ecdpm The centre for Africa-Europe relations

The CHARTER PROJECT Africa
Democracy | Elections | Governance

DISCUSSION PAPER No. 331

Digitalisation and democracy: Is Africa's governance charter fit for the digital era?

By Ennatu Domingo and Lidet Tadesse Shiferaw

November 2022

Digital technologies have had a huge impact on governance around the globe. While increasing access to communication technologies has made it easier for citizens to mobilise politically, it also presents security risks. Social media platforms, for instance, are increasingly used to amplify and disseminate hate speech and incite violence. Digital technologies have also enabled some governments to expand their surveillance of political opponents, journalists and activists. Yet, policy instruments and frameworks have not kept up with the rapid adoption of digital technologies and their impacts on democratic processes. This is also the case for the African Charter on Democracy, Elections and Governance (ACDEG), which was adopted in 2007 to improve the quality of democracy and electoral processes across Africa and promote human rights and governance.

In this paper, we zoom in on the ACDEG and analyse the interlinkages between digital transformation, political activism and governance. We argue that the ACDEG should be adapted to respond to new challenges such as disinformation, hate speech and the digital divide. Digital technologies offer opportunities to further strengthen the provisions of the ACDEG. Furthermore, given the great potential of digital technologies to both limit and promote democratic processes, we recommend that the ACDEG includes stipulations on the diverse uses of digital technologies by state and non-state actors, particularly during electoral processes.

Table of Contents

List of Figures

Acknowledgements

This paper is part of the Charter Project Africa, a pan-African effort focused on the commitments in the African Charter on Democracy, Elections and Governance (ACDEG), which promotes the use of technology to amplify citizen voices and open spaces of collaboration between citizens, civic initiatives and African Union policymakers, at the national, regional and continental levels with an emphasis on digital formats. It receives funding from the European Union.

The authors thank Aisha Dabo from AfricTivistes. The authors are also grateful for the review and valuable feedback provided by ECDPM colleagues Martin Ronceray, Maelle Salzinger and Chloe Teevan. A big thanks goes to Michelle Luijben for editing, Joyce Olders for layout and Yaseena van't Hoff for infographics. All errors remain those of the authors. Comments and feedback can be sent to Ennatu Domingo (edo@ecdpm.org) or Lidet Tadesse Shiferaw (lta@ecdpm.org).

Acronyms

ACDEG	African Charter on Democracy, Election and Governance
ACHPR	African Commission on Human and Peoples' Rights
AU	African Union
AUC	African Union Commission
AUCSEG	African Union Cybersecurity Expert Group
AUDA-NEPAD	African Union Development Agency
BBC	British Broadcasting Company
CAR	Central African Republic
CCTV	Closed circuit television
CfA	Code for Africa
CHRGJ	Centre for Human Rights & Global Justice
CIPESA	Cooperation on International ICT Policy for East and Southern Africa
CPJ	Committee to Protect Journalists
CSO	Civil society organisation
DPA	Data Protection Act
DW	Deutsche Welle
ECA	Ethiopian Communications Authority
ECOWAS	Economic Community of West African States
EPRDF	Ethiopian People's Revolutionary Democratic Front
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GERD	Grand Ethiopian Renaissance Dam
ID	Identity document
IDS	Institute of Development Studies
IEBC	Independent Electoral and Boundaries Commission
IFC	International Finance Corporation
INMS	Intelligent Network Monitoring System
ITC	Information and Communication Technology
ITU	International Telecommunication Union
KIEMS	Kenyan Integrated Election Management System
LGBTQA+	Lesbian, gay, bisexual, transgender, queer, intersex, and asexual

MINUSCA	United Nations Multidimensional Integrated Stabilisation Mission in the Central African Republic
MOU	Memorandum of understanding
NEPAD	New Partnership for Africa's Development
NIIMS	National Integrated Identity Management System
ODI	Overseas Development Institute
RSF	Rapid Support Forces
SARS	Special Anti-Robbery Squad
SERAP	Socio-Economic Rights and Accountability Project
UN	United Nations
UNECA	United Nations Economic Commission for Africa
UPND	United Party for National Development
US	United States
USIP	United States Institute of Peace
ZANU-PF	Zimbabwe African National Union – Patriotic Front

1. Introduction: Digitalising democracy

The advent of innovative communication technologies has deeply changed how societies and their governments interact, affecting both democratic processes and the ways citizens engage on political issues. Social media, for example, offers users easy and inexpensive ways to follow global events in real time. leaders. Thanks to expanding access to mobile phones and internet connectivity, citizens can seek out alternative sources of information, collectively organise for both online and offline action, voice their concerns and demands vis-à-vis government authorities, and hold government actors accountable, for example, by naming and shaming. Digital tools are also becoming indispensable in key 'democratic rituals' such as elections.

Though the impacts of digital technology on democracy have been immense, these have been negative as well as positive. On the positive side, technologies have helped to improve political pluralism, facilitate government accountability and transparency, and expanded political participation through the democratisation of communication platforms (Cheeseman and Garbe 2021). For example, the relatively low entry barriers to participate in digital activism and organise have allowed previously unheard social groups, such as women and marginalised minorities, to exercise their agency and take leadership positions in social mobilisations. Indeed, these groups have faced social and cultural backlash when they assume prominent positions in the public sphere. On the negative side, governments are increasingly using digital technologies to consolidate and extend existing repressive practices, such as mass surveillance, targeted monitoring of users' digital footprints, curtailment of digital spaces through legislation and internet shutdowns, and promotion of pro-government digital platforms (Roberts et al. 2021). In 2021, governments of 12 African countries shut down the internet at least 19 times; while in 2020 this happened in 9 countries (Diaz Hernandez and Anthonio 2022). Furthermore, moving electoral processes online brings new risks of voter manipulation and tampering with voter registrations, polling results and vote tallying.

The interlinkages between digitalisation and political empowerment or repression in Africa are to be juxtaposed with the continent's overall low connectivity, the significant differences in internet use between social groups and between regions, and a strong urban-rural divide. In 2021, internet penetration rates ranged from 22% to 43%, with Eastern Africa and Southern Africa recording the lowest and highest connectivity respectively (Mwakideu 2021, Kramer 2022a and b). That same year, according to the International Telecommunications Union, close to 30% of Africa's rural population lacked mobile broadband coverage, while the number of internet users in Africa's cities was double that in rural areas (ITU 2021). In least developed countries (LDCs), most of which are in Africa, there is a particularly wide gender digital divide – only 19% of women in LDCs used the internet in 2020 compared to 86% of men (Kapiyo 2022).

This paper presents an explorative analysis of the responsiveness of the African Charter on Democracy, Election and Governance (ACDEG) to the societal and political transformations induced by digitalisation. Since its adoption by the African Union (AU) in 2007, the ACDEG has served as a legal "blueprint" – and in many ways a summary of other policy documents – outlining Africa's continental governance agenda (Wiebusch et al. 2019). It is legally binding and sets out principles to which state parties must conform. For example, states commit to promote and ensure democracy, rule of law, constitutional order, and peace and security for their citizens.

The ACDEG came into force in 2012, when it received the required minimum number of signatures. As of 2022, 35 countries had ratified it, and 46 had signed it (Ronceray and Shiferaw 2022; Engel 2022). The five years between the ACDEG's adoption and its entering into effect, as well as the continued lack of progress towards unanimous ratification, indicates that not all states are ready to submit to the ACDEG's expectations (Engle 2019). Moreover, like many AU legal and policy provisions, enforcing the provisions of the ACDEG has not been easy. Nonetheless, the ACDEG has proven its value in setting norms on accountable and democratic governance.

At the time of its adoption, the ACDEG was a 'progressive' legal document that identified and addressed some of the continent's main governance challenges, such as civil participation, inclusion and representation of women and minority groups, free and fair elections, and unconstitutional changes of government (Abdulmelik and Belay 2019). Yet, at the time of ACDEG's adoption in 2007, internet and mobile phone penetration was very low in Africa. Only 5% of the continent's population was online and just one out of four Africans owned a mobile phone (ITU 2008). While social media platforms, such as Facebook, were fast emerging elsewhere in the world, in much of Africa, social media were not commonly used due to limited connectivity. By 2022, however, the situation had changed markedly. Today Africa presents the highest share of mobile internet web page visits, and social media platforms are popular – even if the continent still lags behind in mobile coverage by global standards (Galal 2022b).

The ACDEG did not anticipate, nor does it address, the prospects and challenges brought about by digitalisation. This paper, therefore, examines the relation between digital technologies and political governance, seeking to understand what the digital era means for the ACDEG's relevance and applicability. Based on desk research, section 2 identifies how digitalisation could enable the realisation of the ACDEG's provisions and support the practice of accountable governance. Section 3 then discusses how digital technologies have exacerbated or made more apparent some of the existing challenges in promoting democratic governance in Africa. Section 4 examines "new" dynamics that are emerging due to digital technologies and their application in various aspects of political governance. The paper then ends in section 5 with a summary of key takeaways and entry points for the adaptation of existing frameworks or the introduction of new norms.

2. Digitalisation as an enabler of governance

While every country has its own path to democracy and political accountability, African countries have subscribed to a number of continental-level principles, ideals and processes around democracy. While much has been written on the role of the AU as a democratic norm setter and the reasons why norm enforcement is difficult and political for the AU, there has been little discussion on how the practice of democracy is changing due to digitalisation.

Advancements in digital technologies are changing electoral processes. For example, several African countries have partially or fully digitised their electoral processes (Mosero 2022). This has the potential to introduce greater transparency and overcome challenges regarding electoral manipulation even if the exclusion of some segments of the population and manipulation of results cannot be fully ruled out, due to the complexity of e-voting processes.

At the same time, digital technologies make state repression easier, from surveillance to control of civic and political spaces, and election rigging. The use of social media has enabled the rise of disinformation, proliferation of hate speech and online harassment based on gender or other identities.

While these developments put to question the relevance of frameworks like the ACDEG in the digital era, this section discusses some of the ways in which the ACDEG is still relevant in the digital age. It specifically explores how digital technologies enable the realisation of the principles of the ACDEG.

2.1. E-governance

The ACDEG primarily addresses states and bestows various responsibilities on them with regards to the promotion of good governance through transparent and accountable institutions. Digitalisation facilitates this by making information dissemination and government service provisions easier. **Governments thus increasingly rely on the internet and digital technologies to communicate with citizens and carry out their responsibilities through what**

is commonly referred to as e-governance. For example, laws, policies and government regulations are announced online and public documents and tenders can also be disclosed to the general public. Many countries also use digital data registry systems to document births and deaths and to issue certificates, passports and other legal documents.

Public services such as e-health and e-education services are increasingly being integrated in public service provision notably due to the momentum generated by the COVID-19 pandemic. In the draft African Union Digital Education Strategy and Implementation Plan, the AU stressed Africa's commitment to build a digitally skilled society and to accelerate the adoption of digital technologies for education. Despite the growing synergies between education and digitalisation in the past two years, a wide rural-urban divide in provision of digital services undermines the implementation of the AU's strategy. Significant ICT infrastructure and greater internet literacy will be needed to expand connectivity to rural areas and include lower socio-economic segments of societies.

E-payment platforms, similarly, have eased the process of collecting taxes and service fees for utilities. This has both reduced administrative burdens on government and given citizens greater access to public information and services. Ghana, Mauritania, South Africa and Tunisia, for example, are rated high on the United Nations' e-government development index (AUDA-NEPAD 2022). Digitalisation allows governments to easily share information across line ministries and departments, in many cases, reducing bureaucracy and increasing efficiency.

Beyond use of the e-payment platform to provide immediate economic relief, other digital technologies, such as satellite imagery, machine learning and mobile data, are helping the government identify beneficiaries and strengthen communities' long-term resilience to shocks (WB 2021a and b). An example in this regard is Togo which used e-payment platforms to provide social welfare during the COVID-19 pandemic. Its Ministry of Digital Economy and Digital Transformation (MENTD) launched the Novisii programme (*novisii* means 'solidarity' in Ewe, a local language). At the peak of the pandemic, the government was able to use this digital social protection cash transfer scheme to distribute some US $23 million to more than 572,852 informal sector workers, of whom 65% were women. By providing a new means of gaining information from citizens, digitalisation has helped some governments design better social protection schemes and enhanced resilience to external shocks even if the mechanisms used for such purposes have also expanded surveillance by states (Alcorn 2021: Roberts et al. 2021)

Increased internet penetration and digitalisation is expected to have positive economic and social contributions in Africa as in elsewhere. The World Bank (2022) for example estimates that a 10% increase in mobile broadband penetration in Africa would generate a 2.5% increase in GDP per capita. In addition to the economic significance, an expanded access to mobile broadband can contribute to financial inclusion and servicing of underserved communities through mobile banking and micro-credit schemes. For example, a globally renowned Kenyan mobile payment system – the M-Pesa was able to transform the mobile money landscape in Kenya and beyond. When M-Pesa was launched in 2007, only 26.7% of the population had access to bank accounts and could transfer money; ten years later that had risen to more than 74% (Ndung'u 2017).

When done well and equitably, e-governance contributes to good governance. Digital tools can promote transparent and accountable institutions, advance civic education and provide means of skills training for citizens, while fostering richer political and social dialogue. All of these are stipulated as state responsibilities in Chapter 5 of the ACDEG. However, although Article 27 of the ACDEG promotes the development of ICT, the charter says nothing about digital governance, online safety, digital rights (such as freedom of expression in online spaces) or cybersecurity (Ronceray and Tadesse 2022). Nor does it address the concept of digital sovereignty. The AU, and some countries individually, are developing their own policies to enable digital governance; yet these frameworks are not explicit about states' responsibility to use digital technologies to uphold democratic principles.

2.2. Direct interfaces between citizens and duty bearers

A guiding principle of the ACDEG is effective citizen participation in democratic processes and in building democratic institutions (Art. 3). In Africa, countries have made varying degrees of progress in building democratic institutions, and the scope and quality of citizen engagement in democratic processes similarly differs. In theory, digital technologies provide additional avenues for governments to expand and facilitate citizen participation and involve them in public institutions. In practice, however, two-way interaction between citizens and public institutions is easier said than done. The difficulty is in part due to uneven access to digital technologies, states' use of digital technologies as an instrument of control, and the questionable effectiveness of online engagement in comparison to – or when divorced from – offline engagement.

Nonetheless, public institutions and officials increasingly use digital tools, such as social media platforms and government websites, to interact with citizens. For example, in 2019 South African president Cyril Ramaphosa held his first Twitter live chat to engage with citizens, though this was part of an online campaign ahead of elections. In Ethiopia, the National Election Board created a Twitter profile and used the platform to conduct online question-and-answer sessions to inform voters about the electoral process ahead of the 2020 national elections. In Kenya's 2022 general elections, one area of progress, according to the country's electoral commission, was in the public online dissemination of results from polling stations. This enabled citizen groups and the media to do their own independent tabulations and tallying of results.

The civic technology sector is still growing, bringing a stream of new web platforms and mobile applications geared at enhancing the political impact of civil society organisations on the continent. In Mali, the mobile phone application 'MonElu' allows citizens to directly contact their elected officials to raise concerns and provide ideas for improving governance, thereby increasing government accountability and citizen engagement (Do4Africa n.d.). In Kenya, the Mzalendo non-partisan parliamentary monitoring organisation uses technology to make the country's parliament more accessible, connecting the representatives with their constituents through the rollout of legislative trackers in selected countries.

Such possibilities allow citizens to claim more influence over public institutions and political processes including through online naming and shaming tactics. For example, Nigerians used social media to express outrage at their government representatives' abandonment of the country's already fragile and under-resourced public health system during the COVID-19 pandemic, while those same representatives sought medical care for themselves abroad (Twitter 2020; Onminyi 2020). In other countries similar expressions of discontent led to offline protests, yet the outcry in Nigeria dissipated in the depth of social media.

While t**he impact of such online mobilisation in effecting greater compliance with the ACDEG principle of transparency and fairness in management of public affairs is limited, these examples indicate that digitalisation can catalyse implementation of the principles enshrined in the ACDEG**. More focus is needed on connecting technology solutions, to link citizens across borders, to connect them with the AU's different organs and jointly press for change (Civic Tech in Africa 2022).

2.3. Citizen activism

The fundamental right of civic and political organisation is another area in which the provisions of the ACDEG apply in the age of digital democracy. Worldwide, the internet has changed how citizen activism is exercised. Individuals and organised groups, including civil society organisations that would not otherwise have formal spaces for expression, are using the internet and social media to create their own platforms. Social media, in particular, have

advanced citizen mobilisation and collective action, especially in contexts where offline spaces are limited and politically controlled. Some of this online mobilisation has influenced decision-making and led to offline action and reform. In Ethiopia, Twitter and Facebook were used to disseminate information on protests that led to the overthrow of the Ethiopian People's Revolutionary Democratic Front (EPRDF) coalition in 2018 (Meseret 2020).

Similarly in Nigeria, social media has allowed activists to transition from online agitation to fully fledged offline protest, as in the 2020 protests against the Nigerian Special Anti-Robbery Squad (SARS). Since 2017, Nigerian citizens have used social media to report excessive violence by SARS. In 2020, this burgeoned into a social media campaign with global reach under the hashtag #EndSARS. The peaceful, offline youth-led protests that followed were met by police violence. The movement was successful in forcing the government to disband SARS. But demands for the compensation of families who lost someone due to police brutality and calls for independent investigation and prosecution of perpetrators of police misconduct were not satisfactorily met (Vanguard 2020; Uwazuruike 2021).

The examples from Nigeria and Ethiopia, as well as those elsewhere, such as the 'Arab Spring', provide precedents for the transformative potential of online social movements. Specifically, they offer two lessons on how digital tools can lead to change. First, **digital activism may be most effective when paired with offline action and not instead of it**. This demonstrates the continuing relevance of offline civic engagement and the value of open offline civic and political spaces for the consolidation of democracy and accountable governance, as stipulated in the ACDEG (Art. 12). In various countries on the African continent, the 'shrinking of civic space' has emerged as a challenge in the past two decades. **While digital tools allow citizens to circumvent some legal and physical barriers, offline civic spaces remain necessary for transformative change.**

The second lesson on how digital tools can lead to change derives from the experiences of women, minorities and other socially marginalised actors. **In digitalised environments, these actors may be able to overcome some cultural and structural barriers and take a more central role in initiating and leading civic and political movements** (Salzinger et al. 2022). Digital activism blurs the line between the public and private spaces; it allows anonymity and provides for broader platforms from which actors can generate support. Digital activism, therefore, has potential to increase women's political and civic participation even if various examples demonstrate that women continue to be excluded from formal processes once online and offline movements formalise (Salzinger et al. 2022).

2.4. Three challenges preventing citizen online participation

The positive contributions of digital technologies towards the realisation of the principles of ACDEG explored in this section, should, however be contextualised. First, in many African countries **digitalisation bypasses certain segments of the population**, due to – among other things – the pervasive rural-urban and gender digital divides. If online engagement becomes the primary form of citizen involvement, without the necessary infrastructural and economic advances, inequitable access to digital tools will only be worsened.

Second, **digital participation and interfaces – on their own – may not offer the depth and quality of citizen engagement that's needed to promote truly accountable institutions** and to ensure checks and balances. In fact, digital activism and public participation conducted online has been termed 'slacktivism' (Lodewijckx 2020), as actions such as 'liking', commenting and forwarding which are done at the users' convenience online, may lead users to feel that they have done their part and need take no further action even if a situation demands it.

Third, government officials tend to use social media to engage with citizens solely when they need to expand their support base. These factors reduce meaningful citizen engagement and democratic reforms in African countries. Fourth, the **tools availed by digital technologies can also be used for repression**. States, too, are resorting to digital

tools, not only to serve their citizens, but also to control and regulate their actions. This 'digital authoritarianism' is the subject of the next section.

3. The digitalisation of governance challenges

Digitalisation can improve state-society relations and facilitate good governance as discussed above. But it is not immune to exploitation by state and non-state actors. Digitalisation has tremendously added to states surveillance capabilities as phones and electronic devices as well as one's digital activities can be tracked and monitored towards both commercial and political purposes. As an extension of political repression, the internet and certain social media or civic tech tools can be fully or partially blocked and/or censored to curtail or contain political dissent.

Such repressive acts resemble tactics used in offline repression and hence are not new per se. They are new facets of existing challenges but they have arguably become more pronounced in the digital age. Misinformation and voter manipulation, which pre-date the internet, are increasingly being used and weaponised by state and non-state actors, including to undermine electoral processes in third countries. **While repression and censorship were once the sole prerogative of states, digitalisation has empowered certain non-state actors,** including businesses (e.g., Facebook and Twitter), to get involved, alongside foreign governments and political opponents with minimal or dubious accountability. These actors present an unprecedented security threat. They can fuel unrest through disinformation campaigns and public manipulation based on societal fault lines. Foreign actors can also interfere through the actions of domestic actors, with the aim of promoting their own political or geopolitical interests (Teevan and Shiferaw 2022; Sambuli 2022).

This section examines the digital aspects of repression and authoritarianism to analyse the potential applicability of the ACDEG in this emerging context.

3.1. Digital repression and shrinking civic space

In repressive political contexts, civil society space is tightly controlled; political opponents are harassed; information flows are regulated, often in favour of the incumbent government and political mobilisation may be curtailed or closely monitored. These repressive tactics are found in many countries in Africa, though the degree of repression or freedom varies in each context. According to a 2019 Afrobarometer study, citizens in 34 African countries expressed concern about shrinking civic and political space, as governments increasingly reduced citizens' freedoms. Interestingly, however, the study also reports a slight decline in citizens' support for freedom. In the context of a threat to collective security, citizens expressed willingness to accept an increase in government control of their activities (Logan and Penar 2019).

Repressive tactics are used in online civic spaces as they are applied in offline spaces. Political opposition is at times met with internet shutdowns, social media blackouts, or restrictive laws which limit citizens' access to digital tools, their privacy and data rights. Such developments are especially common in periods leading up to elections and in the heat of anti-government protests. For example, in 2019 Chad imposed a social media blockade for over a year – the longest social media outage to date in Africa (Ro 2019). In June 2021, Nigeria banned Twitter for four months after the company deleted a controversial tweet from President Mohammadu Buhari. The tweet allegedly linked the 1967-1970 Nigerian Civil War with recent attacks on government offices by secessionist groups in the south-east of the country (BBC 2021). In this case, the Nigerian government accused Twitter of double standards: removing content while sponsoring dissent in the most populous country in Africa. It went on to demand that the platform be used only for "business and positive engagement" (Nyambura 2021).

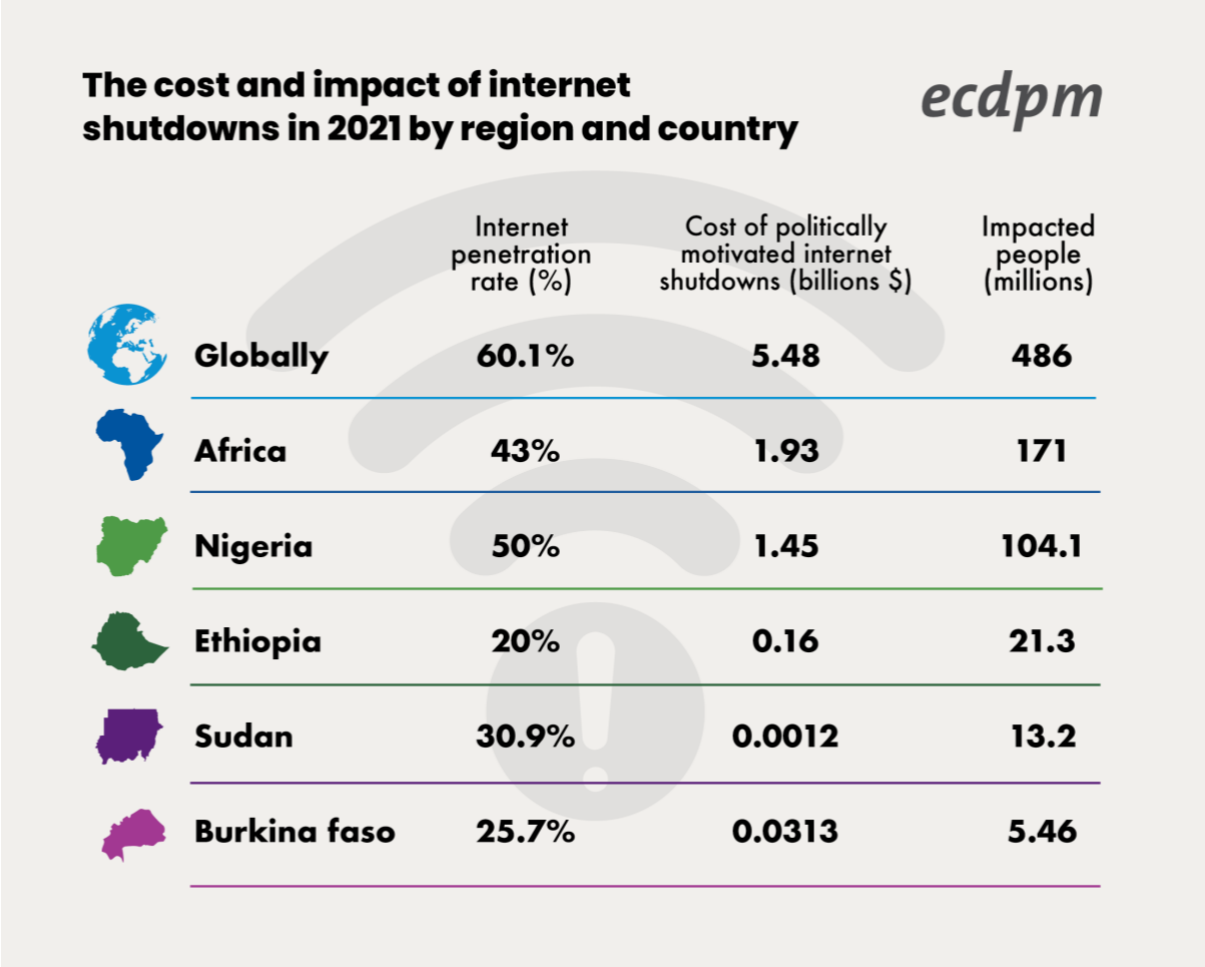
Beyond full or partial internet shutdowns and the banning of social media platforms, **some countries have enacted laws and regulations that indirectly limit social media usage, mainly by increasing the cost of connecting to the internet**. Uganda's government, for example, introduced an over-the-top tax (also known as social media tax) imposing a daily fee of US $0.05 for using social media platforms, such as Twitter, Facebook and WhatsApp. Implementation of the tax was presented as a means to increase the country's revenue base, so that it could pay off a $18.4 billion debt. However, the effect was a drop in internet use from 47% in 2018 to 35% two years later, as low-income users stopped using the internet (Digwatch 2021: Becker 2021). After the policy failed to raise the targeted revenue, the government introduced a direct tax on internet usage, making Uganda one of the most expensive countries in terms of data usage (Figure 1; see also Karombo 2022). In 2021, Uganda's government passed a bill imposing an additional 12% tax on data packages, bringing the total amount of tax on internet service provision to 30% (Kafeero 2021).

Foreign actors, too, have leveraged digital technologies against African nations' sovereignty through disinformation campaigns aimed at shifting national discourses, especially ahead of elections. For instance, in December 2020, Facebook identified French and Russian disinformation campaigns attempting to influence internet users ahead of elections in the Central African Republic and Nigeria (Stubbs 2020). A year earlier, the Israeli political consulting and lobbying firm Archimedes conducted a disinformation campaign to boost Muhammadu Buhari's presidential candidature in Nigeria (Debre 2019). Since these events, Facebook and other social media have been subject to greater scrutiny, including of their newly acquired authority over the most influential digital spaces where narratives are shaped. These companies' authority to enable or disable online (political) content gives them a unique position to control participation in online spaces and moderate content. In addition, the amount of data that social media platforms collect and the unregulated influence of a few technology giants are also issues that warrant further exploration.

Governments have embraced restrictive measures with the justification that exerting control over parts of the internet will help them maintain national security and public order, halt foreign interference and disable violent mobilisation induced by online and offline incidents or hate speech. However, these measures have also enabled them to clamp down on political opposition. Their attempt at curtailing disinformation and holding social media users accountable in some cases contravene international human rights instruments, including the African Charter on Human and Peoples' Rights.

In June 2021, the Court of Justice of the Economic Community of West African States (ECOWAS) ruled that Nigeria's four-month ban on Twitter was unlawful and inconsistent with the provisions of both Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the International Covenant on Civil and Political Rights (Africanews 2022). Similarly, Ethiopia's Hate Speech and Disinformation Prevention and Suppression Proclamation has been criticised by organisations such as the Cooperation on International ICT Policy for East and Southern Africa (CIPESA) for failing to meet the necessity and proportionality tests stipulated by the International Covenant on Civil and Political Rights (CIPESA 2020). CIPESA also found the proclamation's definition of hate speech and disinformation to be broad and ambiguous and therefore open to arbitrary interpretation by law enforcement, putting at risk citizens' rights to freedom of expression and access to information. In terms of content flow, CIPESA observed that holding intermediaries liable for content policing, in this case of false information and hate speech, without clear aims, contravenes international human rights instruments such as the African Charter on Human and Peoples' Rights.

Figure 1: The cost and impact of internet shutdowns in 2021, by region and country



Worldwide, governments have used internet shutdowns to exert fuller control over access to and use of information. In 2021, the #Keepiton coalition recorded 182 internet shutdowns in 34 countries. That same year, 19 shutdowns were recorded in 12 African countries (Access Now 2022). Faced with governments' increasing use of this measure, activists have raised concerns about the erosion of democratic principles. This issue is difficult to address as governments regulate telecommunication operators and allocate their licences.

Blocking internet service and banning social media platforms can be understood as elements of an increasingly sophisticated package of government measures used to control citizens' online engagement. Since 2017, 31 of Africa's 54 countries have blocked social media. In an analysis of the digital rights landscape of 10 African countries, the African Digital Rights Network concluded that when governments close offline civic spaces, citizens respond by accessing social media platforms that offer an unrestricted open civic space, including reliance on encrypted instant message apps (IDS 2021).

However, when faced with government censure of social media platforms, internet shutdowns and state surveillance, citizens generally become fearful of openly and freely participating in political activities. Furthermore, internet shutdowns can mask other human rights violations amidst information blackout, away from public scrutiny. That said, the fact that the internet is equally used for violent mobilisation cannot be overlooked (UN 2022).

Politically motivated internet shutdowns exact a high price on national economic stability. In July 2020, the Ethiopian government shut down internet services for more than 20 days after the killing of the prominent Oromo singer and activist Hachalu Hundessa and subsequent targeted killings of 166 non-Oromo people by ethnic Oromo armed groups. The shutdown was to stop the hate speech being broadcast by the Oromo Media Network based in Minnesota and to counter attempts to instigate violence by online diaspora activists (Minority Rights Group 2020; BBC 2020a). During that shutdown, however, Ethiopia is estimated to have lost at least US $100 million, according to NetBlocks (Tekle 2020). In another example, Uganda's FinTech sector lost some $17.9 million per day during the 100 hour internet shutdown that started 14 January 2021 (Bhalla and McCool 2021).

As Africa's digital economies grow, and businesses and ordinary citizens become more reliant on the internet and social media for communication and livelihood generation, governments will therefore need to calibrate their actions to minimise potential harm to the economy and innovation (Allen and Kelly 2022).

3.2. State surveillance

African governments have made significant strides in their technical capacity to intercept and conduct surveillance. The United States, China, Russia, France and the United Kingdom are exporters of artificial intelligence technology, including mass surveillance and facial recognition equipment. Moreover, these actors have been competing for dominance in foreign security markets and policies, and in doing so have influenced digital authoritarianism in Africa. The Israeli NSO Group develops technology for use by governments to prevent local and international threats. Its Pegasus spyware is in use by countries including Egypt, Morocco and Togo to spy on dissidents. Political and military leaders in countries using such technologies have substantial leeway in the absence of robust regulation of global surveillance technology transfer (Kodjani 2021; Dadoo 2022).

Chinese state based and private companies have been dominant investors in African digital infrastructure. Organisations associated with China have built 14 government intranets and gifted computers to 34 African governments (Harsono 2020). As of 2020, thirteen African countries including Egypt, Ghana and South Africa had deployed surveillance technologies (Jili 2020). In 2014, the Kenyan government awarded a tender to Safaricom to build a communications and security surveillance system worth US $14.9 million, including installation of closed-circuit television (CCTV) cameras on roads and in public spaces. The equipment is to be procured from the Chinese company Huawei. Such systems, operated in a context where there is an absence of data protection law, raise concerns about the potential to target opposition groups, activists and researchers (CIPESA 2019).

Some African countries shore up their mass surveillance capacities and engage with foreign governments and private companies with the stated objective of counterterrorism and law enforcement measures. In 2017, South Korea signed an agreement with Tanzania to enhance the latter's cyber capabilities. In Uganda, the government set up an intelligent network monitoring system (INMS); among other things, the system can intercept calls on all networks (CIPESA 2019). Intelligence officials in Uganda rely on technology to access encrypted communications of opposition leaders, other countries, such as Kenya, are said to use 'eyedropper' remote-control hacking systems to access text, calls and locations of opposition leaders (Jili 2020).

In 2021, the Nigerian government approved a US $2.1 billion supplementary budget to equip the military with new surveillance tools purportedly aimed to curb the spread of COVID-19; however, $11.2 million of that amount was allocated to the National Intelligence Agency to intercept, monitor and track calls and messages on the country's most popular social media platforms, WhatsApp and Thuraya (Aborisade 2021). In response, the Socio-Economic Rights and Accountability Project (SERAP), a non-profit organisation promoting transparency and accountability in Nigeria's management of natural resources, sued the Buhari administration for allegedly violating Section 37 of the

constitution, which guarantees and protects "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications". The government justified intercepting WhatsApp messages citing the need to deter cybersecurity attacks. Yet, the announcement of the measure came after the government banned Twitter, leading activists to fear mass surveillance and loss of their right to privacy and expression. Some have expressed fear that the measure will open the door to the targeting of political opposition and journalists dealing with critical information (Vanguard 2021).

While surveillance is not new, use of digital technologies has expanded surveillance capabilities, not only of states but also of commercial actors, in Africa and elsewhere. States' adoption of new laws expanding government surveillance power, in the absence of data protection laws, risks violating citizens' right to privacy (Roberts et al. 2021). Some 80% of African countries have national cybersecurity laws, which puts Africa on par with other world regions in this domain. Nonetheless, establishment and implementation of data protection frameworks in Africa have lagged. Only 28% of African countries had adopted data privacy laws in 2021 (Lemma et al. 2022). Furthermore, some of these data privacy laws have been criticised for failing to strongly specify the legitimate use of data, provide accountability mechanisms and for allowing the easy processing of sensitive personal data.

Beyond examples of states abusing their surveillance powers, concerns have also been raised regarding more benign and even productive e-services and e-governance platforms. Without appropriate regulation, these too can become tools of surveillance, repression and exclusion. According to the New York University Law School, robust evidence has emerged from different contexts showing that the digital ID systems that are being embraced across Africa for their development potential, especially for financial inclusion, can in fact result in exclusion, discrimination and other human rights violations (CHRGJ 2022). **In countries where registration for an ID is tied to possession of official identification documents, such as birth certificates and national identity cards, individuals without such documents may be excluded from basic services,** like education, healthcare and social services (CIPESA 2022). Without broad reforms, and especially policies addressing data privacy risks, digital ID systems tend to replicate existing inequalities. In Uganda, for example, the digital ID system does not recognise the Maragoli community; thus, offline discrimination is carried over into the digital space, as those who do not register may not access public services.

The regulation of public data, namely data acquired through digital ID systems is pertinent to maintaining citizens' right to privacy. In Ethiopia, the Digital Identification Proclamation was launched in August 2022 with the aim of issuing 70 million IDs by 2025. This legislation was not accompanied by adoption of a personal data protection proclamation that would allow the establishment of an independent data protection commission (Teshome 2021). Critics have expressed concern that the rather vague and simple privacy guidelines in place are insufficient to resolve questions surrounding privacy, data collection and storage. They have proposed that sections of the proclamation be amended to ensure establishment of a data protection commission with full budgetary and political independence (Wodajo 2022; Eneyew 2022).

The majority of countries that have adopted national data protection laws have not yet ratified the Malabo Convention on Cyber Security and Personal Data Protection. As of 2022, that convention had been signed by only 14 countries and ratified by 13, (AU 2022d). African governments can still rally behind a common regulatory approach, both to promote fuller data protection and privacy and to develop a shared understanding of how to respond to threats to privacy in the digital space (CIPESA 2022b).

Collective standard setting on data and privacy regulation is pertinent in Africa because information systems that are located abroad and operate under foreign regulatory standards present particular complications for digital governance. Despite the construction of more than 100 data centres on the continent, much of the digital

infrastructure that Africa relies on is hosted outside the continent, raising concerns about high costs of managing and exchanging data and vulnerability of African governments to foreign economic and political agendas (Domingo and Tadesse 2022). The AU's new Data Policy Framework, is a step in the right direction as it intends to facilitate cooperation between countries on data protection to safeguard and secure data flows

3.3. Gender-based digital harassment

Digital technologies are enabling African women to increase their role in politics, including helping them to challenge gender norms. Using encrypted messaging, for example, women, including those from rural areas, engage on policy issues and express their political interests and priorities. However, traditional conceptions of women's roles have remained pervasive, and the gender digital divide in fact widened in the least developed countries in recent years. In 2020, 24% of African women had access to the internet, compared to 35% of African men (Salzinger et al. 2022). Women were also less likely to own mobile phones and computers, or to have regular access to such technologies (Lardies et al. 2019).

Many examples from across Africa demonstrate that women use information technologies to influence decision-making processes, albeit with limitations. For instance, women played a crucial role in the 2018-2019 protests that brought down the administration of President Omar-al-Bashir in Sudan. They mobilised supporters using social media hashtags such as #TasgotBas (meaning #FallThatIsAll) even if they were side-lined in the transition negotiations(Salzinger et al. 2022).

While even successful mobilisations may not have immediate impact on gender equality, women at the forefront of such online and offline movements face backlash and remain targets of online gender-based harassment. Online gender-based harassment is a reflection of violence inflicted offline, mostly on women, LGBTQA+ and other communities (Achieng 2022). A 2016 survey of women legislators worldwide conducted by the Inter-Parliamentary Union found that 82% had experienced digital gender-based violence, including circulation of humiliating fake sexual images. More recently, Policy found that more than half of the surveyed 3,306 women in five African countries had experienced or witnessed accounts of online violence. Although **African countries are developing laws on cyber-harassment and cyberbullying, these seldom acknowledge the gender aspect of digital harassment.**

Many African countries have committed to boost women's political participation through both national policies and international and continental frameworks, such as the Maputo Protocol on Women's Rights. Regarding **the ACDEG, even though one of its objectives is to "promote gender balance and equality in the governance and development process", it falls short in recognising the interlinkages between digital transformation and gender issues.** Greater recognition of women's limited access to digital technologies and of the specific challenges women face in the digital space would help governments ensure that digital technologies and associated regulations do facilitate women's greater political and economic participation.

3.4. Election manipulation

Elections are a major area in which digital technologies have made inroads. The idea that technology can improve electoral credibility and legitimacy is popular among digitalisation's proponents. Even before the pandemic, governments across Africa had introduced digital technologies in various phases of their electoral processes. Digital voter registration, voter verification and results transmission had been implemented, and technologies were in use to help voters find polling locations. During the COVID-19 pandemic, advocates pushed for even more extensive digitalisation of electoral processes, as an effective means to balance public health concerns with the need for credible elections (Ilo and Osori 2021).

Yet, studies indicate that while digital technologies can reduce electoral manipulation and bring greater clarity and transparency to electoral outcomes, the political context in which these technologies are used matters (Wolf 2017; K'onyango 2022). The quality of democracy and the independence of electoral commissions determine to what end and in what ways digital technologies can add value to electoral processes (Cheeseman et al. 2018). In the 2017 elections in Kenya, the Supreme Court declared the results ``illegal, null and void" despite the wide use of digital technologies, including voter registration and verification and real-time transmission of voting results, due to lack of checks and balances to curb corrupt practices (Mutung'u and Biddle 2017).

Biometric voter identification is a digital technology seen as an effective response to large numbers of 'ghost' voters casting ballots. Implementation of the technology has brought increased confidence in electoral results among opposition leaders and their supporters. On the other side of the spectrum are voter manipulation, smear campaigns and political influencing. These are pre-existing challenges to electoral processes which have been scaled up as a result of digital technologies. Deliberate voter manipulation such as the one carried out by the British political consulting firm Cambridge Analytica in the 2017 elections in Kenya, whereby it used social media-based political advertisement to target specific users, continues to be a risk to democracy (Nyabola 2019). The Cambridge Analytica scandal also demonstrated that, unlike analogue electoral processes in which local actors – usually public institutions – are the primary culprits undermining electoral competition and integrity, **digital technologies create ample opportunity for non-state actors such as private firms and international actors (state-affiliated or otherwise) to influence election outcomes in any given country**.

But private firms are not the only influencers in the electoral landscape. Of late social media influencers are becoming popular avenues through which political parties shape narratives, voter perceptions and the credibility of their opponents in the run up to elections. In 2018, Zimbabwean President Emmerson Mnangagwa urged the Zimbabwe African National Union – Patriotic Front (ZANU–PF) youth league to use social media to undermine the opposition (Zimeye 2018). Allegedly, the ZANU–PF paid savvy internet users to disseminate pro-government political information ahead of the voting (Freedom House 2022). Social media can therefore be a strong tool for accountability and participation in the electoral process, but it can also serve as an instrument for defamation of opponents.

Electoral manipulation and rigging undermine not only the consolidation of accountable governance in Africa but also peaceful transitions of power. The ACDEG and various formal and informal AU normative frameworks reiterate the importance of electoral integrity and election monitoring. Oversight and observation of the whole electoral cycle is one of the AU Commission's foremost operational roles. Yet, digital technologies and electronic voting pose both challenges and opportunities for monitoring missions. What this means in relation to the ACDEG and the AU's role in election observation is discussed below.

4. New challenges to democratic governance and the ACDEG

Section 1 and 2 of this paper explored how digital technologies are changing politics. Governments increasingly rely on digital tools to carry out their responsibilities. Citizens, in turn, are accessing social media to participate in politics and make their governments accountable. Digital technologies have been embraced as promoting transparent, fair and inclusive democratic societies, though with few caveats. These are the digital divide, surveillance, the manipulation of electoral processes and harassment of minorities and political opponents. Though some of these challenges pre-dated digital technologies, they have been amplified by digitalisation.

This section discusses new challenges in governance that have been brought about by digital transformation. The aim is to highlight the linkages between civic and political activism, governance and digital transformation which may be overlooked by the ACDEG.

4.1. Regulating the digital sphere: Non-state actors

The past two decades has seen exponential innovation and expansion of digital technologies and internet penetration, in Africa and elsewhere. This has created a booming global digital economy where non-state actors, namely local and international private companies and individual citizens have been empowered. This digital transformation has numerous social benefits. But it also presents challenges regarding taxation, data flows and intellectual property rights, to name a few. For governments, regulating some of the global tech giants that operate in their countries but which may be registered elsewhere presents both an economic and political challenge. **Regulating the data that is generated through social media platforms, e-government portals, commercial services and internet search engines also has economic, political and ethical implications.**

The protection of citizens' personal data vis-à-vis both foreign technology companies and governments has been a particular item of discussion of late (Elmi 2020). The former extract data for profit while the latter collect data for security and public policy purposes. African governments are developing their own comprehensive data protection laws, with Kenya, Rwanda and South Africa leading the way. But norms around regulating the digital ecosystem to ensure ethical data extraction, local economic benefits, and state sovereignty are just emerging (Teevan and Shiferaw 2022).

While there's an emerging literature on digital repression as discussed in previous sections and also on digital governance and the regulation of tech companies, the policy discourse around **the digital accountability of non-state actors, such as citizens and media is still limited**. Digital tools namely social media and tech solutions empower citizens, yet these same tools are also exploited and abused by individuals and groups for the dissemination of hate speech, incitement of violence, misinformation and also political manipulation. Holding actors that are behind such actions has not been easy not only because it's not easy to identify who's behind them but also because it takes tremendous human and technological resources to identify and respond to harmful online content in a timely manner.

The increasing use of paid social media influencers to attack political opponents for local political gains or around elections also blurs the line between private citizen engagement and commercial advocacy. The monetisation of a person's social media following for political ends – without full disclosure – may be well within one's freedom of expression but it highlights how civic engagement and activism can easily be instrumentalised.

Furthermore, because social media platforms do not limit the number of accounts that an individual user can create, political contenders can operate fake accounts to disseminate disinformation and evade accountability. In 2021, for example, Facebook reported shutting down a network of nearly 1,000 accounts and pages with more than 1 million followers run by people allegedly linked to the paramilitary Sudanese Rapid Support Forces (RSF) led by the deputy head of the ruling Sovereign Council Mohamed Hamdan Daglo (known as Hemedti). In the same period, the platform also shut down a network of more than 100 accounts and pages with 1.8 million followers connected to Omar-Bashir's supporters in Sudan (Eltahir et al. 2021).

The ACDEG stipulates that state parties should take "measures to ensure and maintain political and social dialogue, as well as public trust and transparency between political leaders and people in order to consolidate democracy and peace" (Art. 13). However, as digital democracy blurs the lines between the various actors, how states can carry out

these responsibilities is unclear. Who should regulate online engagement or global multinational tech companies and in what ways, is a controversial issue. Finding the right balance between the maintenance of state sovereignty, the promotion of digital innovation and upholding fundamental human rights such as the right to privacy and free speech is not straightforward either (Roberts et al. 2021).

4.2. Social media: Polarisation, disinformation and hate speech

Social media has a net positive effect in democratising information flows, particularly by enabling mass mobilisation and creating spaces for accountability through public naming and shaming. Especially in the face of shrinking offline spaces for civil society, social media offer a valuable alternative. Social media has played a major role in ending the traditionally 'secretive' conduct of domestic and international politics whereby key debates and decision-making occurred away from the public spotlight (Nyabola 2020). Today, politicians can and do use social media to make their positions clear and to communicate to their constituencies and audiences in a targeted manner (Nyabola 2020).

Despite social media's positive contributions, they also pose several challenges that risk undermining democracy and accountable governance. **First, social media informs public opinion and government policy, giving a semblance of 'citizens' voices' while in reality, online citizen engagement is not representative of offline reality**. This is because internet connectivity is limited, not everyone uses social media for social or political activism and algorithms also influence what's 'trending' and goes viral.

As of 2020, Africa counted just 233 million Facebook subscribers, out of a population of 1.3 billion; indeed, only 48% of Africans had electricity in that year (Boakye 2021). Moreover, even when Africans are online, social media algorithms de-emphasise their interests, while amplifying the concerns of others deemed more relevant (Ndlela 2022). For example, communities using non-colonial languages are misrepresented or disregarded in online discourse as algorithms are not trained in them.

In a similar vein, 'bots' or internet robots – automated software that simulates human activity on social media, interact with social media users through 'likes' and comments – systematically producing manipulative messages aimed at shifting public opinion on major issues (Dahir 2018). Due to such developments, online discourse and hashtags have limited use as a measure of popular opinion or 'thermometer' of public attitudes towards a social or political issue. Thus, **inasmuch as social media platforms are celebrated for facilitating citizen engagement, they can at the same time, perpetuate existing inequalities and distort reality**.

A second challenge posed by social media relates to their 'echo chamber' effect. That is, users are stimulated to interact with others in the same ideological camp, which restricts constructive exchanges with users expressing different views. Echo chambers produce a selective reality in which one's own views are validated by similar others. Within these groups, new sets of values emerge and are shared by members, exacerbating social polarisation (Menocal 2021). Echo chambers are also conducive to the spread of fake news, misinformation and disinformation, as information flows go unchallenged within the groups (Figure 2). For women activists and women-led political movements, echo chambers can result in an inability to reach a support base outside their own bubble, preventing them from contributing to broader political change (Salzinger et al. 2022).

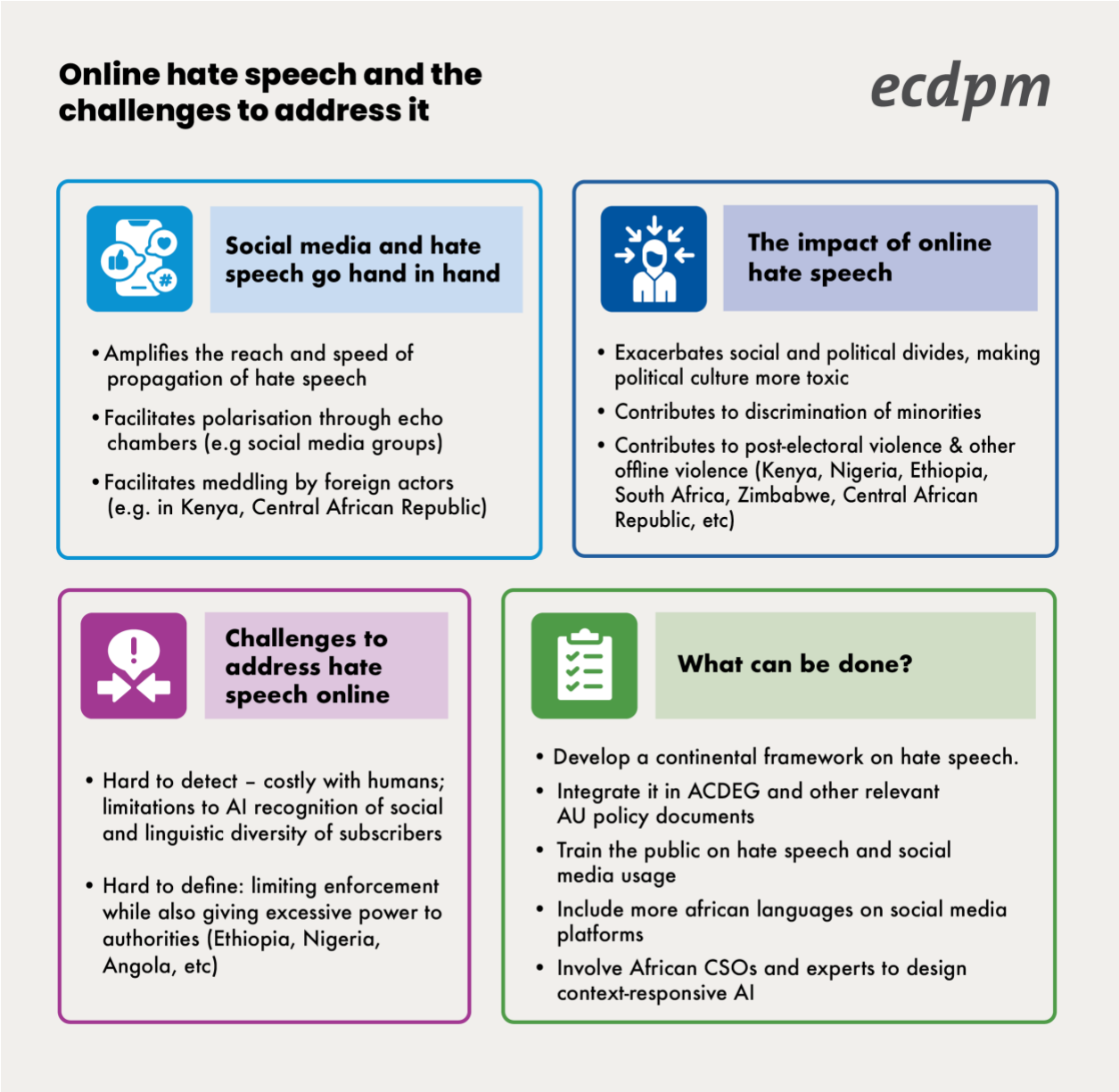
Language barriers also play a role in limiting the inclusivity of online exchanges. Google algorithms do exist in a spectrum of languages, but they cannot detect whether content written in one language is replicated by another. This hinders the ability to flag and eliminate disinformation and fake news (Southern 2022). For a more inclusive internet, in early 2022 Facebook announced plans to look into 55 African languages and improve the accuracy of its algorithms in decoding them. Twitter has taken similar steps. It reported that its team of trained reviewers, who

respond to reports of hate speech in diverse languages on the platform, filter 50% of abusive content online (Trust 2021). But overall, global social media platforms operating in Africa exhibit poor understanding of local context (Ngila 2022).

Disinformation campaigns on social media are a rising problem that has proven particularly difficult to address. State and non-state actors alike have called for development of better tools to counter the dissemination of fake news. At the beginning of the war in northern Ethiopia, the government established its own fact-checking unit SOEFactCheck with an associated Twitter account that registered more than 119 million followers. The unit, however, has been accused of attempting to dictate what information is legitimate and what not based on the government's political positioning, and of undermining local media's role in providing checks and balances. Beyond this government-led example, the rise of fact checking across Africa has been spearheaded mainly by independent media organisations through the launch of accountability projects and incubators, for example, in Nigeria, Mozambique, Zimbabwe, Congo, Ghana and South Africa (Jamlab 2020: Code for Africa 2022).

A third challenge of social media platforms is their instrumentalisation for hate speech and mobilisation of violence. This too has proven difficult to govern, for example, by holding internet service providers and social media platforms accountable. African governments and digital rights activists have accused Facebook, Twitter, Instagram and TikTok of failing to moderate hate speech inciting violent ethnic protests, thereby creating tensions between incumbent governments and the platforms. Ahead of the latest Kenyan elections, for example, the National Cohesion and Integration Commission gave Facebook a week to comply with the country's hate speech regulations. This measure followed reports that the platform had failed to detect hate speech in both English and Swahili; in this case, the platform had already taken down more than 37,000 posts violating its own internal hate speech policies (Gebre 2022). This provides an indication of the scale of the problem. Since these platforms have not managed to introduce tools to effectively moderate content, governments around the world have adopted state-centric strategies on hate speech, going as far as to regulate both information and dissent. In practice, this has meant government blockages and censorship of online content through legislation and regulation – an example is Tanzania, Nigeria and South Africa's removal of false information on COVID-19 (Accord 2017; Garbe et al. 2021). Some governments have resorted to internet shutdowns.

Figure 2: Online hate speech and challenges in addressing it



As of yet, there is no global or continental framework to address hate speech or hold for-profit social media platforms accountable. On 21 September 2021, the International Day of Peace, the AU Youth Ambassador for Peace launched the 'No Room for Hate Speech' campaign targeting young people in Africa, recognising their vulnerability. Yet, this initiative has remained largely symbolic. African governments have taken diverse approaches to address the dissemination of hate speech on social media. However, **the hate speech laws introduced seldom address the root causes of online hate speech, and they often bring even greater consequences for civil society movements, journalists and opposition leaders that criticise the government** on social media or simply share alternative information.

For instance, Tanzania's Cybercrime Act seeks to counter the dissemination of false information and content inciting genocidal, racist and xenophobic violence. Yet, the government also used the act to suspend and fine media outlets and journalists that provided alternative information on the pandemic and raised questions on the government's

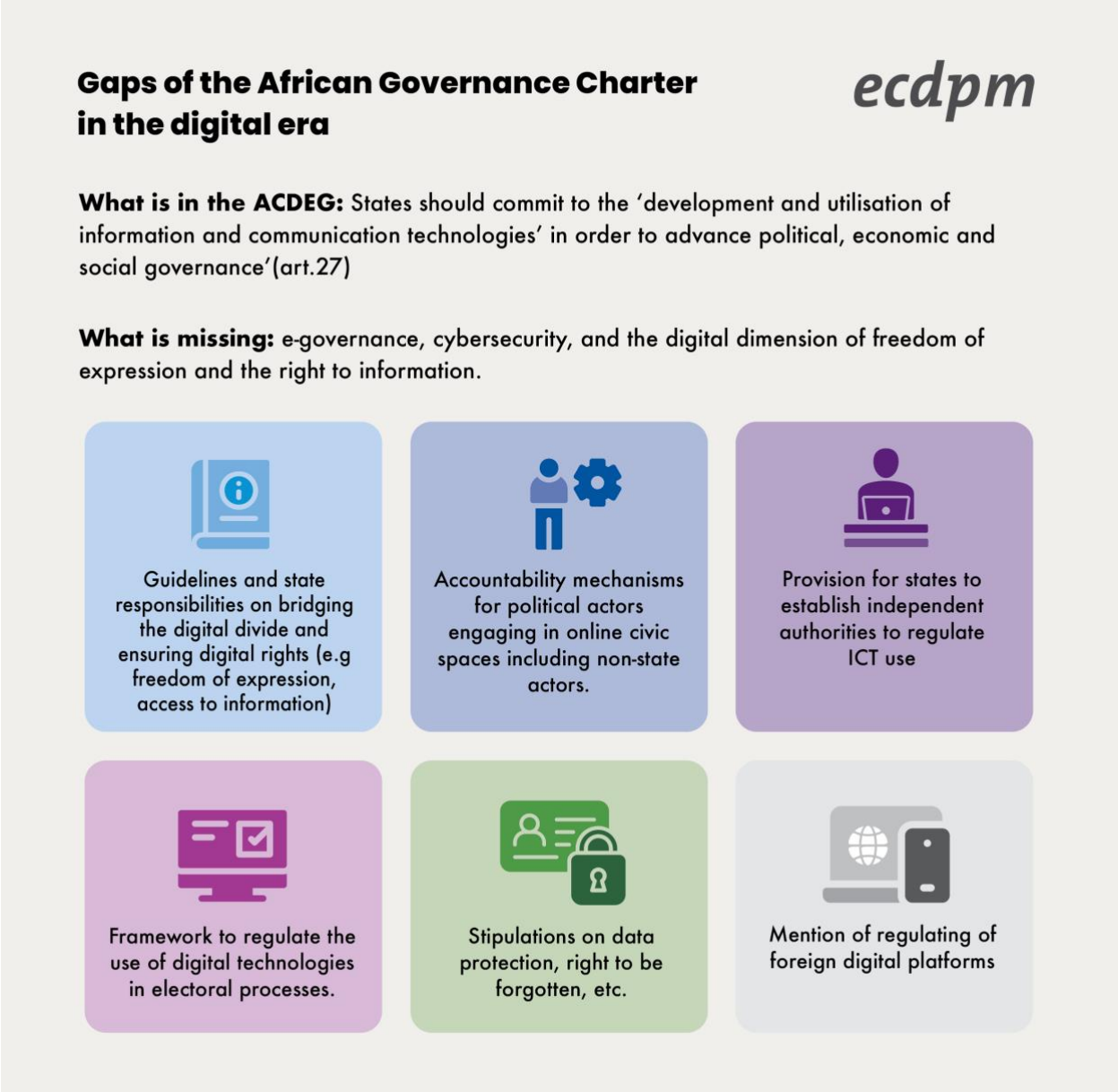
management of the crisis. In this case, the government had initially denied the existence of the pandemic and stopped providing statistics on the spread of COVID-19 (CIPESA 2020b). In Benin, the Committee to Protect Journalists expressed concern about the country's Digital Code Act, stating that the act criminalises expression online and threatens press freedom. Indeed, in 2021 two journalists were arrested under the act, after they had posted content critical of government work and officials on social media (Rozen 2021; Cheeseman and Garbe 2021). Internet shutdowns, the blocking of online media, and introduction of government-led fact-checking have breathed new life into an age-old debate on what 'free speech' means, who can exercise it, and who is responsible for regulating it (Degol and Mulugeta 2021).

With the examples above in mind, many gaps can be identified in the ACDEG in terms of information management. For instance, the ACDEG does not consider contestation between governments and non-governmental actors on what is 'accurate' information. There is an emerging trend whereby governments attempt to take a monopoly over 'truth' or information as seen above in the case of Tanzania's initial response to COVID-19 and Ethiopia's fact checking unit at the onset of the war in the north. Moreover, while social media platforms have empowered citizens and have given some individuals a great deal of influence. The ACDEG doesn't address the responsibility of individuals and non-state actors even if there is an apparent need to hold individuals and social media platforms accountable for online messaging. **The dominant influence of non-state actors, be they organised groups or international technology companies, on the practice of democracy, also remain unaddressed in the ACDEG, which emphasises instead the duties of states.**

Regarding speech and disinformation, the ACDEG's provision on civic education and creating a culture of peace (Art. 12) and its provision on the freedom of expression (Art. 27) are relevant. **Efforts to promote a culture of peace should address the potential of digital platforms to amplify polarisation and power asymmetries,** while actively harnessing the added value of the internet and digital tools to connect people and societies. By the same token, civic education in the digital age should incorporate responsible citizenship in online and offline spaces, digital literacy, and tactics of disinformation and misinformation. Moreover, to ensure active digital political participation, states should continue expanding access to electricity, the internet and digital technologies.

There are recent initiatives that can be built upon to elaborate and integrate the digital dimensions of the rights of access to information and freedom of expression. One is the 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa (ACHPR 2019). Among the principles is the guarantee of non-interference, privacy and the protection of personal information, with practical guidelines provided for states to achieve these. However, the principles do not consider states' use of economic measures, such as taxes, levies and duties, to limit access to ICT services. Building on African legal frameworks, another recent initiative is the legal guidance on internet restrictions and shutdowns published by the International Commission of Jurists.

Figure 3: Gaps in ACDEG provisions on political participation and democratic elections



4.3. Digital election monitoring

As democratic rituals, elections have become common and are periodically performed in most African countries, the exception being Eritrea, which has not conducted elections in the past three decades. While the degree of fairness, competitiveness and independence of electoral processes varies greatly, both across countries and between electoral cycles even within the same country, electoral democracy has generally become accepted as the primary and preferred way of attaining power.

Yet, challenges remain in the institutionalisation of elections and in normalisation of the AU's zero tolerance policy towards coups. Moreover, election rigging, political repression and structural crackdowns on political opponents are all too commonplace, and undermine the credibility and transparency of electoral systems and institutions. Between

2000 and 2018, 47 presidential term limits were changed in 28 countries. This tendency towards 'third termism' has been a matter of both open and closed-door dialogue at the AU and with civil society organisations (OSISA 2021). Since 2019, five Sahelian countries and Sudan experienced military coups, at times supported by the general population. This has spurred discussion of whether the comeback of military coups is evidence of a depreciation of democratic norms in Africa and also of the AU's ineffectiveness in strictly enforcing its zero tolerance policy towards coups.

The ACDEG contains a number of provisions regarding elections. One of these stipulates that states should "ensure that there is a binding code of conduct governing legally recognised political stakeholders and government and other political actors prior, during and after elections". Similarly, the AU Declaration on the Principles Governing Democratic Elections in Africa states that governments should "take all necessary measures and precautions to prevent the perpetration of fraud, rigging or any other illegal practices throughout the whole electoral process".

Since the 2002 launch of the Guidelines for African Union Election Observation and Monitoring Missions, observing elections has been a foremost task of the AU, welcomed by both member states and the AU's donors. These missions have evolved into sophisticated and well-designed operations comprising both short-term and long-term actions, depending on the electoral context. Electoral processes are also incentivised and enforced by provisions of the ACDEG and the AU's Constitutive Act, both of which reject unconstitutional changes of government, including by force. Deployment of AU election observation missions in the past decade has, overall, strengthened the transparency and credibility of elections and enhanced acceptance of election results, though AU member states have also used the observation missions as a stamp of credibility (Aniekwe and Atuobi 2016).

Digital technologies have drastically changed how elections are conducted. As already observed, politicians and political parties are going online to disseminate political information and engage with their constituencies. Many have already integrated online campaigning into their political strategy. Independent result tabulation has also become possible and easier to do, providing a basis for challenging official electoral results.

Moreover, according to the Carnegie for Endowment for International Peace, 27 African countries have adopted digital technologies to promote fair and transparent elections (Mosero 2022). Furthermore, 27 electoral management boards in Africa now rely on biometric technology to verify voter identities on election day; this too has enhanced trust in electoral processes (Mosero 2022). These technologies also come with negative spill over effects such as the exclusion of certain individuals and segments of the population (CIPESA 2022). For example, during the 2022 Kenyan elections, voters including high profile ones, were unable to cast their ballot on time because the Kenyan Integrated Election Management System (KIEMS) biometric kits could not read their fingerprints (e.g., because of the use of henna) and there were technical challenges in voter identification (Macdonald 2022).

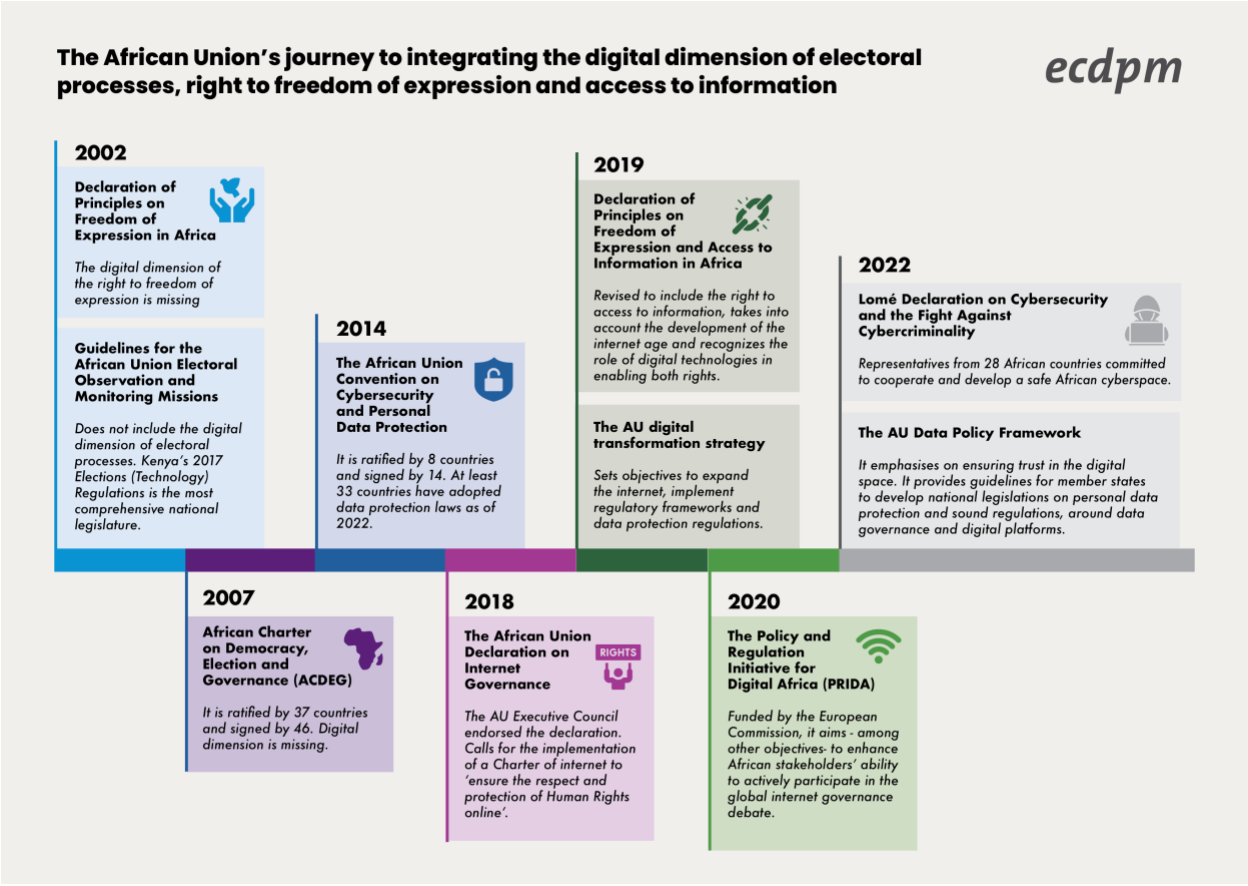
While digital technologies and online engagement have not replaced offline dynamics, they continue to drastically change all parts of the electoral process. The ACDEG, the AU election observation mission guidelines, the AU Charter on Human and Peoples' Rights, and the Declaration on the Principles Governing Democratic Elections in Africa are complementary documents that define the role of states and non-state actors and the responsibilities of each in regard to the organisation of safe and inclusive elections. None of these documents acknowledges the impact of digital technologies on democracy, electoral processes and communication between citizens and politicians. They therefore offer no solutions to the significant challenges that digital democracy presents.

The question therefore is whether election observation missions by the AU and others have been able to catch up to these changes. AU election observation missions do recognise the role of media as an actor in election processes, but they focus mainly on how international and national media cover electoral processes. Yet, as

concluded earlier, digital technologies and political engagement online has blurred the lines between private citizens, commercial influencing, journalism and political activism. Adapting to the digital era requires staff trained to monitor online electoral activities. In this regard, strengthening the AU's electoral support to member states to include guidelines on how to integrate digital technologies in election processes and how to govern them, will be essential to ensure electoral observation missions are comprehensive and fit for purpose.

African governments are using digital technologies to meet their responsibilities, yet their efforts at governing the security, integrity and inclusivity of electoral processes are rather an ad hoc basis (Obinna Ibeanu 2022; Mosero 2022). The existing tools to regulate the digital space, FinTech, and the use of digital technologies during elections are scattered across different continental and national frameworks, without a comprehensive continental strategy on digital governance (Kimumwe 2022).

Figure 4: The AU's policy frameworks relevant to digital governance, freedom of expression and access to information



5. Summary and key takeaways

This paper has examined the impact of digital technologies on democratic governance and what it means of the African Charter on Democracy, Elections and Governance (ACDEG). Section 2 discussed the empowering effects of digitalisation in promoting democratic governance and supporting states' obligations under the ACDEG. Section 3 examined barriers in the digital space to the exercise of accountable governance and upholding the provisions of the ACDEG. Section 4 explored some emerging challenges related to digital technologies and the governance agenda,

and identified blind spots of the ACDEG. This concluding section summarises the main takeaways of this analysis and recommends areas for further research.

1. Digital technologies enable citizen participation and expand states' ability to meet their obligations vis-à-vis citizens; yet the governance of digital spaces and the responsibilities of non-state actors merit further investigation.

Where internet penetration is broad and of high quality, it has enabled e-government and e-services, giving connected citizens efficient and convenient access. This positive development, however, is in most places outweighed by the digital divide within and across countries in Africa and by the risk of exclusion, whereby segments of the population go underserved. Gaps in service availability are due not only to connectivity issues, but also to technological failures and design faults. Moreover, how data gathered through the burgeoning e-services are used and by whom are questions with both ethical and economic relevance. They should therefore be high on the data governance agenda of Africa, as elsewhere in the world.

Digital technologies make a significant contribution in enabling freedom of expression, in democratising access to and flows of information, and in facilitating civil and political organisation. This is a global phenomenon, but one that is clearly evident in Africa. From the early days of the Arab Spring to the more recent popular protests in Sudan and Ethiopia, activists on the continent have relied on social media to organise in the face of closed offline civic spaces.

A key challenge here regards the growing number and types of political actors in the online space. Their increasing variety has introduced a shift in the traditional relations between states and their citizens and the respective responsibilities of each. In addition, social media's tendency towards hate speech, political manipulation, mobilisation of violence, (gendered) harassment and disinformation warrant deep and critical reflection on how best to govern the digital space and non-state actors, be they citizens, media or for-profit social media platforms like Facebook and Twitter.

The need for more adequate governance of digital spaces raises several questions, which arguably were unanticipated and hence overlooked by ACDEG:

- Who defines the contours of norms in the digital space, and who defines where the spectrum of free speech ends?
- What accountability should individuals and commercial entities bear on social media, for example, with regard to voter manipulation and monetisation of social media influence, or the discrediting of electoral systems and political opponents in a coordinated yet opaque manner?
- How can states hold international technology companies accountable for their failure to moderate content and for inappropriate use of citizen data, when international norms in these domains are not yet fully developed and most of these companies are foreign based?

At the continental level, policy frameworks relevant to data governance include the AU's 2022 Data Policy Framework, the 2019 declarations on freedom of expression and on access to information in Africa of the African Commission on Human and Peoples' Rights, and the AU's engagement on hate speech. Moreover, various African states are formulating or adapting existing policies and regulations to prevent or manage disinformation and hate speech online. Initiatives in this direction, however, need to proceed in a manner that does not undermine online civic engagement, as such regulations can easily be instrumentalised to repress dissenting narratives, censor criticism and overall limit civic and political engagement.

Adapting the ACDEG to reflect concerns raised by digitalisation may not be necessary or possible, but there is a need to systematically address the challenges identified. This entails obtaining a deeper understanding of the dynamics

between digital technologies and accountability, through empirical and qualitative studies that demonstrate contextualised linkages. It also requires a bird's eye view on the linkages between digital transformation and governance – to ensure that continental and national regulations do not dwell on specific aspects of digital governance (e.g., data governance, digital infrastructure, e-IDs and surveillance) while remaining oblivious to the bigger picture. Finally, beyond regulation, preventive mechanisms are needed, such as online civic education. These could address, for example, online extremism, online political participation, fact checking and electoral processes.

2. Although digital spaces facilitate open participation, they should not be overestimated or seen as a replacement for offline civic engagement.

Via online platforms, citizens can exercise their rights by taking part in digital discussion forums, signing online petitions and participating in hashtag campaigns. By drawing attention to political issues within these spaces, citizens can make duty bearers accountable. This resonates with the principles of the ACDEG, such as civic engagement, accountability and the oversight role of citizens vis-à-vis public institutions. Hence, these activities can be viewed as ways in which digital technologies can serve as an enabler of the realisation of the ACDEG.

Yet, online activism can turn into 'slacktivism', in which citizens limit their participation to online comments or clicks. Similarly, politicians and duty bearers may interact with citizens only on issues that happen to be trending. This would have serious consequences for the quality of civic and political engagement, as online activism can be performative, short lived (as new topics emerge) and superficial or symbolic rather than transformative and sustainable.

There are a few key takeaways from this observation.

- Experience demonstrates that online activism and social media movements are more effective if and when combined with offline engagement, such as demonstrations, policy dialogue, public exchanges and discourse, and offline advocacy for legal and policy reform.
- The development sector's often overly optimistic adoption of digital technologies as the ultimate solution to civic engagement and citizen empowerment, particularly in closed civic spaces, merits interrogation. Realism on the functioning of digital technologies in Africa is particularly pertinent, given that access to the internet and social media is highly mediated by identities, such as urban-rural residency, gender, educational background, linguistic skills and socio-economic standing. This points to the need for careful analysis of whose voice is heard and 'trending' on social media and who might be included or excluded in online discourse in a particular country context or when seeking to implement interventions focused on 'digitalisation for democracy'.
- Digitalisation for democracy or for development initiatives should include expansion of digital infrastructure and formulation of digital regulations to guarantee the rights of citizens, the protection of communities, and accountability of all stakeholders – state and non-state alike.

3. Digitalisation of elections should be matched with advanced monitoring systems that can provide oversight of both the digital and the analogue aspects of elections and guarantee their credibility, inclusivity, transparency and effectiveness.

The diverse examples cited in this analysis demonstrate that digital technologies can be valuable in boosting democracy when they are used to strengthen government service delivery and improve citizen political participation. This applies to the use of digital technologies in various aspects of elections, such as voter registration, vote casting, counting and tallying. It also applies to citizen engagement with electoral commissions, voter education and electoral processes overall, as well as the use of digital technologies in political campaigning and sensitisation.

As more countries introduce digitalisation and shift towards digital electoral processes, so too should the election monitoring missions by civil society and the AU. Up to now, these missions have been primarily designed and practised in the context of analogue, paper-and-pen electoral systems. Thus, their approaches and lines of oversight and inquiry need to be adapted to capture changes brought about by new technologies. Digital technologies cannot be introduced to electoral processes without checks and balances. As the examples have shown, digital technologies can actually undermine democracy.

Given the centrality of elections in democratic practice, they are a prominent consideration in the ACDEG. Moreover, election monitoring is one of the foremost roles of the AU Commission, and is an activity that enjoys considerable support from AU member states and donors alike. Currently, a number of continental policy documents and frameworks relevant to this role are being updated. As such, with the aim of including the use of digital technologies in elections, the AU recently undertook a technical review of its draft Electoral Assistance Guide and revised the Declaration of Principles on Freedom of Expression in Africa to include the right to information.

However, further research is needed on how election observation missions by the AU and national civil society organisations can adequately monitor the technical and more complex digitalised aspects of electoral processes. This involves a number of issues that merit further study: political advertisements in the digital space, instrumentalisation of social media platforms for voter manipulation, election-related foreign interference, and content moderation in African languages to better prevent electoral violence. It is important to understand if and how these aspects might be monitored by the AU or other bodies in a timely manner to preserve election integrity. However, any consequent reforms and adaptations should be done in addition to and in support of initiatives to promote free, fair and competitive elections in Africa and accountable governance broadly speaking.

While this paper focused on opportunities and challenges facing the African governance agenda, and the ACDEG as its main legal document, the need to revive accountable governance, enhance enforcement mechanisms and combat resurfacing challenges such as constitutional manipulation, third termism and unconstitutional changes of government cannot be overlooked. Some practitioners have advocated revision of the AU's legal provisions regarding unconstitutional changes of government and constitution manipulation. Yet, for this to be possible, (some of) the AU's member states must demonstrate a willingness to champion the cause. Notwithstanding debates on the contextualisation of the democratic agenda in Africa, as well as the instrumentalisation of models of government (democracy or autocracy) for geopolitical purposes, the recent upsurge of instances of electoral manipulation and unconstitutional changes of government, as well as often violent political crises in various regions of the continent – such as West Africa, the Sahel and the Horn of Africa – point to the need for a continent-wide conversation on the state of digital and analogue governance and the continent's sovereignty.

Bibliography

Abdulmelik, N. and Belay, T. 2019. Advancing Women's Political Rights in Africa: The Promise and Potential of ACDEG. Sage Journals. 22 December 2019.

Abimbola, O. Aggad, F. Ndzendzen, B. 2021. What is Africa's Digital Agenda?. Africa Policy Research Institute.

Aborisade, S. 2021. NIA gets N4.87bn budget to track, intercept calls, messages. Punch. 12 July 2021.

Access now. 2022. Internet shutdowns in 2021 report: resistance in the face of blackouts in Africa. 28 April 2022.

Accord. 2017. South Africa and Kenya's Legislative Measures to Prevent Hate Speech. 21 July 2017.

Achieng, G. 2022. A Ten-Point Strategy Towards Ending Technology-Facilitated Gender-Based Violence in Africa. Tony Blair Institute for Global Change. 7 March 2022.

African Commission on Human and People's Rights (ACHPR). 2019. Declaration of principles on freedom of expression and access to information in Africa. Banjul. 10 November 2019.

African Union (AU). 2019. African Union Cybersecurity Expert Group holds its first inaugural meeting.

African Union (AU). 2022a. African Union Launches Initiative to unlock USD20 billion for Financial and Economic Inclusion of African Women and Youth. 11 March 2022.

African Union (AU). 2022b. Workshop on Technical Review and Validation of the Draft AU Electoral Assistance Guide. 29 March 2022.

African Union (AU). 2022c. The African Union Deploys Election Expert Mission to Kenya. 28 June 2022.

African Union (AU). 2022d. List of countries which have signed, ratified/acceded to the African Union convention of cyber security and personal data protection. 25 March 2022.

African Union (AU). X. African Charter on Democracy, Elections and Governance. African Union.

Africanews. 2022. ECOWAS Court declares Nigeria's Twitter ban unlawful. 14 July 2022.

Africanews. 2022. Social media Influencers cash in as presidential election approaches in Kenya. 5 May 2022.

Alcorn, T. 2021. One of the World's Poorest Countries Found a Better Way to Do Stimulus. Bloomberg. 8 November 2021.

Allen, N. 2021. Africa's Evolving Cyber Threats. Africa Centre for strategic studies.

Allen, N. and Kelly C.L. 2022. Deluge of Digital Repression Threatens African Security. Africa Centre for Strategic Studies. 4 January 2022.

Aniekwe, C.C. and Atuobi, S.M. 2016. Two decades of election observation by the African Union: a review. 1 June 2016.

AUDA-NEPAD. 2022. Improving Africa's Service Delivery Through E-Governance. 21 February 2022.

BBC. 2020. How the Ends Sars protests have changed Nigeria forever. 24 October 2020.

BBC. 2020a. Hachalu Hundessa: Ethiopia singer's death unrest killed 166. 5 July 2020.

BBC. 2021. Muhammadu Buhari: Twitter deletes Nigerian leader's 'civil war' post. 2 June 2021.

Becker, C. 2021. Taxing the digital economy in sub-Saharan Africa. International Bar Association. 1 December 2021.

Bhalla, N. and McCool, A. 2021. 100 hours in the dark: How an election internet blackout hit poor Ugandans. Reuters. 20 January 2021.

Boakye, B. 2021. Social Media Futures: How to Change The African Narrative. Tony Blair Institute for Global Change. 19 April 2021.

Borkena. 2020. Egypt based hackers attempted cyber-attacks on Ethiopian government sites.

Bridget Boakye. 2021. Social Media Futures: Changing the African Narrative. Tony Blair Institute for Global Change.

Calvin-Smith, G. 2021. Niger post-election violence kills two, hundreds arrested. France 24. 25 February 2021.

Centre for Human Rights & Global Justice (CHRGJ). 2022. Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID. June 2022.

Cheeseman, N. Lynch G. and Willis, J. 2018. Digital dilemmas: the unintended consequences of election technology, Democratization. 25:8, 1397-1418. 8 June 2018.

Cheeseman, N. and Garbe, L. 2021. A collection of essays exploring the interplay between digital technologies, politics, and society across Africa. Democracy in Africa.

Cipesa. 2019. State of Internet Freedom in Africa 2019 - Mapping Trends in Government Internet Controls, 1999 - 2019. September 2019.

Cipesa. 2020b. Tanzania Tramples Digital Rights in Fight Against Covid-19. 19 October 2020.

Cipesa. 2022. The Rise of Biometric Surveillance. September 2022.

Cipesa. 2022b. Leveraging the African Union Data Policy Framework to Bolster National Data Governance Practices. 29 June 2022.

Civic Tech in Africa. 2022. Embracing Civic Technology to Amplify African Voices - Justin Arenstein. Spotify. 11 July 2022.

Code for Africa. 2021. Meet the newsrooms. Published in African Fact Checking Alliance. 28 October 2021.

Code for Africa. 2022. Combattre la Més/Désinfo en Afrique francophone! 4 October 2022.

Committee to Protect Journalists (CPJ). 2021. Number of journalists behind bars reaches global high. 9 December 2021.

Dadoo, S. 2022. Israel's Spyware Diplomacy in Africa. Orient XXI. 12 September 2022.

Dahir, A.L. 2018. How social media bots became an influential force in Africa's elections. Quartz Africa. 18 July 2018.

Debre, I. 2019. Israeli disinformation campaign targeted Nigerian election. AP News. 17 May 2019.

Degol, A. and Mulugeta, B. 2021. Freedom of Expression and Hate Speech in Ethiopia: Observations. AJOL. 30 September 2021.

Diaz Hernandez, M. and Anthonio, F. 2022. The return of digital authoritarianism - Internet shutdowns in 2021. Access now. April 2022.

Digwatch. 2021. Uganda Government to impose 12% tax on all internet packages. 5 May 2021.

Domingo, E. and Tadesse, L. 2022. The African Union at twenty: A new leader in digital innovation? ECDPM commentary. 4 July 2022.

Domingo, E. and Teevan, C. 2022. Africa's journey towards an integrated digital payments landscape and how the EU can support it. ECDPM brief. 23 May 2022.

Elmi, N. 2020. Is Big Tech Setting Africa Back? ForeignPolicy.com. 11 November 2020.

Eltahir, N., Tapper, M. and Abdelaziz, K. 2021. Facebook shuts fake accounts in Sudan, as fight for public opinion rages online. Reuters. 19 October 2021.

Eneyew, Y. 2022. Data Protection Policy Brief for Ethiopia. CARD. 11 October 2022.

Engel, U. 2019. The 2007 African Charter on Democracy, Elections and Governance: Trying to Make Sense of the Late Ratification of the African Charter and Non-Implementation of Its Compliance Mechanism. Sage Journals. 22 December 2019.

Ferebee, B. and Sullivan, R. 2021. Beyond Fake News: the Central African Republic's Hate Speech Problem. United States Institute Of Peace (USIP). 16 August 2021.

Fintech Global. 2022. FinTech investment in Africa nearly quadrupled in 2021, driven by PayTech and Lending deals. 19 January 2022.

Freedom House. 2022. Freedom on the net 2022 - Zimbabwe.

Galal, A. 2022a. Market share of social media platforms in Africa from January 2021 to May 2022, by platform. Statista. 24 June 2022.

Galal, A. 2022b. Social media penetration in Africa in 2022, by region. Statista. 22 August 2022.

Garbe, L., Selvik, L-M. and Lemaire P. 2021. How African countries respond to fake news and hate speech. Taylor & Francis online. 9 November 2021.

Gebre, S. 2022. Social Media Platforms Under Scrutiny Ahead of Kenyan Elections. Bloomberg. 30 July 2022.

Goltermann, L. 2016. Unequal Empowerment; African Civil Society in the Digital Age. Humanity in Action. October 2016.

Harsono, H. 2020. China's Surveillance Technology Is Keeping Tabs on Populations Around the World. The Diplomat. 18 June 2020.

Human Rights Watch (HRW). 2020a. Cameroon: Election Violence in Anglophone Regions. 12 February 2020.

Human Rights Watch (HRW). 2020b. Guinea: Post-Election Violence, Repression. 19 November 2020.

IAB. 2021. Study finds internet economy grew seven times faster than total U.S. economy, created over 7 million jobs in the last four years. 18 October 2021.

IADB. 2018. Exponential disruption in the digital economy. III CEO Summit of the Americas Peru 2018.

IEBC. 2017. Kenya Gazette Supplement no. 61 - Legislative Supplement no. 27 - Legal notice no. 68. 21 April 2017.

IFC. 2020. New Google-IFC report estimates Africa's Internet economy could be worth $180 billion by 2025. 11 November 2020.

Ilo, U.J. and Osori, A. 2021. Covid-19 Disruptions and use of Technology in Elections: Lessons for Africa. Open Society Initiative for West Africa.

Institute of Development Studies (IDS). 2021. Digital Rights in Closing Civic Space: Lessons from Ten African Countries. 26 February 2021.

ITU. 2021. Measuring digital development - Facts and figures 2021.

Jamlab. 2020. Fact-checking in Africa. 21 May 2020.

Jili, B. 2020. The Spread of Surveillance Technology in Africa Stirs Security Concerns. Africa Center for Strategic Studies. 11 December 2020.

K'onyango, O. 2022. Use of technology improved Kenya electoral transparency: Carter Centre. The East African. 9 September 2022.

Kafeero, S. 2021. To control speech, Uganda is taxing internet usage by 30%. Quartz Africa. 3 July 2021.

Kapiyo, V. 2022. Bridging the Gender Digital Divide is Critical for Achieving Digital Rights in Africa. CIPESA. 30 June 2022.

Karombo, T. 2020. Tanzania has blocked social media, bulk SMS as its election polls open. Quartz Africa.

Karombo, T. 2022. "It's a lazy tax": Why African governments' obsession with mobile money could backfire. Rest of World. 7 January 2022.

Kataneksza, J. 2018. Zimbabwean Twitter is shifting politics. Africa is a country. 10 November 2018.

Kimumwe, P. 2022. Digital Authoritarianism hurting Democratic Participation in Africa. CIPESA. 23 June 2022.

Kodjani, D. 2021. NSO Group's Pegasus Spyware Use: Six African Governments Named. Afroware.

Kramer, L. 2022a. Internet penetration rate Africa 2021, compared to the global rate. Statista. 1 August 2022.

Kramer, L. 2022b. Internet penetration rate Africa 2022, by region. Statista. 1 August 2022.

Lardies, C.A., Dryding, D. and Logan, C. 2019. Gains and gaps - Perceptions and experiences of gender in Africa. Afrobarometer Policy Paper no. 61. November 2019.

Lemma, A., Mendez-Parra, M. and Naliaka, L. 2022. The AfCFTA: unlocking the potential of the digital economy in Africa. ODI. July 2022.

Leyva, B. and Leipzig, D.S. 2022. Africa's Innovation – July Developments Signal Attention Must Be Paid to Data Privacy Developments in Africa. Mayer Brown. 5 August 2022.

Lodewijckx, I. 2020. 'Slacktivism': Legitimate Action or Just Lazy Liking? Citizenlab. 20 May 2020.

Logan, C. and Penar, P. 2019. Are Africans' freedoms slipping away? Afrobarometer Policy paper no. 55. April 2019.

MacDonald, A. 2020. Ghana procures 75k biometric voter verification devices ahead of elections. Biometric Update. 9 November 2020.

MacDonald, A. 2022. Voters face biometric verification kit glitches in Kenya elections, failures 'not widespread'. Biometric Update. 10 August 2022.

Masuku, J. 2021. A Brutal Lesson From Zambian Politics: No Internet, No Votes. Medium.com. 24 September 2021.

Menocal, A.R. 2021. Digital technologies and the new public square: revitalising democracy? DIA. 23 February 2021.

Meseret Assefa, A. 2020. *Role of social media in Ethiopia's recent political transition*. Journal of Media and Communication Studies. Research paper. April-June 2020.

Minority Rights Group. 2020. Recent violence in Ethiopia's Oromia region shows hallmark signs of ethnic cleansing, says MRG. 22 July 2020.

Mosero, R. 2022. In Kenya's 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand. Carnegie. 8 August 2022.

Mungadze, S. 2020. Life Healthcare Group hit by cyber attack amid COVID-19. Itweb.

Mutung'u, G. and Biddle, E.R. 2017. Did Fake News Save Kenya from an Internet Shutdown? Emerging Trends in Tech and Elections in Africa. Berkman Klein Centre. 4 October 2017.

Mwakideu, C. 2021. Can Africa achieve universal internet access by 2030? Deutsche Welle. 5 November 2021.

Nackerdien, R. 2021. Voting in a pandemic: Lessons for elections in Africa in 2021. Brookings. 1 February 2021.

Ndelela, M. 2022. Algorithms, bots and elections in Africa: how social media influences political choices. The Conversation. 30 March 2022.

Ndung'u, N. 2017. M-Pesa - a success story of digital financial inclusion. Practitioner's insight. July 2017.

Ngila, F. 2022. Meta's AI can now translate more African languages, helping create a more inclusive internet. Quartz Africa. 15 July 2022.

Nyabola, N. 2019. Platform Governance of Political Speech. Cigi. 28 October 2019.

Nyabola, N. 2020. Governance and Public Policy in the Digital Age. DIA. 9 October 2020.

Nyambura, H. 2021. Nigeria Lifts Twitter Ban With Limits After Four-Month Sanction. Bloomberg. 1 October 2021.

Obinna Ibeanu, O. 2022. Digital Technologies and Election Management in Africa's Democratisation Process. In Africa Development / Afrique et Développement. Vol. 47, No. 2, Special Issue (2022), pp. 15-40 (26 pages). CODESRIA.

Onminyi, E. 2020. Chief Justice Of Nigeria Tests Positive For COVID-19, Flown Abroad For Treatment. The Gistday. 15 December 2020.

Osisa. 2021. Presidential term limits in Africa: what should be done? 9 February 2021.

Privacy International. 2022. Letter from global CSOs to the World Bank. 6 September 2022.

Ro, C. 2019. Chad Smashes The Record For Social Media Censorship. Forbes. 3 May 2019.

Roberts, T. 2021. Digital rights in closing civic space: lessons from ten African countries. Institute of development studies.

Roberts, T., Ali, A.M., Farahat, M., Oloyede, R. and Mutung'u G. 2021. Surveillance Law in Africa: a review of six countries. Institute of development studies. October 2021.

Ronceray, M. and Tadesse, L. 2022. A guide to the African Charter on Democracy, Elections and Governance. ECDPM guide. 28 February 2022.

Rozen, J. 2021. In Benin, growing fears over law that can jail journalists for posting news online. CPJ. 8 December 2021.

Salzinger, M., Tadesse, L. and Ronceray, M. 2022. From hashtags to the streets: Digital technologies for women's political activism. ECDPM discussion paper 326. June 2022.

Sambuli, N. 2022. Africa is a strategic techno-geopolitical theatre. Will the continent's leaders take advantage of this? APRI. 9 June 2022.

Southern, M. 2022. Google Uses Different Algorithms For Different Languages. Search engine journal. 20 January 2022.

Stubbs, J. 2020. French and Russian trolls wrestle for influence in Africa, Facebook says. Reuters. 15 December 2020.

Teevan, C. and Tadesse Shiferaw, L. 2022. Digital geopolitics in Africa: Moving from strategy to action. ECDPM briefing note 150. 10 October 2022.

Tekle, T. 2020. Month-long internet shutdown cost Ethiopia over $100m: NetBlocks. The EastAfrican. 27 July 2020.

Teshome, M. 2021. First structured personal data protection proclamation in the making. Capital Ethiopia. 28 September 2021.

The Conversation. 2021. Surveillance laws are failing to protect privacy rights: what we found in six African countries. 21 October 2021.

UN Women. 2021. Addressing the digital gender divide in Africa through the African Girls Can Code Initiative. 8 October 2021.

UNESCO. 2021. UNESCO Supporting Countering Disinformation and Disinfodemic in Ethiopia. 26 September 2021.

United Nations (UN). 2022. Activists: Internet shutdowns violate human rights. 19 August 2022.

Uwazuruike, A. 2021. #EndSARS: An Evaluation of Successes and Failures One Year Later. Georgetown Journal of International Affairs. 13 December 2021.

Vanguard. 2020. Five demands from #EndSARS protesters. 12 October 2020.

Vanguard. 2021. Redirect N4.8bn to monitor WhatsApp calls to pay doctors' salaries, SERAP tells Buhari. 15 August 2021.

Wanyama, E. 2020. Analysis of Ethiopia's Hate Speech and Disinformation Prevention and Suppression Proclamation. Cipesa. No. 11 85/2020. July 2020.

Wiebusch, M., Aniekwe, C.C., Oette, L. and Vandeginste, S. 2019. The African Charter on Democracy, Elections and Governance: Past, Present and Future. Cambridge University Press. 14 May 2019.

Wodajo, K. 2022. Digitalizing Identity: Precautionary Thoughts on Ethiopia's "Fayda" Number. OpinioJuris. 10 February 2022.

Wolf, P. 2017. Introducing BiometricTechnology in Elections. IDEA.

World Bank (WB). 2021a. Prioritizing the poorest and most vulnerable in West Africa: Togo's Novissi platform for social protection uses machine learning, geospatial analytics, and mobile phone metadata for the pandemic response. Results Briefs. 13 April 2021.

World Bank (WB). 2021b. Prioritizing the poorest and most vulnerable in West Africa. 8 July 2021.

World Bank (WB). 2022. Digital development - overview. 20 April 2022.

World Economic Forum (WEF). 2022. Tech start-ups key to Africa's digital transformation but urgently need investment. 20 January 2022.

Xinhau. 2021. China Focus: China spurs digital economy as new driver of growth. Xinhuanet. 4 August 2021.

Zimeye. 2018. Mnangagwa Unleashes Social Media Cyber “Attack Dogs” Against Opponents. 9 March 2018.

About ECDPM

ECDPM is an independent 'think and do tank' working on international cooperation and development policy in Europe and Africa.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

In addition to structural support by ECDPM's institutional partners: Austria, Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, The Netherlands and Sweden, this publication also benefits from a contribution by the European Union for the Charter Project Africa.

ISSN1571-7577

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Avenue des Arts 44, 1000
Brussels *Bruxelles*
Belgium *Belgique*
Tel +32 (0)28 825 008

info@ecdpm.org
www.ecdpm.org
KvK 41077447