among employees.

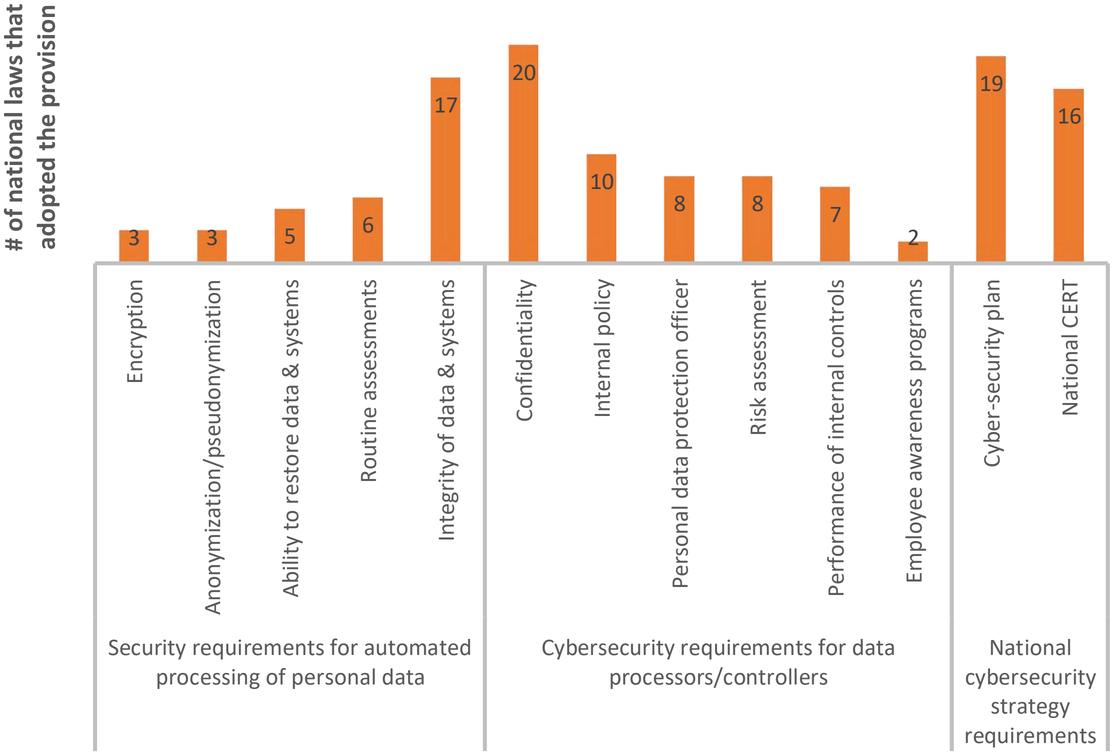


Figure VII. Comprehensiveness of African cybersecurity frameworks

Source: Authors based on Global Data Regulation Diagnostic

In contrast to a lack of comprehensive cybersecurity requirements imposed on data processors or controllers, African countries in the Diagnostic sample perform strongly on adopting provisions against cybercrime (Figure VIII). For instance, unauthorized damaging deletion, deterioration, alteration, or suppression of data collected or stored as part of databases holding personal data is identified as cybercrime in most African countries. These comprehensive provisions could provide rules of conduct and standards of acceptable behavior for online users. Such consistent rules provide a good foundation for coordinated actions to combat cybercrime activities across countries in the region.

Cybercrime rules are found in different pieces of legislation throughout the continent. In a set of countries, such as Tunisia, cybercrime rules are enshrined within the criminal code. Benin's Digital Code, which came into force in 2018, is divided into seven chapters addressing different aspects of digital activities, including a chapter dedicated to "cyber criminality and cybersecurity". Ghana took a similar approach, inserting cybercrime rules into its Electronic Transactions Act. While some countries, like Burkina Faso, cover cybercrime within their data protection laws, others, including Cote d'Ivoire, Egypt, Madagascar, Nigeria, Senegal, and Tanzania introduced laws focusing solely on cybercrime. Finally, for some countries, like Sierra Leone, cybercrime regulation is found within the telecommunications act. The Democratic Republic of Congo stands out as the only African country in the sample that has not updated its legislation to address cybercrime. Every other country studied in the region criminalizes at least the unauthorized damage, deletion, deterioration, alteration, or suppression of data collected or stored as part of databases holding personal data.

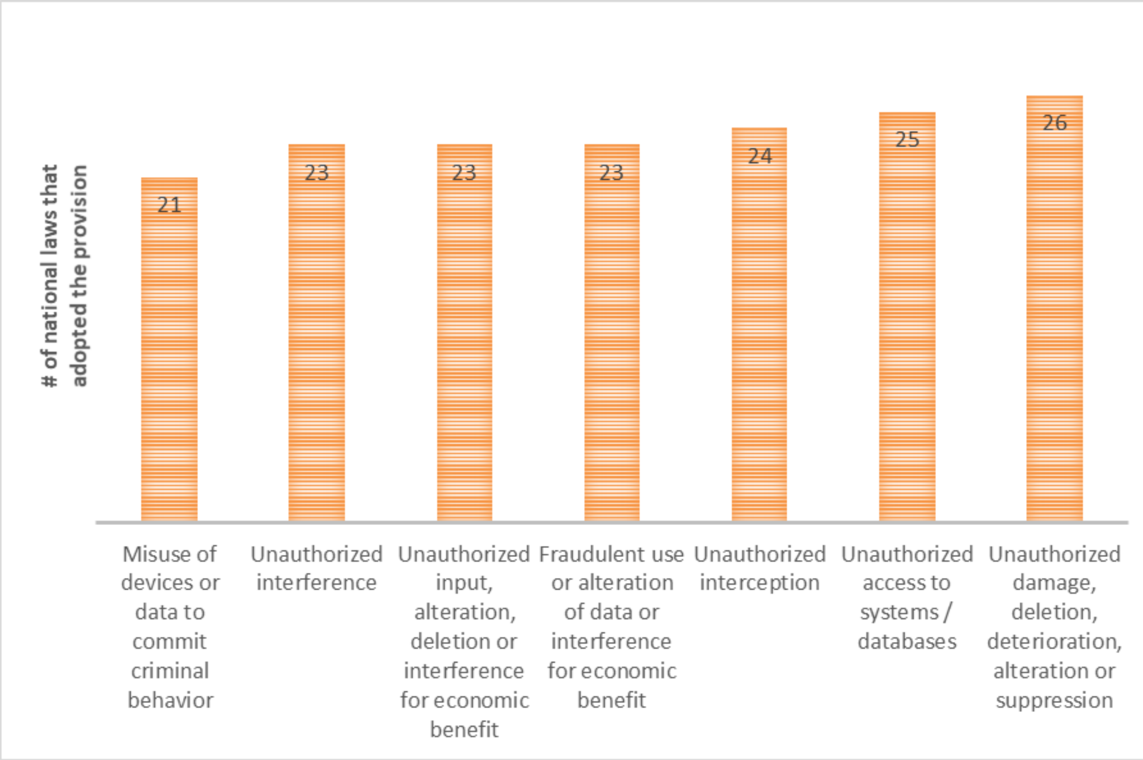


Figure VIII. Comprehensiveness of African cybercrime frameworks

Source: Authors based on Global Data Regulation Diagnostic

In addition, half of the African countries included in the sample provide for the creation of a national cybersecurity strategy, infrastructure, and institutions to identify, investigate, and address cyber-security threats. For example, Benin's national agency for information systems security, created by the Digital Code, has a set of responsibilities, including centralizing requests for assistance following security incidents on information systems and networks, maintaining a database with data breaches, and providing recommendations and assistance for the prevention of cyber threats. While some of the countries mandate either a national strategy or a national cybersecurity institution, five African countries were found lacking any of these requirements.[36] Finally, out of 44 African countries surveyed by the International Communications Union, only 13 countries had a national CERT and 14 had a NCS, making the region the worst global performer in both respects.[37] While having strong laws in place is important, an adequate institutional framework is crucial to ensure proper implementation of the strategies and enforcement of the rules.

Several African countries including South Africa, Eswatini, Zimbabwe, Mauritius, Kenya, Nigeria, Tanzania, Egypt, and Rwanda have instituted cybercrime laws or regulations that prevent the spread of false news, particularly amid the disinformation surrounding the Covid-19 pandemic. Although, as developed in this section, cybercrime and cybersecurity prevention are relevant to a proper digital development, these regulations could be used to curb freedom of speech or violate user's rights. Some examples of regulations that can create risks to data governance given their broadness of scope include Egypt's cybercrime law, which requires service providers to collect and store user's data (including phone calls and text messages) for 180 days, preventing users from communicating anonymously and creating risk of abuses or data hacks, and Rwanda's Law on Prevention and Punishment of Cyber Crimes which prohibits the publication of "rumors" giving the state ample interpretation power to prosecute speech. In this sense, the development of cybercrime regulation should be carefully designed and implemented in a transparent and accountable way to foster online expression and prevent human rights violations.[38]

3.2 Regional collaboration on cybersecurity and cybercrime

Safeguarding cybersecurity and combatting cybercrime activities are on the working agenda of a few regional organizations. The African Union Commission organized the first African Forum on Cybercrime in 2018, seeking to promote the adoption of cybercrime policies and legislation, to improve international cooperation on the fight against cybercrime, and to strengthen African criminal justice systems.[39] The AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) also includes a chapter on cybersecurity and cybercrime. Each party to the Convention is required to establish a cybersecurity policy as well as a national strategy to implement this policy. Notably, the Convention is the only regional instrument that encourages members to establish CERTs or CSIRTs to coordinate emergency responses to cyber threats. However, the Convention has not been adopted by the minimum number of members and is not in force. Initiatives to identify gaps in the Convention and other options to establish an regional framework are underway.

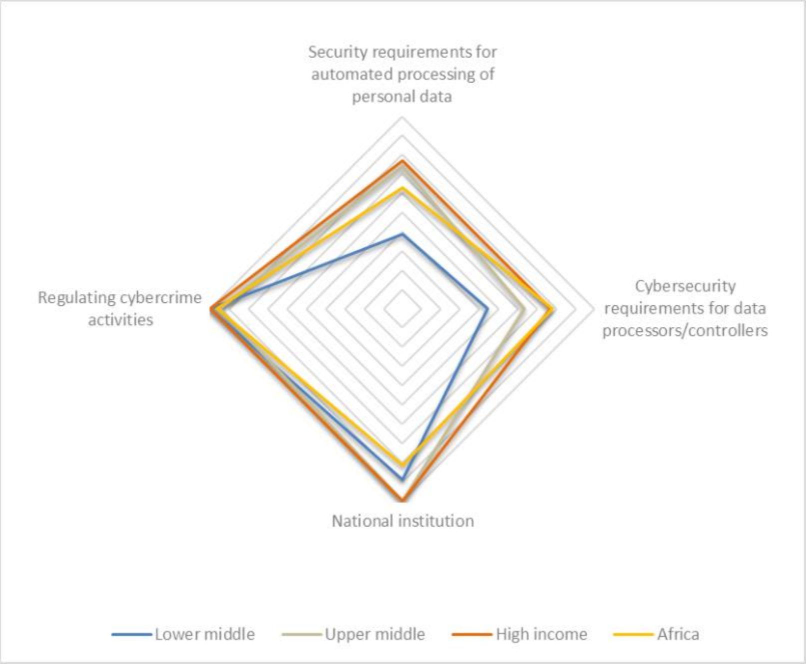
ECOWAS appears to be one of the most active African organizations on cybersecurity and cybercrime. In 2011, it introduced the Directive on Fighting Cybercrime. The Directive provides a list of offenses related to ICTs, compelling member states to adapt their procedural and criminal laws to address cybercrime issues and promotes international cooperation on cybersecurity. Although implementation is required by all member states, most member states included in the sample either have no relevant legislation or are still in the process of adopting it. Senegal stands out as the only country that had introduced cybercrime legislation prior to the Act, and Cote d'Ivoire, The Gambia, and Ghana have incorporated the Act.

Other subregions are also taking different initiatives. In 2012, the SADC published its Model Law on Computer Crime and Cybercrime. The non-binding instrument provides guidelines for the development of cybersecurity laws among member states. According to the Model Law, electronic evidence cannot be denied as evidence in court solely on the basis of being generated from a computer system, and online intermediaries are shielded from liability for cybercrimes under certain circumstances, such as expeditious removal of the infringing content upon becoming aware of it. Several SADC member states, including Mauritius, already had national cybercrime laws in place before the release of the Model Law. Following its adoption, the remaining Member States have either transposed the Model Law or have a relevant legal framework in place. In 2008, the EAC promulgated the Framework for Cyberlaws, which includes recommendations to adapt criminal laws and criminal procedure rules to address the issues presented by the use of ICTs and recommended that the Partner States accede to the Council of Europe Convention on Cybercrime. In 2016, the Economic Community of Central African States (ECCAS) adopted the Declaration of Brazzaville, seeking to harmonize national policies and regulations in the region, including cybersecurity laws and capacity building.

Finally, a few African countries have joined international efforts to combat cybercrime. The Convention on Cybercrime, also known as the Budapest Convention, is an international treaty that addresses crimes committed via the internet and other computer networks, requiring parties to criminalize certain offenses.[40] The Council of Europe drafted the Convention in 2001 and it has been ratified by 65 countries. Mauritius was the first African country to ratify the convention in 2013, followed by Senegal in 2016, and finally Ghana and Morocco in 2018. South Africa signed the Convention in 2011 but has not ratified it yet.

3.3 Africa vs. other income groups on cybersecurity and cybercrime

Compared to other countries around the world, there remains significant room for further improvement for African countries to develop robust cybercrime and cybersecurity regulatory environments (Figure IX). African countries, as well as other low- and middle-income countries are lacking a comprehensive regulatory framework to ensure cybersecurity. Mauritius is one of the few African countries that require data processors to comply with a full range of security requirements for the automated processing of personal data, including encryption, anonymization, and/or pseudonymization of personal data, ensuring integrity of data and systems that use or generate personal data, proving ability to restore data and systems that use or generate personal data after a physical or technical incident, as well as conducting ongoing assessments of security of systems that use or generate personal data. Finally, while all high-income countries in the sample adopt both a cybersecurity plan to protect key national infrastructure and a national CERT, this is the case for less than half of the African countries in the sample.



Note: Different types of cybercrime activities and different cybersecurity requirements are covered under the Global Data Regulation Diagnostic. The adoption rate reflects the percentage of countries that have adopted a full range of activities/requirements.

Figure IX. Percent of countries per country income group that have adopted good practices on cybersecurity and cybercrime

Source: Authors based on Global Data Regulation Diagnostic

Box 4. Good regulatory practices on cybersecurity and cybercrime

Two African countries have made noteworthy efforts to ensure cybersecurity and combat cybercrime. Mauritius was quick to respond to the rapidly threatening nature of the global pandemic on cyber space. In April 2020, the Data Protection Office issued a Guide on Data Protection for Health Data and Artificial Intelligence Solutions in the Context of the COVID-19 Pandemic. The Guide sought to reiterate that data protection rules were still applicable, while providing guidance for compliance under the challenging situation faced by all, including data processors. It broke down the steps for compliance, from identification of the type of data being processed to the measures needed when processing sensitive data, such as health data collected to prevent the spread of the virus. Additionally, it reminded data controllers of cybersecurity requirements which are particularly relevant in this context, such as data confidentiality. In May 2020, the Government adopted a COVID-19 emergency legislation, introducing an additional legal basis for the processing of personal data.

In 2003, Morocco supplemented the criminal code with a law on infractions relating to automated data processing systems. In 2012, the Kingdom adopted a national cybersecurity strategy and established the Strategic Committee for Information Systems Security (CSSSI). In its efforts to tackle cybercrime, it also created the Directorate General for Information Systems Security (DGSSI), responsible for developing Morocco’s cybersecurity strategy, as well as the Moroccan Computer Emergency Response Team (maCERT), in charge of responding and mitigating cybersecurity incidents of national importance. Regional forensics laboratories for digital and anti-cybercrime trace analysis we also created under the Directorate General for National Security. Morocco has also joined international efforts in this context. In 2016, the first Euro-African Cybertrust and Cybercrime Forum was held in Rabat, bringing together stakeholders from the public and private sectors to discuss a strategy to confront this issue, and in 2018 Morocco ratified the Budapest Convention on Cybercrime. Recognizing the need for skills among internet users and professionals, the Ministry of Industry, Commerce, Investment and the Digital Economy engaged in an awareness campaign, seeking to ensure that all Moroccans have the tools to avoid falling victim to cybercrime. Moroccan SMEs needing compliance assistance have also received expert advice from government agencies.

3.4 Implementation of cybersecurity initiatives

Throughout the continent, governments have engaged in initiatives to improve cybersecurity. Like data protection, the maturity of cybersecurity capacity varies greatly across Africa, with some countries that have not introduced a cybersecurity framework, others that have but failed to implement it, and others that have taken the appropriate measures toward a successful cybersecurity strategy.

Benin

Although the Government of Benin announced the development of a National Cybersecurity Strategy in 2018, it has not been adopted to date.[41] The bjCSIRT, established under the Digital Code, is responsible for responding to national cybersecurity incidents. However, there is a lack of communication and collaboration among the relevant stakeholders. Additionally, the country lacks critical infrastructure protection, leaving room for vulnerabilities. No cybersecurity crisis management plan exists at the national level. Following the adoption of the National Cybersecurity Strategy in 2020, stakeholders expected a decree to be issued to establish a national critical infrastructure framework.

Benin’s Digital Code includes a comprehensive section on Cybercrime and Cybersecurity. The section contains substantive and procedural provisions related to crimes committed online. Cybercrime matters are handled by the National Police’s cybercrime division, and other units are encouraged to communicate with the division when necessary. Agents in the division as well as in other law enforcement agencies in the country have received cybercrime capacity building from other countries and international organizations. Finally, the Division holds periodic training for leaders in local agencies throughout Benin. Nonetheless, stakeholders highlight a lack of relevant knowledge in the judicial branch, leading to a limited capacity to handle cybercrime cases.

Liberia

Liberia has no national cybersecurity strategy or program in place.[42] Since 2019, the Telecommunications Authority and the Ministry of Posts and Telecommunications have been collaborating on the drafting of a national cybersecurity strategy. Once the draft is ready, they intend to meet with stakeholders from the public and private sectors to review it. The current draft strategy envisions the creation of LB-CERT, which would fill the existing void with regard to national incident response.

The Draft Cybercrime Act provides for the creation of a Critical National Information Infrastructure. However, no critical infrastructure framework has been established to date, and there is no communication among critical infrastructure operators. Furthermore, the country has no national cybersecurity emergency response plan nor a cyber defense strategy.

Liberia has no legal framework for cybersecurity or cybercrime. Citizens rely on broader laws to address these issues, such as the Criminal Procedure Law, the Telecommunications Act, and the Intellectual Property Act. Although a Cybersecurity Act has been submitted for review, there is no indication as to when it will be approved. Finally, there is a shortage of relevant skills among law enforcement agents, who rely on traditional measures when responding to cybercrime issues.

Nigeria

Nigeria released its Cybersecurity Policy and Strategy in 2014.[43] However, implementation has not been effective, mostly due to a lack of coordination among the relevant agencies. The Strategy established ngCERT, to coordinate activities, facilitate cooperation among relevant stakeholders, and communicate with international and multilateral organizations. Although the team has skilled analysts and managers, capacity building is crucial to be able to carry out ngCERT's mandate. Furthermore, there are several other national agencies, such as the Ministry of Communications, the National Police, and the Ministry of Justice, working independently with scarce resources and insufficient authority, resulting in an inadequate response to cybersecurity issues.

The Strategy also calls for the creation of a National Cybersecurity Coordination Center, which has not been established to date. Although the ngCERT is responsible for coordination, it lacks the resources and capacity to guide and support sectoral CERTs. Finally, although the Strategy highlighted the need for a Critical National Information Infrastructure, this has not been implemented.

	Benin	Liberia	Nigeria
National Cybersecurity Strategy	Announced in 2018, not yet adopted	Strategy being drafted	Released in 2014
Cybersecurity crisis management plan	None	None	None
Emergency Response Team	bjCSIRT	LB-CERT envisioned under draft cybersecurity strategy	ngCERT
Critical information infrastructure	None; envisioned under cybersecurity strategy	None; envisioned under Draft Cybercrime Act	Established under strategy; not yet implemented

Table II. Implementation and enforcement of cybersecurity rules

4 Data regulation and governance

Laws and regulations play an important role in determining the cost of transaction in economic activities and shaping the public's perception on governments. A data governance environment, exemplified by the robustness of the regulatory framework on personal data protection and cybersecurity and cybercrime is also essential in engendering trust in digital economic activities and government accountability and transparency.[44] Regulations that lay out rights and responsibilities of market players provide them "a recourse to institutionalized forms of redress in the case of trust breaches". Effective enforcement of such regulations also boosts public confidence in government capability.

In African countries with more comprehensive and robust data governance regulatory frameworks, there is a higher level of public perception on regulatory quality. Such perceptions reflect the public's belief on the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development. Moreover, countries that have adopted more regulatory good practices on cybersecurity and cybercrime, have more confidence on the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies. This shows that countries with a better rule of law tend also to have stronger frameworks on cybersecurity and cybercrime. The moderate level of positive association between data governance environments and the public's perception on government implies the importance of data regulations, and more research shall be conducted to explore a causal relationship. Moreover, the association between country's personal data protection regulatory environment and regulatory quality is not particularly high. This might reflect that personal data protection is only one aspect among various needed efforts for governments to enhance public confidence but also that there are delays in adopting data protection rules.

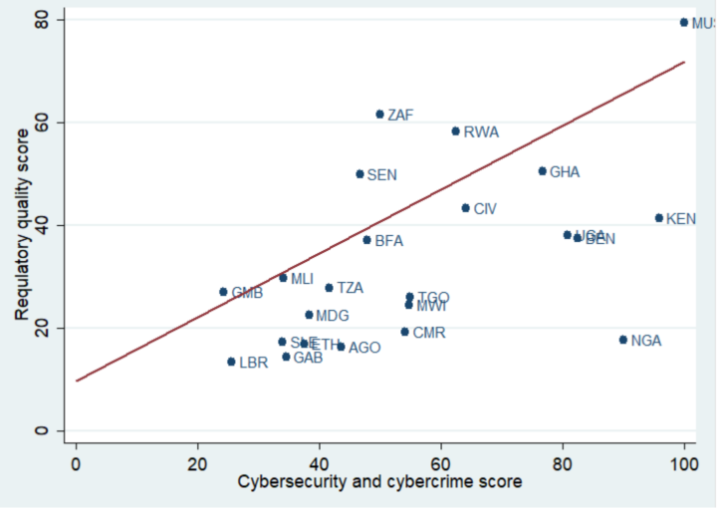


Figure IX. Regulatory quality and cybersecurity and cybercrime score

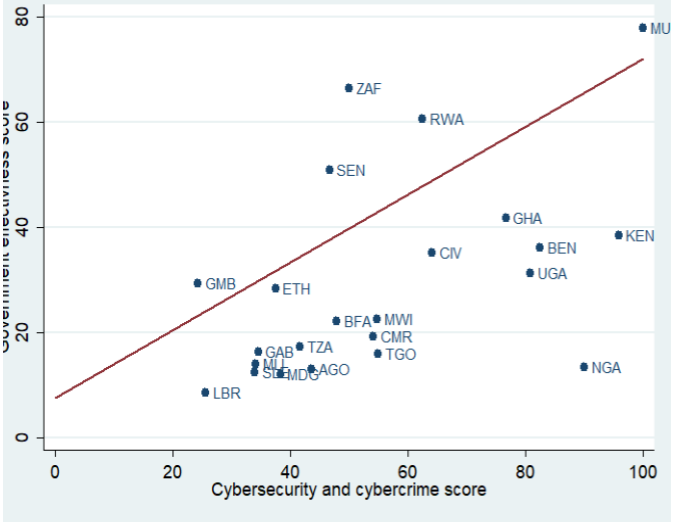


Figure X. Government effectiveness and cybersecurity and cybercrime score

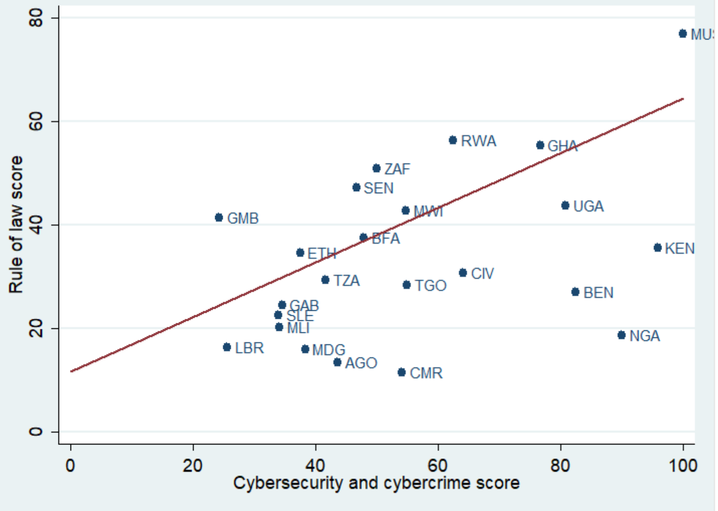


Figure XI. Rule of Law and cybersecurity and cybercrime score

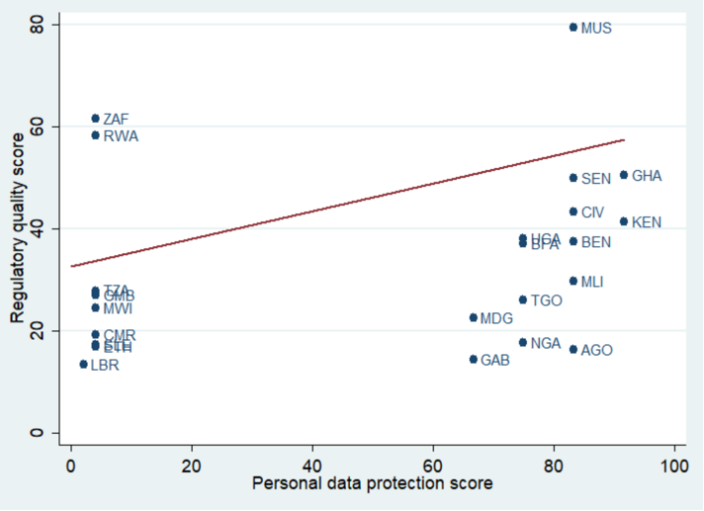


Figure XII. Regulatory quality score and personal protection score

Note: Data on "Government Effectiveness", "Rule of Law", and "Regulatory Quality" are from the World Governance Indicators. The correlation coefficients between cybersecurity and cybercrime score and Government Effectiveness score is 0.50; between cybersecurity and cybercrime score and Regulatory Quality is 0.55; between cybersecurity and cybercrime score and Rule of Law score is 0.44; between Personal data protection score and Regulatory Quality score is 0.25.

5 Use and reuse of data and cross border data flows

5.1 Enabling the use/reuse of public intent and private intent data

Creating a trusted environment to facilitate data economic activities not only requires robust safeguards to protect personal data and ensure cybersecurity, but also needs enablers to facilitate the use and reuse of public and private intent data. Public intent data is defined as data collected for public purposes while private intent data is collected by the private sector as part of routine business process.[45] Enablers include applying open data laws or policies on public sector data, granting citizens with access to information rights to request access to government records or data, facilitating data portability, and adopting an open licensing regime.

Compared to other regions, Africa performs poorly on facilitating the use of public intent data (Figure XIII). Less than a fifth of the African countries in the Global Data Regulation Diagnostic require public entities to use common technical standards that enable interoperability of systems, registries, and databases. Such an interoperable system could be effective in providing e-government services. In addition, compared to other low and middle-income countries, Africa has the lowest adoption rate on mandatory use of common data classification categories across all government database applications or document management systems. It is worth noting that most of the African countries studied have Right to Information/Access to Information (ATI) legislation, granting individuals the right to request access to government records or data, and providing exceptions to this right. However, such ex-post guarantee of accessing government information or data is not sufficient. Open Data Acts or open data policies are needed to provide an ex-ante channel to advocate the sharing and using of public data. Nevertheless, about half of the African countries analyzed do not have an Open Data Act or an open data policy applicable across the entire public sector. Furthermore, although most African countries have established ID systems that use digital technologies, almost half of the population in sub-Saharan Africa lack an official proof of identity.[46]

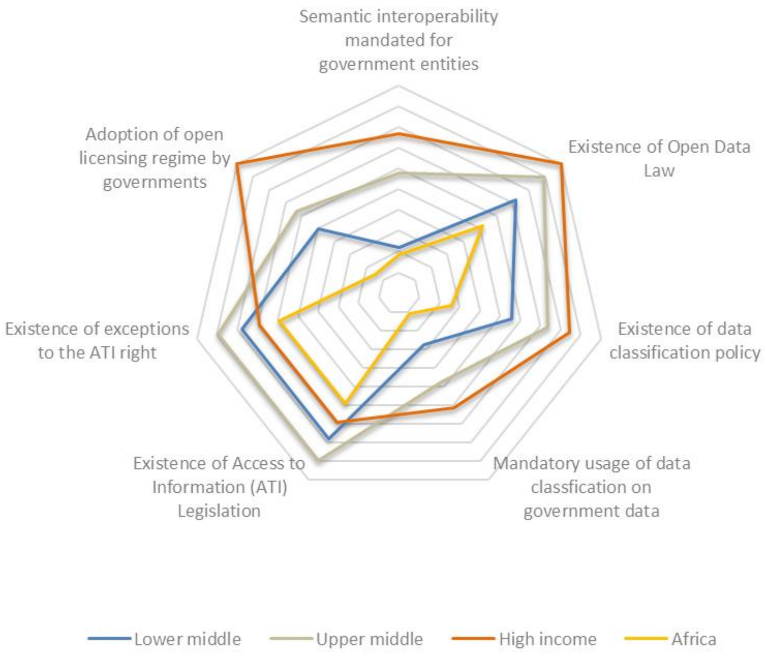


Figure XIII. Percent of countries per income group that have adopted good practices on public intent data

Source: Authors based on Global Data Regulation Diagnostic

These results are consistent with other open data diagnostic tools, such as the World Wide Web's Open Data Barometer. The Barometer measures the extent to which governments publish and use open data for accountability, innovation, and social impact. According to a review of 30 in Sub-Saharan African countries in the 2016 edition of the Barometer, the region lags in terms of implementation and impact of open data.[47] Kenya stood out as the regional leader, coming in at 35th globally. In North Africa, the Barometer found little progress on open data. Although some African countries showed some interest in open data initiatives, little effort had been made to implement them. Open Knowledge International's Africa Open Data Index compares the extent to which open government data is published around the world. These two tools fed into the 2018 Africa Data Revolution Report, which found that a lack of information on government agency websites results in confusion about which data is considered authoritative.[48] Less than one fourth of the datasets studied by the Index are available online in the African countries covered. Where data is published, only one third of the data is updated in a timely manner. Finally, out of 420 datasets analyzed, only 28 are openly licensed, allowing the public to use the information for any purpose.

With regards to private intent data, though most transactions are contractual based among private sector players, an enabling environment could help facilitate data sharing and the use/reuse of private intent data. Further endeavors are needed to create an enabling environment in Africa (Figure XIV). For instance, only about a tenth of the countries allow private sector service providers to digitally verify or authenticate the identity of a person against data stored in the ID system. In Nigeria, per the National Identity Management Commission Act, 2007, National Identification Number (NIN) can be digitally verified or authenticated, which helps ensure various e-transactions are conducted in a smooth and transparent manner. In more than 85 percent of the African countries studied, individuals do not have the right to obtain their data processed by a controller in a structured, commonly-used and machine-readable format and to request the data transferred to another service or product provider (data portability). Limitation on data portability prevents switching of service providers and could potentially result in hoarding of valuable data by existing players thus inhibiting innovation. Finally, none of the African countries studied allow standard-setting organizations to mandate patent or intellectual property right (IPR) holders to provide voluntary licensing access to "standard essential" data or applications on FRAND (fair, reasonable, and non-discriminatory) terms, falling behind upper-middle and high-income countries.

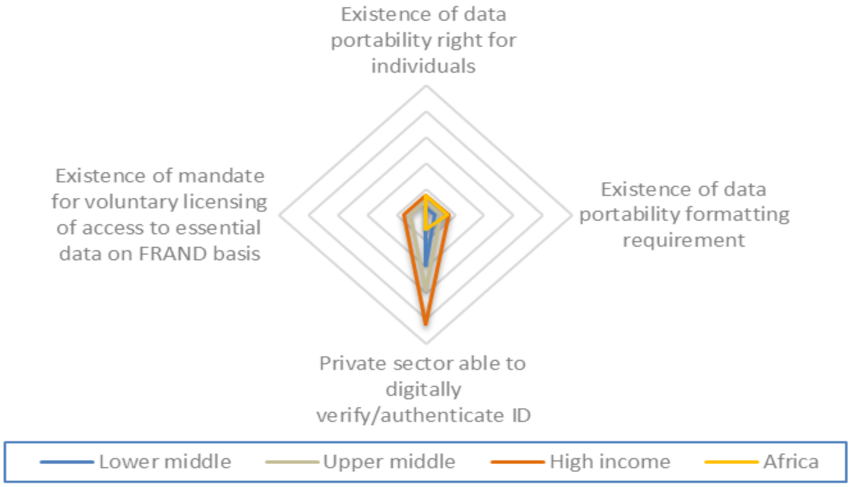


Figure XIV. Percent of countries per income group that have adopted good practices on private intent data

Source: Authors based on Global Data Regulation Diagnostic

5.2 Cross-border data flows

The ability to transfer data across borders is an increasingly important pillar of economic competitiveness.[49] Countries have implemented different approaches to foster data flows while at the same time protecting personal data, digital security, and intellectual property.[50] Conditioning the movement of data across borders or mandating that data is stored locally are the two main strategies implemented.[51]

The mechanisms through which countries, collectively or individually, have regulated cross-border data flows are highly diverse. In this sense, Casalini, López-González & Nemoto (2021) have identified four regulatory approaches:

- Unilateral mechanism: where a country regulates under which conditions and which data can exit its territory. These regulations can establish "open safeguards" in which the private entity has discretion in deciding whether to transfer the data; on the contrary, the "pre-authorized safeguards" require public sector approval for the transfer.

- Trade agreements: since 2008, 29 trade agreements involving 72 countries have included data flows regulation into their provisions.
- Standards and technology-driven initiatives: data is central to technological innovation. In consequence, the design of standards increasingly includes provisions on data transfers.
- Plurilateral arrangements such as the Council of Europe Convention 108 or 108+ or the Malabo Convention if it enters into force: despite the fact that there are several international agreements regulating cross-data flows Casalini, López-González & Nemoto (2021) have shown that there is a significant overlap between these agreements which would facilitate the implementation and the flow of data across borders. Plurilateral agreements can also set the basis for interoperability between national frameworks.

The fragmentation and plurality of regulations on cross-border data flows have brought, on many occasions, uncertainty and undermined the objectives toward which they were implemented. Like personal data protection regulation, which was analyzed in Section 2.2, fostering clear and interoperable regulations across countries is essential to simplify the implementation of data regulations both from a private and public perspective. This approach is more feasible in the short term while harmonization could be a target in the long term.

Among unilateral mechanisms, adequacy and accountability approaches are two typical ways for cross-border transfers of personal data. The adequacy approach, also known as pre-authorized safeguards, allows transfers to countries that afford an equivalent level of data protection. This is the approach adopted by half of the African countries analyzed. For example, Kenya allows personal data transfers where the controller or processor has given proof to the Commissioner that the laws in the country where the data is being transferred are equivalent and that the transfer is necessary. Other African countries, like Ghana, adopt the accountability approach, holding the controller responsible for ensuring that the recipient of the data complies with the personal relevant laws. In Madagascar, Togo, and Senegal, if the destination country does not afford an adequate level of data protection, the DPA can authorize the transfer if the controller ensures the protection of the data through contractual clauses or internal rules.

Although cross-border flow of data can bring benefits to societies promoting new business models and fostering the growth of the data-driven economy, countries are setting limitations due to security, economic, and political concerns.[52] As data traffic grows, it also brings challenges as hacking, data breaches, and the possibility of citizens to be exposed to surveillance. In an attempt to foster the positive externalities of data flows while preventing its negative ones, governments have implemented different data sovereignty regulations aiming to protect the personal data of their citizens, promote economic development, and protect national security. These policies can take many forms, including data localization requirements imposing companies the burden of storing the data, or a copying of it, in the territory of that country, or subject the use and transfer of data to certain regulations. In some cases, these rules can also facilitate surveillance and censorship, highlighting the need of accountability for data policy implementation. Globally, these policies are reshaping how states relate between each other and internally with their own societies.

This debate surrounding data sovereignty and data localization has gained traction in Africa. For example, South Africa's Minister of Communications and Digital Technologies published the Draft National Data and Cloud Policy for public comments on April 2021. This Draft expressly mentions data sovereignty as one of the objectives of the regulation and establishes data localization requirements, which compel the storage or processing of data within the country where the service is provided. This draft also proposes the implementation of data protection and privacy rules to the transfer of data. Countries are taking different approaches for data localization. Nigeria's Guidelines for Content Development in ICT requires companies to store subscriber and consumer data within the country, while South Africa's Draft National Data and Cloud Policy envisions a different approach, allowing the cross-border transfer of the data, but requiring that a copy of the data be stored in the country for law enforcement purposes. In Africa, there are initiatives such as the African Union Data Policy, the African Network of Data Protection Authorities and the Smart Africa Data Protection Program, which provide fora to discuss approaches to facilitate and regulate cross-border data flows, but implementation is the main challenge.

Governments can also promote data usage and data related business by fostering the development of proper technological infrastructure. The growing dependance on digital technology to conduct business and daily tasks requires an infrastructure that can accommodate the need for internet access and data processing. Several African countries have moved in this direction by promoting public investment in, for example, data centers. An example of this tendency is Togo's state-owned data center in Lomé, that was inaugurated in January 2021 to accommodate the country's need for more processing capacity both by the state and the public sector. For these policies to be effective, appropriate management structures are needed to ensure that data infrastructure is operated efficiently, keeps up with technological progress, including to protect and secure data, provides services and prices that respond to users' needs, and that public data infrastructure does not crowd out private initiatives.

Despite the justifications related to data protection, national security, and cross-border law enforcement, data localization, and state data infrastructure are not necessarily the most effective policy instruments and raise risks of negative impact on a country's ability to participate in the global economy, attract private (including foreign) investment and boost cross-border trade. Cory and Dascoli (2021) estimate that restricting data flows reduces the total volume of trade, lowers productivity, and increases prices for data-based downstream industries. Furthermore, locating servers in a specific country is the opposite of a cybersecurity measure, as the data may be better protected and distributed in servers in different jurisdictions.[53] Even with data localization rules, international collaboration is needed given the transnational nature of digital services and crime, but also considering that electronic evidence is relevant for various investigations, including on antitrust, taxation, and money laundering involving non-digital economic activities. For this, more effective mutual legal assistance treaties would be needed.

Burdensome, complex and disproportionate rules on cross-border personal data transfers can result in substantial costs for businesses, especially small and medium-sized enterprises. The aim should be to adopt a risk-based approach, with more stringent cross-border data flows rules where it is necessary to protect more sensitive personal information and essential security interests. Cloud computing allows users to store, manage, and process data remotely in other countries, which is highly beneficial to users – including digital business startups - who can choose to pay only for the quantity and time needed.[1] Ensuring that data protection frameworks permit African citizens and firms to access those services while protecting personal data is important.

6 Conclusion

A robust data governance environment and a sustainable digital economy are of great importance for Africa to ride the current wave of digital technology advances and to reap the digital dividends while avoiding the inherent risks. Among the various aspects that define a data ecosystem, data regulation and cybersecurity are two important aspects to boost digital trust and therefore the use of data-based digital technologies, while rules on the use, transfer and re-use of data are important to enable for innovation and development of digital technologies. Nonetheless, African countries still lag on many of the different regulatory dimensions compared to other income group countries. As can be seen in Figure XV, African countries have similar standards to upper middle-income countries, but fall behind high-income ones when it comes to e-commerce or online transactions, personal data protection, cybersecurity, and cybercrime protection. These results show that although there has been progress in these aspects, there is still more to be done to promote a proper data framework. Similarly, the analyzed Sub-Saharan African countries have average scores closer to high income countries when it comes to non-personal data protection, a standard where upper middle-income countries seem to lag. Finally, the analyzed countries ranked lower compared to high, upper, and lower middle-income countries when it comes to enabling the use of public and private intent data, showing that these dimensions need particular attention from regulators to foster the development of a more comprehensive usage of the data available. This includes adopting policies to facilitate cross-border data flows in a way that security is preserved, and data-driven solutions are developed for African citizens and firms.

Over half of the countries in Africa have introduced general data protection legislation, applicable to all sectors. Many of the regulatory frameworks have adopted a variety of good regulatory practices such as data minimization, purpose limitation, and right to redress. However, more novel practices such as data protection by design and data protection by default are not prevalent. Adoption and implementation of such practices require not only legal recognition but also advanced technology infrastructure which is missing in Africa. Furthermore, legally mandated DPAs in the continent are not always well-resourced or functional, hindering the implementation and enforcement of the laws. The establishment of a capable and effective enforcement authority is key to ensure adequate implementation of data protection legislation.

Cybersecurity concerns are mounting in the region with increasing incidences of data breaches and leakages. The regulatory environment to safeguard cybersecurity is far from complete in the region. Very few countries have required data processors and controllers to comply with a full range of security requirements for the automated processing of personal data or imposed a series of cybersecurity requirements on data processors and controllers. Mauritius is the best performer in the region in this regard. It was also quick to adopt emergency initiatives to respond to potential threats in cyberspace during the COVID-19 pandemic. However, about a third of the African countries analyzed do not have a cybersecurity plan to protect key national infrastructure or a national CERT. Cybersecurity strategies, infrastructure, and institutions are key factors to identify, investigate, and address cyber-security threats and protect key national infrastructure. In contrast to the gap in adopting cybersecurity measures, many

African countries have promulgated provisions to regulate cybercrime activities. Such consistent rules could help facilitate coordinated actions across countries to combat cybercrime activities.

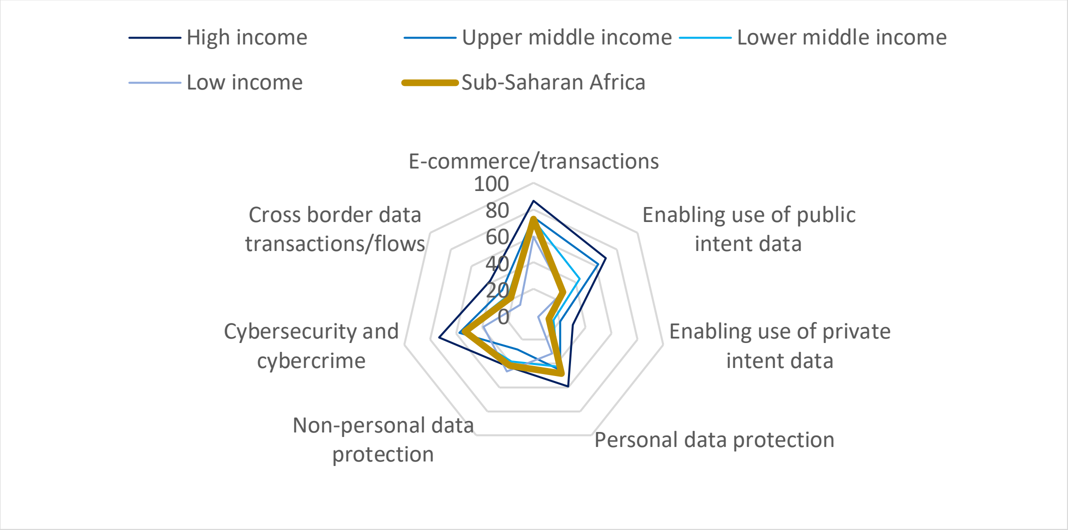


Figure XV. Average scores on different data governance dimensions by income group/region

Integration is a key component to achieving economies of scale. A few African regional communities, including ECOWAS and the African Union, have taken initiatives to promote regional integration on personal data protection. Similarly, the AU Commission, ECOWAS, and the SADC have included safeguarding cybersecurity and combatting cybercrime activities in the working agendas, given the importance of integration to have economies of scale. Finally, African countries have joined international efforts to safeguard personal data and combat cybercrime and some African countries have signed the Council of Europe's Convention 108 (and more recently 108+) and the Convention on Cybercrime. Ensuring interoperability of national frameworks by joining international conventions or establishing an adequacy framework or safe harbors mechanism to allow for cross-border data sharing with appropriate safeguards is important from a regional digital economy perspective.

Enabling data regulation environments that provide adequate safeguards contribute to shaping public trust. More comprehensive and robust data governance regulatory frameworks are associated with a higher level of public perception of regulatory quality. Regulatory provisions on cybersecurity and cybercrime are particularly positively related to more confidence in the quality of public services and the credibility of the government's commitment. Adequate institutions and regulation are crucial to implement data governance frameworks that encourage investments to develop and use digital solutions, and thereby reap the benefits of the digital economy.

7 References

Albarran, A. B. 2000. Electronic commerce. In A. B. Albarran & D. H. Goff (Eds.), Understanding the Web: Social, political, and economic dimensions of the Internet (pp. 73–94). Ames: Iowa State University Press.

AlGhamdi, Rayed, Steve Drew, and Waleed Al‐Ghaith. 2011. "Factors Influencing E-Commerce Adoption by Retailers in Saudi Arabia: A Qualitative Analysis." The Electronic Journal of Information Systems in Developing Countries47(1): 1‒23.

African Union. 2022. African Union Data Policy Framework

African Union. 2018. The First African Forum on Cybercrime.

Bartley Johns, Marcus, Mombert Hoppe, Martin Molinuevo, Konesawang Nghardsaysone, and Lillyana Sophia Daza Jaller. 2018. Taking advantage of e-commerce: legal, regulatory and trade facilitation priorities for Lao PDR. Washington, DC: World Bank.

Bennett, Colin, and Charles Raab. 2006. The Governance of Privacy. MIT Press.

Bowmans. 2021. Data Protection in Kenya: New Developments. March 2. https://www.bowmanslaw.com/insights/data-protection/data-protection-in-kenya-new-developments/.

—. 2021. Public Participation on the draft Data Protection Regulations. April 20. https://www.bowmanslaw.com/insights/data-protection/public-participation-on-the-draft-data-protection-regulations/.

—. 2020. "Welcoming the Appointment of Kenya's First Data Protection Commissioner." November 25. https://www.bowmanslaw.com/insights/data-protection/welcoming-the-appointment-of-kenyas-first-data-commissioner/.

Casalini, Francesca, and Javier López-González. 2019. "Trade and Cross-Border Data Flows." OECD Trade Policy Papers, no. 220.

Casalini, Francesca, Javier López-González, and Taku Nemoto. 2021. "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers ." OECD Trade Policy Paper no. 248.

Chander, Anupam, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu. 2021. "Achieving Privacy : Costs of Compliance and Enforcement of Data Protection Regulation." Policy Research Working Paper; No. 9594, World Bank. https://openknowledge.worldbank.org/handle/10986/35306.

Chen, Rong. 2021. Mapping Data Governance Legal Frameworks Around the World: Findings from the Global Data Regulation Diagnostic. Policy Research Working Paper; No. 9615. © World Bank, Washington, DC. http://hdl.handle.net/10986/35410 License: CC BY 3.0 IGO.

Cimpanu, Catalin. 2020. "Personal data of 16 million Brazilian COVID-19 patients exposed online." ZDNet.

CNDP. 2020. "Bulletin CNDP: Tiers de Confiance Numérique." https://www.cndp.ma/images/bulletin/Bulletin-CNDP_Tiers-de-Confiance-Num%C3%A9rique-N01.pdf.

Corfield, Gareth. 2020. "Personal data from Experian on 40% of South Africa's population has been bundled onto a file-sharing website." The Register. September 14. Accessed August 5, 2021. https://www.theregister.com/2020/09/14/south_africa_experian_data_breach_wesendit/.

Cory, Nigel and Luke Dascoli. 2021. How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology & Innovation Foundation.

Council of Europe. 2001. "Convention on Cybercrime."

DataGuidance. 2021. Global Privacy Laws. https://www.dataguidance.com/advisories/global-privacy-laws.

Daza Jaller, Lillyana, Simon Gaillard, and Martin Molinuevo. 2020. The Regulation of Digital Trade: Key Policies and International Trends. Washington, DC: World Bank.

Daza Jaller, Lillyana, and Martin Molinuevo. 2020. Digital Trade in MENA: Regulatory Readiness Assessment. Policy Research Working Paper, Washington, DC: World Bank.

Díaz Hernández, Marianne, Rafael Nunes, Felicia Anthonio, and Sage Cheng. 2021. "#KeepItOn update: who is shutting down the internet in 2021?" Accessnow. June 7. Accessed August 5, 2021. https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/.

Feldman, Sarah. 2019. "Governments Are Shutting Down the Internet More INTERNET ACCESS." Statista.com. April 24. Accessed August 5, 2021. https://www.statista.com/chart/17794/number-of-internet-shutdowns-by-government/.

Ganguly, Meenakshi. 2019. "Kashmir Shutdown Raises Healthcare Concerns." Hrw.org. August 30. Accessed August 5, 2021. https://www.hrw.org/news/2019/08/30/kashmir-shutdown-raises-healthcare-concerns.

Gordon, Lawrence A, Martin P Loeb, William Lucyshyn, and Lei Zhou. 2015. "Increasing Cybersecurity Investments in Private Sector Firms. Journal of Cybersecurity." Journal of Cybersecurity 1 (1): 3-17.

Human Rights Watch. “Abuse of Cybercrime Measures Taints UN Talks,” May 5, 2021. https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

ICO. 2021. Guide to the General Data Protection Regulation (GDPR). Information Commissioner's Office.

ITU. 2019. Global Cybersecurity Index 2018. International Telecommunications Union.

Klein, Sam. 2015. "The Data Is in the Details: Cross-Border Data Flows and the Trans-Pacific." The Diplomat. November 23.

Koske, Isabell, Rosamaria Bitetti, Isabelle Wanner, and Ewan Sutherland. 2014. "The Internet Economy - Regulatory Challenges and Practices." OECD Economic Department Working Papers (OECD Publishing) 1171.

Makoni, Munyaradzi. 2020. "Cyberattack surge highlights Africa security risk - Sub-Saharan Africa." SciDev.Net. August 10. https://www.scidev.net/sub-saharan-africa/news/cyberattack-surge-highlights-africa-security-risk/.

McAfee, and CSIS. 2018. "Economic Impact of Cybercrime- No Slowing Down."

McCarthy, Niall. 2020. "The Countries Shutting Down The Internet The Most." Statista.com. January 22. Accessed August 5, 2021. https://www.statista.com/chart/15250/the-number-of-internet-shutdowns-by-country/.

Ndhlovu, Lungelo . 2019. "Facing internet restrictions, journalists turn to VPNs." Ijnet.org. May 26. Accessed August 5, 2021. https://ijnet.org/en/story/facing-internet-restrictions-journalists-turn-vpns.

OECD. 2013. Privacy Framework. Paris: OECD.

OECD. 2015. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Paris: OECD.

Oloyede, Ridwan. 2020. "Nigeria: One year of the Data Protection Regulation." DataGuidance.

Osborne, Charlie. 2020. "Working from home causes surge in security breaches, staff 'oblivious' to best practices." ZDNet. August 20. https://www.zdnet.com/article/working-from-home-trend-causes-surge-in-cybersecurity-costs-security-breaches/.

Smart Africa. 2020. December 21. https://smartafrica.org/.

Toka Cyber Builders. 2020. "Supporting Nigeria's Cybersecurity Readiness and Strategy Implementation."

UNCTAD. 2016. Data protection regulations and international data flows: implications for trade and development. New York and Geneva: United Nations.

UNICRI. 2015. Guidelines for IT Security in SMEs. Turin: United Nations.

United States Council of Economic Advisers. 2018. "The Cost of Malicious Cyber Activity to the U.S. Economy." CEA Report, February 16.

Van Bell, Jean-Paul. 2018. Africa Data Revolution Report 2018: The Status and Emerging Impact of Open Data in Africa. Centre for Information Technology and National Development in Africa (CITANDA).

West, M. Darrell. 2016. Internet shutdowns cost countries $2.4 billion last year. Governance Studies, Washington DC: Center for Technology Innovation at Brookings Center.

World Bank Group. 2021. "Data for Better Lives." World Development Report 2021, Washington DC.

World Bank. 2018. "ID4D Global Dataset." Washington, DC.

World Bank. 2020. "Cybersecurity Capacity Review: Benin."

World Bank. 2020. "Cybersecurity Capacity Review: Liberia."

World Wide Web. 2016. Open Data Barometer Fourth Edition: Sub-Saharan Africa Regional Snapshot.

[1] BCG (2019).

[2] Suri (2017).

[3] (Makoni, Cyberattack surge highlights Africa security risk 2020)

[4] (Corfield, Personal data from Experian on 40% of South Africa's population has been bundled onto a file-sharing website 2020)

[5] See Preamble, African Union Convention on Cyber Security and Personal Data Protection.

[6] Cory and Dascoli (2021)

[7] World Bank Group (2021).

[8] Chen (2021). The World Development Report 2021 conducted a Global Data Regulation Diagnostic. The Diagnostic is based on a detailed assessment of domestic laws, regulations, and administrative requirements in 80 countries. Data are collected through standard questionnaires which are completed mainly by lawyers specializing in ICT and data governance. Data are further verified through detailed desk research of legal texts, reflecting the regulatory status of each country as of June 1, 2020.

[9] The African countries included in the Global Data Regulation Diagnostic analysis are Angola, Benin, Burkina Faso, Cameroon, Democratic Republic of Congo, Cote d'Ivoire, Egypt, Ethiopia, Gabon, The Gambia, Ghana, Kenya, Liberia, Madagascar, Malawi, Mali, Mauritius, Morocco, Nigeria, Rwanda, Senegal, Sierra Leone, South Africa, Tanzania, Togo, Tunisia, and Uganda.

[10] Albarran, A. B. (2000); AlGhamdi et al. (2017).

[11] Constructed from the expressed "privacy-related" concerns of individuals in 41 countries. Data are drawn from GlobalWebIndex's Q1–Q4:2018 research waves among a sample of 391,130 internet users aged 16–64. Respondents are representative of the online populations of the markets covered.

[12] Datum Future and GlobalWebIndex (2019).

[13] Fernandez Vidal and Medine (2019).

[14] CIGI-Ipsos (2019)

[15] Daza Jaller and Molinuevo (2020); UNCTAD (2016); OECD, Privacy Framework (2013)

[16] In addition to the data obtained from the Global Data Regulation Diagnostic, desktop research was conducted to analyze the existing data protection legal frameworks in every African country.

[17] Bennett and Raab (2006)

[18] Daza Jaller, et al. (2020)

[19] UNCTAD (2016)

[20] The countries that have ratified the Convention are Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, and Senegal.

[21] The framework was published in July 2022 and is available at https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

[22] Oloyede (2020)

[23] Chander, et al. (2021)

[24] Chander, et al. (2021)

[25] Chander, et al. (2021)

[26] Chander, et al. (2021)

[27] Chander, et al. (2021)

[28] These decisions are not published, and no information is provided regard fines imposed.

[29] CNDP (2020)

[30] Bowmans (2021)

[31] Convention 108 of the Council of Europe

[32] United States Council of Economic Advisers (2018)

[33] UNICRI (2015)

[34] Gordon, et al. (2015)

[35] ITU (2019)

[36] These countries are the Democratic Republic of Congo, The Gambia, Liberia, Madagascar, and Mali.

[37] ITU (2019)

[38] Human Rights Watch (2021)

[39] AU (2018)

[40] Council of Europe (2001)

[41] World Bank, Cybersecurity Capacity Review: Benin (2020)

[42] World Bank, Cybersecurity Capacity Review: Liberia (2020)

[43] Toka Cyber Builders (2020)

[44] WDR (2021)

[4545] World Bank Group (2021).

[46] World Bank (2018)

[47] World Wide Web (2016).

[48] Van Belle (2018).

[49] Bartley Johns, et al. (2018)

[50] (Casalini, López-González & Nemoto, 2021)

[51] (Casalini and López-González, 2019)

[52] Cory and Dascoli, 2021

[53] Klein (2015)

GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA

MAIN REPORTS

VOLUME 1 Digital for Governance: Reaching the Potential for the Digital Economy in Africa—Digital Tools for Better Governance

VOLUME 2 Governance of Digital: Regulating the Digital Economy in Africa—Managing Old and New Risks

TECHNICAL BACKGROUND PAPERS

- ICT Procurement in Africa
- Adoption of eGP in Africa
- Vulnerabilities of ICT Procurement to Fraud and Corruption
- Regulating Digital Data in Africa
- Taxes and Parafiscal Fees on Digital Infrastructure Services in Africa
- Corporate Governance and Transparency of State-Owned and State-Linked Digital Enterprises in Africa
- State-Owned Enterprises in Digital Infrastructure and Downstream Digital Markets in Africa
- Competition Advocacy for Digital Markets in Africa
- Competition Policy in Digital Markets in Africa

WORLD BANK GROUP

DIGITAL DEVELOPMENT PARTNERSHIP