THE DANISH INSTITUTE FOR HUMAN RIGHTS

BRIEFING NOTE – MARCH 2023

DEVELOPMENT FINANCE FOR DIGITALISATION: HUMAN RIGHTS RISKS IN SUB-SAHARAN AFRICA

BRIEFING NOTE – MARCH 2023

DEVELOPMENT FINANCE FOR DIGITALISATION: HUMAN RIGHTS RISKS IN SUB-SAHARAN AFRICA

Authors: Cathrine Bloch Veiberg and Mathilde Dicalou, as well as Ioana Tuta and Dr. Jonathan Andrew

e-ISBN: 978-87-7570-132-2

Cover photo: Sora Shimazaki, pexels.com
Layout: Michael Länger

This briefing note draws on background research conducted by Grace Mutung'u and Marlena Wisniak for an internal scoping paper on human rights implications in the digital transition in Ethiopia, Kenya and Tanzania. We would also like to thank our colleagues Signe Andreasen Lysgaard and Nora Götzmann for their review of the briefing note.

This publication is part of the Responsible Business Conduct in Sub-Saharan Africa Project, made possible thanks to the support from the Permanent Mission of Denmark to the United Nations in Geneva. Responsibility for the content rests entirely with the Danish Institute for Human Rights.

You can read more about the Responsible Business Conduct in Sub-Saharan Africa project here: https://www.humanrights.dk/projects/responsiblebusiness-conductsub-saharan-africa

Denmark's National Human Rights Institution
Wilders Plads 8K, DK-1403 Copenhagen K
Phone +45 3269 8888
www.humanrights.dk

CONTENTS

ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
AI	Artificial intelligence
DFI	Development finance institution
E&S	Environmental and social
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IFC	International Finance Corporation
OECD	Organisation for Economic Co-operation and Development
PbD	Privacy by design
UNGPs	United Nations Guiding Principles on Business and Human Rights

ABOUT THIS BRIEFING NOTE

This Briefing Note aims to support development finance institutions (DFIs) in integrating a human rights into their decision-making and stewardship efforts related to digital investments in Sub-Saharan Africa.

The note includes:

- A contextual presentation of the digital transition in Sub-Saharan Africa, including relevant human rights legal and policy frameworks and current trends in financing digitalisation for development.
- An overview of human rights opportunities and challenges relevant for DFIs investing in digital projects in the region.
- Perspectives and ways forward for DFIs informed by human rights frameworks applicable to financial actors.
- Practical resources that can be used to inform the development and implementation of relevant policies and procedures on human rights risks in development finance for the digital transition in Sub-Saharan Africa.

More specifically, this briefing note deals with digitalisation projects, meaning the conversion of products and services to the digital form. Its main audience is DFIs and other investors with digital investments in Sub-Saharan Africa, international and national policy-makers working in the space of development finance, as well as civil society organisations working at the intersection of digital rights, business and human rights and development.

This briefing note does not seek to have a comprehensive approach to the human rights implications of the digital transition in Sub-Saharan Africa. It is intended to serve as basis to stimulate discussion with DFIs and other relevant actors involved in such projects.

WHY SHOULD DFIS CONSIDER HUMAN RIGHTS WHEN INVESTING IN THE DIGITAL TRANSITION IN SUB-SAHARAN AFRICA?

DFIs investing in digitalisation projects have a critical role to play in underpinning that the African digital transition is one that is firmly based in human rights, especially in the in Sub-Saharan African context, where human rights related to digitalisation remain fragile.

In the context of digitalisation projects, compliance with environmental and social (E&S) standards is insufficient as these were conceptualised for projects with a physical footprint. Impacts/risks associated with digital technologies are different from impacts associated with traditional development projects with a heavy physical footprint (e.g. infrastructure, energy, agriculture). E&S standards are therefore not sufficient to address human rights impacts occurring in the digital sphere.

In general, DFIs, along with all other business entities, are expected to respect human rights as set out by the UN Guiding Principles on Business and Human Rights (UNGPs).

The UNGPs clarify the responsibilities of states and businesses to avoid and address adverse human rights impacts related to business activities. All actors, including DFIs, have a responsibility to respect internationally recognised human rights standards wherever they operate and irrespective of whether home or host states meet their own human rights obligations. The responsibility to respect human rights is to be implemented by businesses, including DFIs, through having a policy commitment on human rights and a process of human rights due diligence geared towards identifying, avoiding and addressing the adverse or negative human rights impacts associated with their activities, services and business relationships. Addressing negative impacts entails providing or contributing to the remediation of actual adverse human rights impacts where necessary.

1 DEVELOPMENT FINANCE FOR DIGITALISATION

QUESTIONS CONSIDERED IN THIS SECTION

- **What are the current trends in investments into the digital transition in Sub-Saharan Africa?**
- **What is the envisaged role of DFIs in the digital transition in Sub-Saharan Africa?**

Supporting the digital transition in the Global South has become an important priority in development cooperation and finance. Twelve out of the 30 member states of the OECD Development Assistance Committee, a forum convening the largest aid providers, have digitalisation strategies, while further six refer to digitalisation in their development cooperation priorities.[1] Between 2019 and 2021, the World Bank, a leading multilateral development bank, has increased its portfolio of digital projects from six to 29 (e.g., fintech, digital identification system, e-health).[2] In addition, most projects financed by DFIs, even if not dealing exclusively with digitalisation per se, will nevertheless carry risks or opportunities related to digitalisation. For example, investments to modernise healthcare services will focus on the renovation of hospital infrastructure and the facilitation of access to medical products, and these can include the use of digital products and carry implications related to data protection, privacy or even discrimination in access to these services.

Digitalisation: Digitalisation is the adaptation of a system, process, etc. to be operated with the use of digital technologies.

Reflecting broader trends in the financing of the 2030 Agenda for Sustainable Development, private finance is deemed a crucial component of the development finance mix contemplated for digitalisation efforts. For example, in 2021, the International Finance Corporation, the private sector arm of the World Bank Group, committed more than USD 1 billion in investments in the telecom sector, with a strong focus on Africa.[3] In 2020, the United States development agency launched Digital Invest, a blended finance programme to mobilise private finance for digital connectivity infrastructure and financial services.[4]

Digital transition in African economies and society has attracted considerable attention amongst international investors and businesses seeking new commercial opportunities in markets that offer substantial growth opportunities, and by DFIs (see section 2). This acceleration of development finance towards digitalisation, while touted in some corners as a developmental opportunity for economies to rapidly advance, has also resulted in calls for caution. Human rights advocates, for example, have raised concerns that deployment of technology may exacerbate underlying patterns of discrimination and exclusion,[5] and bolster authoritarian tendencies by enhancing states' surveillance

capabilities.[6] The widely noted observation that technology is a double-edged sword remains particularly apt and captures well the human rights dilemmas underlying the digital for development agenda.* On the one hand, such investments hold the potential of redressing a multi-dimensional digital divide that impairs people's access to information and essential services such as education and healthcare.[7] On the other hand, such projects can also enable mass surveillance of populations, interferences in the right to privacy and discriminatory public policies that reinforce rather than address drivers of inequality. For example, digital healthcare technologies can enable populations living in remote areas without access to physical healthcare services access such services, while running the risk of increased leaking of sensitive private information that may lead to discrimination, harassment or violence. Furthermore, the reliance on digitalised services to provide public services and address gaps in access, may also result in exclusion for digitally illiterate individuals and communities.

Against this backdrop, the OECD report "Development Co-operation Report 2021: Shaping a Just Digital Transformation" focusses on a just digital transition, highlighting the importance of 'upholding human rights and democratic values' and call for development actors to address negative outcomes through institutional strategies, safeguards and risk assessments.[8] However, there are only a few examples of development actors, including especially DFIs, taking measures to better understand, avoid and address the human rights risks related to investments in digital development projects.[9] It is therefore pressing that DFIs embed human rights considerations into the project and investment life cycle, including by making changes at the level of policies, risk management procedures, and internal capacity building. This briefing note explores how this can be done in section 4, but first section 2 describes the current state of play around digitalisation in Sub-Saharan Africa and section 3 highlights key associated human rights challenges.

* Digital for development refers to the design and implementation of digital tools for development outcomes.

2 DIGITAL TRANSITION IN SUB-SAHARAN AFRICA

QUESTIONS CONSIDERED IN THIS SECTION

- **What are the current trends in investments into the digital transition in Sub-Saharan Africa?**
- **What is the envisaged role of DFIs in the digital transition in Sub-Saharan Africa?**

Africa is the continent with the lowest levels of internet penetration globally.[10] As a region, it also has the least affordable data packages[11] for the populations served, and huge disparities in access to the internet persist between rural and urban areas.[12] The COVID-19 pandemic accelerated the digitalisation of economies and societies around the globe, including in Africa. By the end of 2020, 28% of the Sub-Saharan African population was connected to the internet, continuing a positive trend seen since 2014.[13] While mobile broadband coverage has also increased substantially in Sub-Saharan Africa, it remains the region with the largest coverage gap; one in five people live in an area without any mobile broadband coverage – this represents an estimated 210 million people.[14] Such discrepancies in coverage can lead to unequal access to essential services and information. More concerning, however, is the current usage gap, which continues to widen year after year: it now stands at 53%.[15] As such, across Sub-Saharan Africa, more than half of the population is still not using mobile internet despite living in an area where mobile broadband coverage is possible.[16]

The digital transition in Sub-Saharan Africa has attracted considerable attention from international investors, businesses and by DFIs. The World Bank Group Digital Economy for Africa initiative,[17] developed jointly with the African Union, sets out a framework for investment in digital infrastructure, digital public platforms, digital financial services, digital businesses, and digital skills to deliver on the continent wide Digital Transformation Strategy for Africa (2020-2030).[18] As of January 2022, the World Bank developed country diagnostics for the majority of countries in Sub-Saharan Africa.[19] These diagnostics provide an assessment of the state of the digital economy and identify key interventions to inform the World Bank's financing and technical assistance. However, the diagnostics do not take account of the legal or policy landscape pertaining to human rights addressed in the section below. This section provides an overview of the legal and policy landscape pertaining to human rights in the context of technology in Sub Saharan Arica. These are especially of interest to DFIs, in understanding the legal human rights landscape applicable to the digital transition in Sub-Saharan Africa.

2.1 LEGAL AND POLICY LANDSCAPE PERTAINING TO HUMAN RIGHTS IN THE CONTEXT OF TECHNOLOGY

All Sub-Saharan African countries, as Member States of the United Nations, are party to the Universal Declaration of Human Rights.[20] The overwhelming majority are also parties to the two main international human rights instruments: the International Covenant on Civil and Political Rights (ICCPR)[21] and the International Covenant on Economic, Social and Cultural Rights.[22]

The right to privacy is protected under Article 17 of ICCPR, which provides that 'no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.' Article 17 of the ICCPR is also to be interpreted as safeguarding privacy in the broader context of personal data collection and processing in respect of the functions public authorities may lawfully perform.[23] In that regard, international law provides that any gathering and holding of personal data on computers, data banks and other devices must be regulated by law and protected by effective implementation measures taken by the state. In 2019, the UN General Assembly adopted a resolution on 'The Right to Privacy in the Digital Age', underscoring the importance of the right to privacy in respect of the principle of non-discrimination (Article 26 of ICCPR). In other words, the right to privacy should be protected in a manner that guarantees that individuals and social groups are protected from discrimination – including by ensuring that the gathering, storing and use of personal data is not utilised to put them at risk of discriminatory treatment. This is especially critical in those contexts where the rights of vulnerable groups and minorities are not safeguarded by solid legal and policy frameworks grounded in human rights and the rule of law.

The ICCPR commits its parties to work toward the realisation and granting of economic, cultural and social rights, such as those pertaining to labour including fair and just conditions of work, but also the right to health, the right to education and the right to an adequate standard of living. Increasingly, access to health, education, work and other such services is being digitalised and, whilst digital connectivity and inclusion in the digital sphere are not considered a human right, Internet access is in many urban and rural communities swiftly becoming as essential to daily life as adequate food and water for survival.[24] Online services are the gateway through which many people access financial services, apply for and access government services such as welfare benefits, search for jobs or accommodation, and access education and health care services, rights protected under the ICCPR. Lack of access to the Internet can prevent people from accessing vital information and services and may lead to some being unable to meet their basic daily needs and guarantee the realisation of internationally recognised human rights.

In Sub-Saharan Africa, the **African Charter on Human and Peoples' Rights** is a critical instrument to guarantee the protection of fundamental rights. Among others, the Charter protects the right to freedom from discrimination (Article 2), the right to receive information and free expression (Article 9), the right to work (Article 15), the right to health (Article 16), the right to education (Article 17), the right to economic, social and cultural development (Article 22) – human rights that are relevant in the context of the

digital transition in the region, provided the breadth of services and aspects of life that digital technologies cover or aim to cover.

While the Charter does not expressly protect the right to privacy, certain provisions of the Charter do in part demonstrate an acknowledgement of specific attributes integral to the right to privacy. Article 4 provides that all human beings shall be entitled to respect for 'the integrity of his person'; Article 5 stating that the dignity of every individual shall be respected; and Article 6 protecting the right to liberty.[25] Furthermore, despite the evident gap vis-à-vis a specific reference to privacy as a fundamental right, it can also be argued[26] that the Charter affords wide dispensations for its interpretation through the mechanism of provisions retained within Article 60, which allows the African Commission on Human and Peoples' Rights to draw inspiration from international law pertaining to the right to privacy.[27] Moreover, subsequent agreements (in particular, such as the African Union Convention on Cybersecurity), treaties and protocols that have developed African human rights law since the Charter came into force also provide pathways to broadening the recognition of the right to privacy.

2.2 HUMAN RIGHTS PROTECTIONS

With the advancement of technological innovation and cross-border trade, compliance with international personal data protection legislation and standards has become imperative for the conduct of international trade, economic development and other issues such as the safeguard of human rights (including the rights to privacy, personal data protection and other interdependent human rights of individuals and groups engaging within the digital sphere). In Africa, negotiations on an African Continental Free Trade Area (AfCFTA) Digital Trade Protocol continue within the wider scope of the AfCFTA framework for establishing a single market on the African continent.[28] The protocol, which will be an integral part of the AfCFTA, will form a framework to conduct digital trade within Africa with the aim of facilitating inclusive development on the continent.[29]

As in other regions**, at present, there is no unified approach to personal data protection across Africa, with certain countries having comprehensive personal data protection legislation in place, whilst others still have no laws enacted or other provisions within their constitutions to provide protection. As of 2022, the following African territories had enacted comprehensive personal data protection legislation: Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Rwanda, Senegal, Seychelles, South Africa, Tunisia, Western Sahara, Zambia and Zimbabwe.[30] As such, it is observed that the extent of provisions to regulate the flow of both personal data and other classifications of electronic data across African jurisdictions remains relatively underdeveloped. Currently, 61% of African countries have legislation in place that regulates electronic transactions, whilst just over half (52%) have laws on digital consumer protection. Legislation relating to privacy and data protection exists in jurisdictions covering 61% of the different jurisdictions across Africa, whilst 72% have enacted legislation on cybercrime.[31]

** With exception of the General Data Protection Regulation in the EU.

With the increase in digitalisation driven by the pandemic, a wider implementation of such laws across the continent has never been more pressing. Most recently, countries including Kenya, Ghana, Madagascar, Mauritius, Nigeria, Rwanda, South Africa, Togo, Uganda and Zimbabwe have been enacting new measures and developing regulatory oversight mechanisms through their legislatures to protect and secure personal data within their jurisdictions.[32] While these are generally considered welcome developments, there have been concerns over the capacity of state institutions to effectively implement these in a way that would adequately protect rights-holders' privacy and personal data online, as well as the parallel adoption of new laws that facilitate surveillance, collection of data and limit the use of encryption.[33] In addition, many countries still lack specific data protection laws.[34]

The existence of international, regional and national frameworks aiming at protecting human rights in relation to the digital transition does not necessarily ensure the effective protection of such rights. Gaps in implementation persist, particularly affecting vulnerable and marginalised groups.[35] In this context, legal compliance does not suffice; particular diligence with regard to those human rights challenges in the Sub-Saharan African context must be given. More specifically, DFIs should especially be attentive to the role they can play in either furthering those gaps or leveraging knowledge of these concrete issues to avoid violations of human rights.

3 HUMAN RIGHTS CHALLENGES RELATED TO THE DIGITAL TRANSITION

QUESTIONS CONSIDERED IN THIS SECTION:

- **What are some concrete human rights challenges related to digitalisation projects that investors should consider before and when investing in the digital transition in the region?**
- **What are some concrete examples of digitalisation projects having failed to assess human rights risks? What have been the consequences in the region?**

As much of human activity continues to shift online, in many instances affording significant scope for greater enjoyment of many human rights, the capacity of different actors to infringe those same rights has also augmented. Digital innovation is reshaping relationships between government, businesses and civil society, as well as the interdependencies between stakeholder obligations, responsibilities and duties. As explained in previous sections, the growth in investment in the digital transition has been accompanied by warnings about the impacts that such projects may have, including concerns related to the exacerbation of existing inequalities based on exclusion and discrimination, as well as the weaponization of digitalised services by states, such as through increased surveillance.[36] The low levels of digitalisation in Sub-Saharan Africa provide a strong rationale for DFIs to pursue investment opportunities, and there exist many entry points for enhancing access to services for all in compliance with international, regional and local human rights instruments and standards through digital technologies. However, the human rights risks associated with these investments may prove acute, and these concerns should thus inform a DFI's decision making and actions, especially since human rights violations cannot be offset by other social initiatives. For example, the expansion of digital infrastructure to support greater connectivity continues to exclude large parts of the population, particularly those living in rural areas.[37] In certain cases, conditions, such as the lack of official documentation, lack of connectivity to the grid and mobile networks, prevent adequate data collection necessary for building well-functioning digital ID systems.[38]

To illustrate the human rights challenges of the digital transition, the sections below provide two examples of digitalisation of services in Sub-Saharan Africa that represent the opportunities and critical risks for human rights associated with these.

3.1 DIGITAL ID: THE RISKS OF DEVELOPING DIGITAL IDENTIFICATION SYSTEMS

Across Sub-Saharan Africa, states have been developing digital identification systems, or 'digital ID', as key components of digital economic policies.[39] Digital ID covers 'identity (personal attributes), identification (processes and systems used in the identification of persons) and identity documents which are increasingly in the form of smart cards, chips

and mobile telephone applications (apps).'[40] Among other things, digital ID allows users to access banking, education, health, government and other essential services. States like Kenya, Nigeria and Ethiopia have already developed such technologies, the development and/or operationalisation of which has been financially supported by DFIs. For example, the World Bank's Ethiopia Digital Foundations Project provides an investment of USD 4.7 million for the development of 'a vibrant, inclusive and safe digital economy', which includes the operationalisation of the digital ID system developed by the government.[41] In Nigeria, the World Bank committed USD 430 million to develop a digital ID technology with the objective of 'increas[ing] the number of persons with a national ID number, issued by a robust and inclusive foundational ID system, that facilitates their access to services.'[42] While these are promoted as inclusive, enabling 'civic and social empowerment'[43] and a way to make economic gains, if poorly designed and without using a human rights-based approach to map out risks, their development and implementation runs the risk of causing adverse human rights impacts.

Risks related to large-scale data mining and the integration of decisions made by AI, including how they are integrated into surveillance or activities of law enforcement, such as predictive policies, must be considered by DFIs and other actors investing into these technologies. In the countries mentioned that currently have adopted digital ID, data protection frameworks remain lacking and may therefore have grave impacts on privacy and personal data protection.

EXAMPLE: HIGH COURT JUDGMENT IMPOSING CONDITIONS ON THE KENYAN DIGITAL ID PROGRAMME

In Kenya, the **Huduma Namba** had the aim of merging legal ID with digital ID by requiring the user to integrate all government-issued ID with mobile phone numbers and, at times, bank accounts. The project was immediately decried by human rights watchdog organisations. In 2019, the Kenya Human Rights Commission, the Kenya National Commission on Human Rights and the Nubian Human Rights Forum filed a petition before the High Court challenging the legality of the National Integrated Identity Management System and the way data would be collected to implement the **Huduma Namba**.[44] The High Court's 2020 judgment shows that the government began collecting personal data without taking adequate steps to ensure that the data would be appropriately protected, contrary to the Kenyan Data Protection Act No 24 of 2019. On the critical aspect of balancing public interest, which may justify the requirement to use digital ID technologies by the state,[45] with fundamental human rights, the Court ruled that, while the benefits of the National Integrated Identity Management System could be acknowledged in theory, these would need a solid human rights-based data protection legal framework, which is currently not the case in Kenyan law.[46] The safeguards guaranteed by the 2019 Data Protection Act No 24 and the mandate of the Data Commissioner were found insufficient in the context of the implementation of the Kenyan digital ID system and as posing 'a risk to the security of data that will be collected in the system',[47] a risk that is even higher for data relating to children.[48] This is especially important because a re-evaluation of the proportionality of data collection and processing activities taking place, for example, will take time, as many of the impacts of this monitoring may be imperceptible to the layperson in the short to mid-term. Accordingly, the judgment orders the government to first complete a data protection impact assessment before implementing the **Huduma Namba** programme.[49]

In implementing digital ID technologies, there exist additional risks regarding the potential exclusion of vulnerable and marginalised groups, in particular by putting these individuals at a risk of statelessness, should the digital ID system be made mandatory to access government services. Examples from other contexts can serve as lessons learned for future digital ID projects in the region. Famously, India's **Aadhaar** was widely criticised for having disenfranchised almost two million people and putting them at risk of statelessness for being excluded from the National Register of Citizens and the digital ID system.[50] In particular, individuals who already face difficulties with providing proof of identity, added to remoteness from the grid and without internet access, could be made particularly vulnerable to further exclusion. These include women, especially in rural areas, including because the process to obtain identification documents can be too difficult or because, among other reasons, they do not see a need for it, as men tend to handle the more formal transactional exchanges that require such documentation.[51] This is exacerbated in areas with poor internet coverage, which is highly prevalent in Sub Saharan Africa.[52]

Further, in addition to inadequate privacy and data protection frameworks, many Sub-Saharan African States have been known to use internet and social media, including by shutting down access, to repress civil society movements, protests and criticisms addressed to the government. For example, in Ethiopia where the digital ID project is currently being planned for full nation roll-out[53], the government was found in 2017 to have used a spyware against Oromo dissenters during protests that resulted in the killing of over 1000 individuals by security forces and the enactment of a ten-month state of emergency called in October 2016.[54] Similarly, civil society organisations raised concerns over the Proclamation to Prevent the Spread of Hate Speech and False Information, which took effect in March 2020, as the text uses broad definitions of hate speech and false information that could be subject to abuse and misinterpretation, as well as arbitrary interpretation by judges, in addition to providing disproportionate penalties that are not compliant with international human rights standards.[55] In this context, it is fundamental that thorough digital rights and privacy impact assessments are conducted before adopting and implementing digital ID technologies and systems. There is a particular role for investors in ensuring that they conduct due diligence when developing systems in countries where the rule of law is weak and where there exists a history of repressive use of online data. This is echoed by a coalition of civil society organisations, researchers and activists' calls to action for the World Bank and donors to centre human rights in the digital ID discussion, including by conducting rights-based impact assessments and baseline studies, ceasing activities that may heighten the risk of human rights abuses, enforcing transparency and creating opportunities for high-level engagement with civil society and experts.[56] For example, the World Bank decided to delay funds for a digital ID programme in Nigeria until the country enacts a legal framework for data protection.[57] While this is a welcome decision, civil society organisations have remarked that the World Bank, and other DFIs and investors, should ensure both that the legal framework in place and that its implementation effectively protect the rights of the most vulnerable.

TABLE 1: SUMMARY OF POTENTIAL BENEFITS AND RISKS ASSOCIATED WITH DIGITAL ID PROJECTS

POTENTIAL BENEFITS	POTENTIAL RISKS
• Economic growth • Reduction of costs of bureaucracy • Enhanced and facilitated access to health, education and other essential services • Reduction of fraud, corruption and security risks related to the use of physical documents • Protection of user privacy • Control over personal data • Improvement of risk management	• Use of private data if access is inadequately protected, including through discrimination • Misuse of private data to target specific individuals or groups, such as human rights defenders, watchdog organisations, or minorities • Risk of further digital exclusion for marginalised and already vulnerable groups without formal identity documentation or without digital literacy, including up to the risk of statelessness • Risks of leaks of sensitive data if inadequate digital infrastructure to protect such data

3.2 DIGITALISING HEALTHCARE: RISKS RELATED TO HANDLING HIGHLY SENSITIVE DATA IN THE 'DIGITAL WELFARE STATE'

The COVID-19 pandemic has been marked with the emergence of digital healthcare services, both in tracking the spread of viruses but also in the digitalisation of medical care. Sub-Saharan Africa was no exception. Examples include Ghana's COVID-19 tracker app, or the African Union's Trusted Travel, a digital vaccination platform that is mandatory to use to travel to certain African countries.

Investment into digital healthcare is going beyond the simple registering of patient data and is looking into applying AI to support drug design, interpret radiology scans, diagnoses of symptoms and logistics.[58] Countries in Sub-Saharan Africa have seen a dramatic increase in investment in eHealth services and digitalisation of medical data in the last year.[59] Other initiatives demonstrate an acute interest in investing into digital healthcare solutions. For example, the IFC's TechEmerge Health East Africa Challenge seeks to match health tech innovators with leading healthcare providers in East Africa to conduct pilot projects and build commercial partnership; in 2021, it gave access to a grant fund pool of USD 1 million, in addition to technical and advisory support from IFC, to the winners of the challenge.[60] Saturation of the fintech market in some sub-regions like East Africa is leading investors to invest in other areas, such as health.[61] On the other hand, many Sub-Saharan African governments are actively seeking investment into this type of products, presenting healthcare as an investment opportunity for corporate investors as well as DFIs.[62] Echoing the points made in the example above, the growth in investment in the digital transition in Sub-Saharan Africa has not necessarily been accompanied by the adoption and effective implementation of appropriate privacy and other digital rights

protection frameworks, giving rise to major concerns in countries that are also known for discriminating against minority groups and repressing dissident voices.

EXAMPLE: THE HYGEIA NIGERIA E-HEALTH PROJECT

In Nigeria for example, there have been significant investments into digital health services by DFIs and the government.[63] However, environmental and social assessments do not reflect risks related to privacy and data protection, mostly because environmental and social standard frameworks typically do not involve consideration of risks in this area. For example the IFC's 2014 assessment of the Hygeia Nigeria project, which involved an investment of USD 12.4 million in equity and involved the implementation of an IT platform upgrade for Hygeia, Nigeria's largest private integrated healthcare services group, did not address data privacy risks and concerns, but rather focused on more tangible environmental, health and social risks associated with hospital sites and associated facilities.[64] With the example of Nigeria, it is particularly concerning provided a history of data privacy breaches and health surveillance with 'little to no regard for the rights to personal privacy'.[65] For example, the digitisation of health-related data raised concerns during the COVID-19 pandemic as, while it was gathered by hospitals, the information was uploaded onto a third-party database with no information regarding how long it will be stored.[66]

Health-related data is especially sensitive and the risk of leaks could expose specific groups, for example sex workers or persons living with HIV&AIDS, to discrimination and violence.[67] As with digital ID projects, digital healthcare services in addition put already marginalised groups at further risks of digital exclusion. Failure to receive adequate health support due to a lack of access to the internet or digital literacy can lead to infringements on economic and social rights.

TABLE 2: SUMMARY OF POTENTIAL BENEFITS AND CHALLENGES ASSOCIATED WITH DIGITALISED HEALTHCARE SYSTEMS

POTENTIAL BENEFITS	POTENTIAL RISKS
• Facilitated access to health services, including by providing more direct contact with medical professionals • Facilitation of purchase, transport and delivery of medical supplies, leading to enhanced healthcare services • Reduction of costs and waiting time for medical treatment	• Risks related to highly sensitive health data leaks, which may lead to discrimination, harassment, and violence against patients • Exclusion of marginalised groups and individuals located away from the grid or without access to the internet from access to healthcare services

4 PERSPECTIVES AND WAYS FORWARD FOR DEVELOPMENT FINANCE INSTITUTIONS

QUESTIONS CONSIDERED IN THIS SECTION:

- **What are opportunities for DFIs and other actors investing into digitalisation projects in Sub-Saharan Africa to ensure that these investments comply with human rights instruments?**
- **How can DFIs and other stakeholders strengthen the consideration of human rights throughout the project lifecycle, at both policy and strategy level and during the E&S risk management procedures?**
- **Where can DFIs learn more about integrating human rights in digitalisation projects?**

Based on the sections above highlighting common human rights challenges related to digitalisation projects, especially in the Sub-Saharan African context, where human rights protections related to digitalisation remain fragile, DFIs investing in such projects have a critical role to play in underpinning that the African digital transition is one that is firmly based in human rights.

Most DFIs strive to identify human rights risks as part of their implementation of environmental and social safeguards (E&S safeguards) policies and processes. With slight variations across institutions, the E&S safeguard practice consists of a sustainability policy that outlines the DFIs' own responsibility to ensure that investments do not result in harm to people and the environment, and a set of E&S standards outlining corresponding binding expectations on clients.[68]

To avoid and address environmental and social risks, most DFIs expect their clients to comply with E&S standards to ensure their activities do not harm people and the planet. However, these standards have historically been developed to address the impacts of investment projects with a heavy physical footprint, such as large infrastructure or construction projects, and have various blind spots when it comes to the identification of human rights risks associated with digital technologies.[69] While there is an increased awareness in the development and DFI community around the need to step up efforts to identify and mitigate these risks,[70] there is little evidence that this commitment has translated into significant operational changes.

Impacts/risks associated with digital technologies are different from impacts associated with traditional development projects with a heavy physical footprint (e.g. infrastructure, energy, agriculture).

First, whereas the digitalisation project represents a relatively 'small' intervention, the **scope of the impacts** is potentially geographically far reaching with thousands

or millions of individuals facing human rights risks. Moreover, especially in respect to privacy issues, many impacted individuals may simply not know that their rights have been or could be impacted. That complicates processes of stakeholder engagement and grievance handling and requires DFIs to pay attention to users and consumers, a rights-holder group that is generally under-emphasised if not entirely missing in E&S safeguards standards and hence overlooked in impact assessments and action plans. Moreover, it requires a shift away from a project-centric 'inside the fence' lens to a wider approach to impact and risk assessment.

Second, the **link between the digital product/service and the human rights** might not always be obvious because of the highly specialised process of technology development, the rapid pace of innovation, and the lack of transparency, notably in respect to automated decision-making and AI. This requires additional capacity for E&S staff to be able to adequately engage with technology companies as well as different technological goods and services in order to obtain meaningful information and data on human rights risks.

Finally, some impacts and risks cannot simply be managed through the implementation of safeguards in relation to a particular investment as they require a **broader consideration** of whether certain interventions are appropriate in a specific context given existing legal frameworks and societal challenges (e.g., digital ID, e-health, etc.).

4.1 SUGGESTED WAYS FORWARD

This section identifies suggested ways forward for DFIs to strengthen the consideration of human rights risks related to investments in digital projects with the aim of ensuring they are adequately identified, addressed and factored in institutional strategies, investment decisions and implementation. It includes recommendations for action at the level of (i) policy and strategy, and (ii) the environmental and social risk management procedures associated with the investment lifecycle. To inform an enhanced approach to managing risks in this area it is recommended that DFIs conduct an internal review to serve as a 'health check' of the state of play.

4.1.1 Internal review

Review internal policies, procedures, capacities and resources and evaluate how and whether human rights risks related to digital projects have been adequately captured therein.

TIP

This review should be carried out by an independent team, e.g. an internal evaluation office or external review group, and should include external stakeholder input. The review can focus on:

- Whether and why digital projects previously financed by the DFI have resulted in adverse human rights risks/impacts including the degree to which such risks

were adequately captured during investment screening, decision-making and in contractual conditionalities in environmental and social action plans.
- The extent to which the environmental and social safeguards used serve as an adequate benchmark when seeking to identify and mitigate human rights impacts that are salient in the development and use of different types of technology solutions and internet infrastructure.
- An assessment of whether investment officers, environmental and social (E&S) specialists and the accountability mechanism staff have sufficient knowledge of and/or have been capacitated on the topic of human rights risks likely to materialise in digital projects.
- An assessment of the levels of human rights awareness and risk management capacities of DFI clients implementing digital projects.

4.1.2 Policy and Strategy

Based on this review, commit to an action plan to close potential gaps in the short and medium term. Below are examples of measures that could be considered for inclusion in such an action plan:

- **New safeguards.** The development of a new performance standard for projects with digital components that would establish explicit expectations for clients on how to identify, prevent, mitigate and remediate human rights risks including in respect to data protection and privacy, non-discrimination and access to information.
- **Capacity building.** The roll out of an internal capacity building programme on human rights and digital technologies, including the development of bespoke resources and guidance (that can also be shared with clients).
- **Resources.** The hiring or contracting of additional environmental and social staff and/or consultants with digital knowledge and expertise to support the appraisal and monitoring of digital projects.
- **Tools.** Updating of internal procedures, tools and templates to ensure they adequately cover human rights risks related to digitalisation.
- **Peer collaboration.** Informed by the findings of the review, sharing good practice and lessons learned with other DFIs and development cooperation actors and identification of areas of joint action to address risks at the systemic level (e.g., broader issues related to discrimination, exclusion, or risks related to state surveillance).
- **Regular communication.** Ensuring disclosure of project-specific documentation as well as in annual reports, on the type of human rights risks identified in digital projects as well as the approach taken to prevention and mitigation.

In respect to digitalisation of investment strategies, factor in emerging evidence on the adverse human rights impacts of the development and use of digital technologies and critically revisit theories of change and assumptions about the expected development impact or positive contribution of such investments. DFIs should discuss the unintended consequences of such investments and not inadvertently tolerate trade-offs between respect for human rights and reaching certain other economic or development indicators.

Develop guidance, possibly in collaboration with peer-DFIs and other stakeholders,

on how impacts such as privacy breaches can be remediated by clients and DFIs.

4.1.3 Integrate Human Rights Considerations Across the Project Life Cycle

These recommendations are organised by the key decision-making milestones in the DFIs' process to assess, address and remediate adverse impacts associated with their investments. The OHCHR has published a comprehensive analysis of the extent to which the procedural and substantive dimensions of the DFIs' safeguards-based risk management across an investment's lifecycle align with the expectations of UNGPs-based human rights due diligence.[71] That analysis and related recommendations should provide the backdrop for any DFI effort to strengthen human rights approaches and methodologies in general. The recommendations below zoom in on certain aspects that require heightened attention in the context of investments in projects with digital components.

Pre-appraisal and appraisal (before DFI decision to invest)
Revise risk categorisation processes to ensure that digital projects are not inadvertently categorised as low risk as result of some their impacts, such as data protection and privacy, not being explicitly covered by the DFI safeguards. A low-risk categorisation translates into fewer resources allocated to the DFI's appraisal and monitoring efforts, including less stringent requirements for clients.

EXAMPLE – FINTECH AND HUMAN RIGHTS

An investment in a fintech solution is likely to receive a low-risk categorisation because of its limited physical footprint and low likelihood of generating adverse impacts in the social areas where DFIs have dedicated safeguards such as land, Indigenous People, community health and safety, and labour rights. However, fintech solutions have been shown to pose risks to privacy and data protection, increase indebtedness of poor individuals and result in discriminatory practices, for example where algorithmic bias or deficient data collection practices negatively impact individuals' credit scoring and access to financial products and services, such as insurance, loans or mortgages.

Conduct contextual risk analysis by drawing on country-level and sector-level human rights data that is relevant and meaningful for the assessment of digital projects. This may also include local experts or stakeholders knowledgeable on digitalisation in the given context. Such contextual information can help DFIs understand the broader human rights and digitalisation context in which their investment is implemented and to engage critically with the environmental and social documentation submitted by clients who might take a narrow project-centric focus and have an interest in downplaying the severity of certain risks.

LEARN MORE

Data sources that could be used to inform contextual risk analyses include:

- Freedom House, Freedom on Internet Index which measures the seriousness of human rights violations in the digital sphere across three categories i.e. obstacles to access, limits on content and violations of user rights.
- Universal Human Rights Index, a database with recommendations to states by different UN human rights bodies. It allows filtering results by themes such as 'privacy', 'freedom of opinion and expression and access to information' or 'equality and non-discrimination'.
- ICT Policy Centre for Eastern and Southern Africa, a regional civil society organisation. Its annual reports include information on legal and policy gaps and human rights violations related to the State and business use of digital technologies.
- Disinformation tracker, an interactive platform that gives an overview of laws and government actions against disinformation with adverse impacts on freedom of expression across Sub-Saharan Africa.
- Data Protection Africa, an open access portal with information on data protection laws in Africa.
- Access Now, Internet shutdowns tracker, a resource on internet shutdown trends globally.

Such contextual-level data can be incorporated in the DFI decision-making process in different ways as illustrated below:

- **Data leads to a decision not to pursue the investment because of an unacceptably high risk** e.g., the financing of a digital ID project requiring the collection of large amounts of sensitive data in a country with weak or non-existent data protection law.
- **Data informs increased engagement with a client in relation to safeguarding human rights,** e.g., the financing of a private telecom provider in a country where the government has faced allegations of unlawful surveillance of opposition leaders.
- **Data is used to develop criteria for technical assistance,** e.g., technical assistance on managing human rights risks is provided to digital clients in countries with a very low score on the Internet Freedom Index.

When identifying and assessing risks and impacts related to digital projects, use international human rights standards as benchmarks and ensure that the analysis extends beyond data protection and privacy issues to capture the full gamut of adverse human rights impacts.

TIP – MITIGATING ACTIONS

Assessments of digital rights projects can reveal human rights risk areas that E&S practitioners might have little experience dealing with and require the development of new types of prevention and mitigation measures. For example, a private sector client developing AI solutions might in its environmental and social action plan be required to:

- develop and implement a data protection policy
- implement a data retention policy and enable routine and secure erasure of personal data that is no longer required for the functioning of the product or service in question
- commit to a process of assessing bias in personal data that is collected and processed
- adopt a plan to assess risks in developing an automated decision-making capabilities
- follow 'privacy by design' (PbD) principles in the development of a technology, and to monitor effectiveness throughout the lifecycle of the technology's deployment
- develop capacity building and awareness raising materials for those intended to utilise the product highlighting human rights risks related to its planned and potential uses and the possible misuses of the technology.

USEFUL RESOURCES FOR IDENTIFYING AND ADDRESSING HUMAN RIGHTS ADVERSE IMPACTS AT ENTITY AND PRODUCT LEVELS

- Screening of prospective portfolio companies and their track record related to human rights and digitalisation (entity level) can be informed by OHCHR B-Tech - Rights-Respecting Investment in Technology Companies (section 2) as well as Ranking Digital Rights.
- DFIs can also use their leverage to push their portfolio companies in performing human rights due diligence for the design, development and use of technology products and services (product-level) and monitor the effective thereof by referring to the OHCHR report: The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies. DFIs can also monitor the human rights due diligence in product-level using the guidance on human rights impact assessment of digital activities issued by DIHR and the Digital Rights Check.

Ensure that the approach to engagement of rights-holders as part of the identification and assessment of impacts is tailored to the specificities of digital projects, i.e., their potential to adversely impact a large number of people in their role as users and consumers and the varying degree of understanding of the functioning of the digital projects by potentially affected groups. A precondition to this is ensuring that impact assessments as well as Terms of References for consultants conducting such assessments adequately include human rights risks associated with digitalisation as well as an emphasis on stakeholder engagement.

Ensure, including through contractual provisions, that clients implementing digital projects publicly communicate on human rights impacts, even when these impacts might not be explicitly covered by the DFI safeguards. For projects with large scale impact, the communication should be of such a breadth and frequency that it reaches affected rights-holders, including especially the most vulnerable segments of the population, with the objective of enabling them to evaluate the adequacy of the measures taken by the DFI to address identified human rights impacts.

LEARN MORE – STAKEHOLDER ENGAGEMENT

The context of digital projects complicates traditional forms of rights-holder engagement in DFI investments where the affected individuals – for the most part, workers and/or communities – work and live in the vicinity of a project, can be easily identified, and where the causal link between the project activities and adverse impacts can be relatively straightforward to establish. The use and deployment of digital technologies can negatively affect a significantly larger number of individuals, who are frequently located geographically diverse areas, belong to different communities and social groups, and may be removed from the entity(ies) that might be causing harm.

To address these practical challenges new methodologies for rights-holder engagement might be necessary. This can be done through requiring the undertaking of environmental and social impact assessments, which emphasise the centrality of meaningful stakeholder engagement. The application of the human rights-based approach to such impact assessments allows for the effective analysis and the addressing of identified potential and actual human rights impacts of concerned groups and individuals.[72]

Given their role of setting expectations for clients, DFIs should take the lead in proposing and road testing such methodologies that should, amongst other, provide guidance on:

- The identification of legitimate, credible proxy organisations that can legitimately represent the interests of affected users/consumers
- The implementation of large-scale information and awareness raising campaigns, especially for projects that involve the digitalisation of administration
- How to protect human rights defenders against the risk of digitally mediated retaliation and harassment.

Relevant resource include:

- Engaging Tech Companies on Human Rights: A How-To Guide For Civil Society
- Stakeholder Engagement Section, Human Rights Impact Assessment Guidance for Digital Business Activities

4.1.4 Monitoring (after contract signature)

Ensure that the monitoring methodology includes indicators and questions that can adequately track the materialisation of human rights risks related to digital projects as well as the client's ability to effectively avoid and address such risks. Levers include integrating the human rights and digitalisation lens into requests for quarterly and annual sustainability reporting for relevant clients as well as using board seats in equity investments to ask for status updates in relation to management of human rights related risks. DFIs may also adjust their approach to 'incident reporting' by clients to include incidents related to impacts on privacy etc.

Ensure that accountability mechanisms staff are adequately capacitated to investigate and provide mediation services in the case of complaints related to digital projects and human rights. Accountability mechanisms should be designed in such a way that they are effectively accessible by any potentially affected rights-holder.

EXAMPLE – IDENTIFYING RELEVANT INDICATORS

For investments in telecom companies, DFIs could put in place measures to monitor for example:

- whether the client received government requests (number and type) for transfer of personal data, the process the client followed to assess the legality of such requests and to communicate in a transparent manner to the public concerns on such risks.

For investments in a software development company, DFIs could monitor for example:

- whether there have been any personal data leaks or breaches and how they were managed
- whether personal data has been gathered in accordance with applicable data protection and privacy laws.

5 CONCLUSION

The ongoing digital transition in Sub-Saharan Africa represents vast opportunities for sustainable investments to further inclusion and increase access to services for all. Achieving this transition will require extensive investments, including from DFIs and other investors operating in the region, and it is expected that the design and implementation of digitalisation projects will accelerate in the coming years, in line with abovementioned international, regional and national development targets. However, Sub-Saharan Africa remains a fragile context with regard to the effective protection of human rights in the fast-evolving digital world. As in other world regions, the adoption of national laws and regulations is not keeping the pace with digitalisation and, even in those contexts where there are relevant legal frameworks in place, these can prove inadequate or poorly implemented. In this context, it is expected that DFIs and investors take concrete steps to assess all potential and actual human rights impacts related to their support to develop digital technologies to ensure that their development objectives are met without sacrificing other human rights, especially those of the most vulnerable. These steps should be implemented both at strategic and policy level, as well as throughout the project lifecycle, using a human rights-based approach.

ENDNOTES

1 See OECD, Development Co-operation Report 2021: Shaping a Just Digital Transformation (Paris: OECD, 2021), Chapter 33.

2 The World Bank, Digitalisation and Development (Washington DC: World Bank, 2022) 12. Note that the Bank invests in many other projects with digital components/aspects. This statistic only refers to projects that have as primary objective digital transformation.

3 Ibid.

4 See 'Digital Invest', USAID, https://www.usaid.gov/digital-development/digital-invest (accessed 23 November 2022).

5 Center for Human Rights & Global Justice, Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID Rights and Digital ID (New York, NY: NYU, 2022).

6 Privacy International, The Keys to Data Protection: The Keys to Data Protection (London: Privacy International, 2018).
See also: Audrey N Selian, 'ICTs Support of Human Rights, Democracy and Good Governance', International Communications Union (2002); Eliot Nsega, 'The Use of Information and Communications Technology in Human Rights Promotion: A Case Study of the African Commission on Human and Peoples' Rights', Diplo (2021), https://www.diplomacy.edu/wp-content/uploads/2021/06/IGCBP2010_2011_Nsega.pdf; Yingqin Zheng et al, 'Conceptualizing Development in Information and Communication Technology for Development (ICT4D)' (2017) 24:1 Information Technology for Development 1; Raéf Bahrini and Alaa A Qaffas, 'Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries' (2019) 7:1 Economies 21.

7 See, e.g., Justine Humphry, 'Bearing the Burden: Digitisation of Government, Health and Welfare', in Homelessness and Mobile Communication (London: Palgrave Macmillan, 2022) 93.

8 OECD, note 1, Chapter 3.

9 See for example 'Digital Rights Check', GIZ, https://digitalrights-check.toolkit-digitalisierung.de/development-finance/; World Bank , Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (Washington, DC: World Bank, 2017); Gordon Myers and Kiril Nejkov, 'Developing Artificial Intelligence Sustainably: Toward a Practical Code of Conduct for Disruptive Technologies', IFC (March 2020), https://www.ifc.org/wps/wcm/connect/e0e928ba-e4a3-4e5d-af0f-4c4477ff22f0/EMCompass_Note_80-10.pdf?MOD=AJPERES&CVID=naqN4Mr.

10 As of March 2021, the internet penetration on the African continent was 43.2%, the lowest rate in the world. See 'Internet Usage Statistics: The Internet Big Picture', Internet World Stats, https://www.internetworldstats.com/stats.htm.

11 Only 17% of Africa's population can afford one gigabyte of data, compared to 37% in Latin America and the Caribbean and 47% in Asia. See OECD and African Union, Africa's Development Dynamics, Digital Transformation for Quality Jobs (Addis Ababa: AUC/Paris: OECD, 2021) 27.

12 Paul Kimumwe, 'Towards an Accessible and Affordable Internet in Africa: Key Challenges Ahead', Cipesa (30 December 2021), https://cipesa.org/2021/12/towards-an-accessible-and-affordable-internet-in-africa-key-challenges-ahead/; 'Individuals Using the Internet (% of population) - Sub-Saharan Africa', The World Bank, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG.

13 Jason Mitchell, 'African e-Connectivity Index 2021: The Final Frontier and a Huge Opportunity', Investment Monitor (10 November 2021), https://www.investmentmonitor.ai/tech/africa-connectivity-index-2021.

14 Anne Delaporte, 'The State of Mobile Internet Connectivity in Sub-Saharan Africa: Why Addressing the Barriers to Mobile Internet Use Matters Now More Than Ever', GSMA (27 October 2021), https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/.

15 Jane Munga, 'To Close Africa's Digital Divide, Policy Must Address the Usage Gap', Carnegie Endowment for International Peace (26 April 2022), https://carnegieendowment.org/2022/04/26/to-close-africa-s-digital-divide-policy-must-address-usage-gap-pub-86959.

16 Delaporte, note 14.

17 'The Digital Economy for Africa Initiative', The World Bank, https://www.worldbank.org/en/programs/all-africa-digital-transformation.

18 'The Digital Transformation Strategy for Africa (2020-2030)', African Union, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

19 'The Digital Economy for Africa Initiative: Country Diagnostics', The World Bank, https://www.worldbank.org/en/programs/all-africa-digital-transformation/country-diagnostics

20 Universal Declaration of Human Rights, UNGA 217 A (III) (adopted 10 December 1948).

21 'Ratification Status for CCPR – International Covenant on Civil and Political Rights', OHCHR, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en.

22 'Ratification Status for CESCR - International Covenant on Economic, Social and Cultural Rights', OHCHR, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/treaty.aspx?treaty=cescr&lang=en.

23 Human Rights Committee, 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', HRI/GEN/1/Rev.9 (8 April 1988), 2, para. 7.

24 See further: Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/RES/47/16 (26 July 2021).

25 African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (adopted 27 June 1981, entered into force 21 October 1986), Articles 4 ,5 & 6. Note: emphasis added.

26 For a more in-depth discussion see: Yohannes Eneyew Ayalew, 'Untrodden Paths Towards the Right to Privacy in the Digital Era Under African Human Rights Law' (2022) 12 International Data Privacy Law 1.

27 African Charter on Human and Peoples' Rights, note 25, Article 60.

28 Alexander Beyleveld and Franziska Sucker, Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade (Johannesburg: Mandela Institute, 2022).

29 John Stuart, 'Digital Trade in Trade Agreements: Lessons for the AfCFTA', Tralac blog (31 August 2022), https://www.tralac.org/blog/article/15739-digital-trade-in-trade-agreements-lessons-for-the-afcfta.html.
30 'UNCTAD Global Cyberlaw Tracker: Summary of Adoption of E-Commerce Legislation Worldwide', UNCTAD (2021), https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.
31 Ibid; see also: Deloitte, Privacy Is Paramount: Personal Data Protection in Africa (Johannesburg: Deloitte, 2021).
32 'Data Security and Privacy Laws Develop Across Africa', Baker McKenzie (28 April 2022), https://www.bakermckenzie.com/en/newsroom/2022/04/data-security-and-privacy-laws-across-africa.
33 Juliet Nanfuka, 'Data Privacy Still a Neglected Digital Right in Africa', CIPESA (27 January 2022), https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/.
34 'Map', Data Protection Africa, https://dataprotection.africa/.
35 See e.g., African Declaration on Internet Rights and Freedoms Coalition, 'Privacy and Personal Data Protection in Africa: A Rights-Based Survey of Legislation in Eight Countries', APC (May 2021), https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica_CountryReports.pdf.
36 Privacy International, note 6; Nsega, note 6; Zheng et al, note 6; Bahrini and Qaffas, note 6.
37 See e.g., World Bank, note 12; Chrispin Mwakideu, 'Can African Reach Universal Internet Access?, DW (11 May 2021), https://www.dw.com/en/can-africa-achieve-universal-internet-access-by-2030/a-59729090.
38 See e.g., Donatien Beguy, 'Poor Data Hurts African Countries' Ability to Make Good Policy Decisions', Quartz (20 August 2016), https://qz.com/africa/762729/poor-data-is-hurting-african-countries-ability-to-make-good-policy-decisions/; and 'Africa Regional Report', Open Data Barometer, https://opendatabarometer.org/3rdedition/regional-report/africa/.
39 Center for Human Rights & Global Justice, note 5.
40 Grace Mutung'u, 'The United Nations Guiding Principles on Business and Human Rights, Women and Digital ID in Kenya: A Decolonial Perspective' (2022) 7 Business and Human Rights Journal 117, 122.
41 'Project Appraisal Document on a Proposed Credit in the Amount of SDR 138.9 mollion (US$200 Million Equivalent) to the Federal Democratic Republic of Ethiopia for an Ethiopia Digital Foundations Project'', The World Bank (March 2021), https://documents1.worldbank.org/curated/en/421681619316030132/pdf/Ethiopia-Ethiopia-Digital-Foundations-Project.pdf.
42 'Nigeria Digital Identification for Development Project', The World Bank (2020), https://projects.worldbank.org/en/projects-operations/project-detail/P167183.
43 Olivia White et al, 'Digital Identification: A Key to Inclusive Growth', McKinsey & Company (2019), https://www.mckinsey.com/businessfunctions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.
44 Nubian Rights Forum and 2 Others v Attorney-General and 6 Others; Child Welfare Society and 8 Others (Interested Parties) [2020] Consolidated Petitions No. 56, 58 and 59 of 2019 (High Court of Kenya, Nairobi) eKLR, 1047 (I).
45 Ibid, paras 1029-30.

46 Ibid, paras 1035 and 1038.
47 Ibid, para 1038.
48 Ibid, para 1033.
49 Ekai Nabenyo, LONDA Kenya Digital Rights and Inclusion 2021 Report (Lagos: Paradigm Initiative, 2022) 5.
50 '#WhyID: World Bank and Dangerous Digital ID Systems Do Not Mix', Access Now (2022), https://www.accessnow.org/world-bank-digital-id-systems/; Silvia Masiero, 'A New Layer of Exclusion? Assam, Aadhaar and the NRC', LSE Blog (12 September 2019), https://blogs.lse.ac.uk/southasia/2019/09/12/a-new-layer-of-exclusion-assam-aadhaar-and-the-nrc/.
51 The World Bank, Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey (Washington, DC: The World Bank, 2019) 16-7.
52 For the example of Kenya, see Ekai Nabenyo, note 59, 6.
53 Chris Burt, 'Ethiopia's National Digital ID Prepares Foundation Ahead of Scale-Up', Biometric Update.Com (3 October 2022), https://www.biometricupdate.com/202210/ethiopias-national-digital-id-prepares-foundation-ahead-of-scale-up.
54 Bill Marczak et al, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', The Citizen Lab (6 December 2017), https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.
55 'Ethiopia: Hate Speech and Disinformation Law Must Not Be Used to Suppress the Criticism of the Government', Article 19 (19 January 2021), https://www.article19.org/resources/ethiopia-hate-speech-and-disinformation-law-must-not-be-used-to-supress-the-criticism-of-the-government/.
56 Marianne Díaz Hernández, 'Digital Identity: Our Five Calls to Action for the World Bank', Access Now (28 September 2022), https://www.accessnow.org/digital-identity-world-bank/.
57 Ibid.
58 Andrew Jack, 'Covid Crisis Offers Lessons in Digital Health and Data Responsibility', Financial Times (31 January 2022), https://www.ft.com/content/c2092e65-b639-4396-9e59-4d93e2e1e1d1.
59 Tage Kene-Okafor, 'African Health Tech Startups in the Supply Chain Segment Show Rapid Growth, Spurring a $7M Investment Initiative', TechCrunch (2 June 2022), https://tcrn.ch/3bnplm5; Alexis Akwagyiram, 'Nigeria's Tech Entrepreneurs Target Healthcare and Education', Financial Times (15 February 2022), https://www.ft.com/content/da2fdc82-fd3d-4628-a9dd-b83bb8a766d3.
60 'TechEmerge Health Challenge', CES, https://www.ces.tech/Global-Tech-Challenge/IFC-TechEmerge-Health-Tech-Challenge.aspx.
61 Tom Neumark and Ruth J Prince, 'Digital Health in East Africa: Innovation, Experimentation and the Market' (2021) 12:S6 Global Policy 65.
62 Ibid.
63 Akwagyiram, note 73.
64 'Hygeia 2014', IFC, https://disclosures.ifc.org/project-detail/ESRS/36007/hygeia-2014 (accessed 16 November 2022).
65 Adegoke and Takon, note 40, 10.
66 Ibid, 11.

67 'Making Digital Tools Work for Young People's Health and Rights – 3 Key Takeaways', Young Experts Tech for Health, https://yet4h.org/making-digital-tools-work-for-young-peoples-health-and-rights-3-key-takeaways/ (accessed 16 November 2022).
68 The E&S standards cover procedural expectations whereby clients should establish an adequate environmental and social management system, as well as substantive expectations that clients should prevent and address negative impacts in the areas of workers' rights, Indigenous People's rights, community health, safety and security, as well as land and resettlement.
69 'Benchmarking Study of Development Finance Institutions' Safeguard Policies, Consultations Draft', OHCHR (7 June 2022), https://www.ohchr.org/sites/default/files/Documents/Issues/Development/DFI/OHCHR_Benchmarking_Study_HRDD.pdf.
70 See e.g., The World Bank, note 2.
71 OHCHR, note 89.
72 Ibid, 58.

THE DANISH
INSTITUTE FOR
HUMAN RIGHTS