Lock-out, lock-in, and networked sovereignty. Resistance and experimentation in Africa's trajectory towards AI

Lock-out, lock-in e soberania em rede. Resistência e experimentação na trajetória da África rumo à IA

Iginio Gagliardone [a, *]

ABSTRACT: The conception of digital sovereignty has been associated, especially in the early stages of the diffusion of the Internet, with efforts to keep specific data and information outside of a state's jurisdiction. AI sovereignty responds to an almost opposite logic, indicating the ability of a state to access and make use of data that are produced within its jurisdiction. These two strategies – which I refer to as *lock-out* and *lock-in* sovereignty – share some common roots (e.g. the attempt to protect and enhance specific cultural attributes recognised as important by a national community), but they also point to different technical, economic, and political characteristics needed to enforce one or the other type of sovereignty. The article examines key elements that set these concepts, and their implementation, apart and how they intersect with both existing and potential articulations of national sovereignty in Africa. In particular it opposes a negative – and still pervasive – definition of sovereignty applied to African states, based on the Westphalian ideal and "measuring the gap between what Africa is and what we are told it ought to be" (Mbembe 2019, p. 26); and the possibilities disclosed by re-appropriating practices of "networked sovereignty" (Mbembe, 2016).

Keywords: Africa; Politics of AI; Digital Sovereignty; Labour and AI.

RESUMO: A concepção de soberania digital foi associada, especialmente nas fases iniciais da difusão da Internet, a esforços para manter certos dados e informações fora da jurisdição de um Estado. A soberania de IA, entretanto, responde a uma lógica quase oposta, no sentido da capacidade de um Estado de acessar e utilizar dados produzidos dentro da sua jurisdição. Essas duas estratégias – que chamo soberania de *lock-out* e *lock-in*– partilham algumas raízes (por exemplo, a tentativa de proteger e melhorar atributos culturais específicos reconhecidos como importantes por uma comunidade nacional). Porém, elas também apontam para diferentes aspectos técnicos, econômicos e políticos necessários para que um ou outro tipo de soberania possam ser atingidos. O presente artigo examina os principais elementos que diferenciam esses conceitos e a sua implementação, além da maneira como eles se conectam com as articulações - tanto existentes quanto potenciais - da soberania nacional na África. Em particular, o artigo opõe-se a uma definição negativa – e ainda influente – de soberania aplicada aos Estados africanos, baseada no ideal de Vestefália e "medindo a lacuna entre o que África é e o que nos dizem que deveria ser" (Mbembe 2019, p. 26); e as possibilidades reveladas pela reapropriação de práticas de "soberania em rede" (Mbembe, 2016).

Palavras-chave: África; Política de IA; Soberania Digital; Trabalho e IA.

[a] *University of the Witwatersrand, Johannesburg, South Africa.*
[*] Correspondência para/*Correspondence to* Iginio Gagliardone . E-mail: iginio.gagliardone@wits.ac.za

Recebido em/*Received*: 16/10/2024; Aprovado em/*Approved*: 11/12/2024.

https://doi.org/10.18617/liinc.v20i2.7319

INTRODUCTION

In 2018 the swearing into office of two African leaders made global headlines bringing hope of a renewed African renaissance and turn towards more technocratic politics. In South Africa, Cyril Ramaphosa – the African National Congress (ANC)'s chief negotiator in the talks that ended Apartheid and Nelson Mandela's preferred heir (Foster 2012; Mkokeli, Cohen 2018) – ended almost a decade of Jacob Zuma's corrupt tenure. In Ethiopia, Abiy Ahmed became Africa's youngest head of government and the first Oromo (the country's largest, yet historically marginalized group) to reach the highest office (Dahir 2018). Both leaders sought to break with their predecessors, presenting themselves as agents of change and prosperity. They both seized digital development and advancements in Artificial Intelligence (AI) as central to their strategies of transformation. How they did it, however, illustrates just how differently AI is being understood, defined, and used in state and nation building projects in Africa. Ramaphosa made the Fourth Industrial Revolution (4IR) a pillar of his national economic strategy, attracting the vast majority of Western investments in AI in the continent (AI Media Group 2022), but also receiving criticism for his neoliberal rhetoric, echoing the World Economic Forum (WEF) (Sutherland 2020). The Ethiopian government's investments in AI, on the contrary, have placed the need to strengthen and safeguard national interests at their centre, following China's commitment towards embracing innovation while guaranteeing the government's tight grip on its direction.

These trajectories appear to place South Africa and Ethiopia in two separate camps of what many have started to refer to as the Digital Cold War led by the US and China (Alden 2022; Champion 2019; Woo 2020). But this overarching narrative of a Digital Cold War conceals a significantly more complex picture of how different ideas and materialities related to AI interact. For example, how AI-powered surveillance in (democratic) South Africa's largest cities is supported by facial recognition algorithms developed by Huawei and scaled up through reliance on affordable cameras manufactured by Hikvision, both Chinese companies (Kwet 2020). Or how (autocratic) Ethiopia's flagship private ventures in AI – iCog Labs and Gebeya – are developed in collaboration with leading AI researchers in the US or EU-based diaspora.

Defying old tropes framing Africa in terms of what it lacks and needs to acquire to avoid being left behind, the article seeks to account for forms of appropriation and contestation of AI emerging in the continent, in ways that can inform distinctive trajectories towards AI sovereignty. It does so in three steps. First, it examines what makes the conceptualisation and implementation of AI sovereignty distinct from digital sovereignty. Second, it explores two different cases of sovereignty claims made by individuals and governments in Kenya and South Africa – one detailing the challenge brought by AI annotators and content moderators in Kenya to Big Tech, including Meta and Open AI; the other charting the evolution of South Africa's Policy on Data and Cloud. Third, building on the work of Achille Mbembe (2019; 2020; 2017), as well as on the arguments presented in the previous two sections, it explores opportunities to experiment with new forms of AI networked sovereignty. From a methodological standpoint, the article relies on documentary analysis – of the case brought by gig workers to Meta and the judgments of Kenya's courts; and of the various versions of the Data and Cloud policy in South Africa, including the responses received after the publishing of the draft policy – as well as on interviews with policy makers, lawyers, technocrats, and members of the civil society who have played distinct roles in each of the two cases analysed.

DIGITAL SOVEREIGNTY ≠ AI-SOVEREIGNTY

Debates focusing specifically on AI-sovereignty, being recent and tackling a complex phenomenon, have inevitably looked at longer-term trends in search of frameworks to explain current events and imagine potential future scenarios. This has almost invariably led to locating AI-sovereignty in the older, but still contested, history of digital sovereignty. This association may appear obvious at first.

Scholarly production on digital sovereignty has reached a certain level of maturity, combining normative (Segurado, Lima, Ameni 2014; Daly, Thomas 2017), infrastructural (Mueller 2010; Musiani 2022), and geopolitical (Fischer 2022; Erie, Streinz 2021) angles to examine its qualities and possible repercussions. It is offering tools to examine digital sovereignty both as practical endeavour, requiring incorporating specific requests into artefacts to control data flows (DeNardis 2009; Mueller 2010) and a discursive construction, variably embraced by authoritarian states and liberal democracies in support of distinctive projects – from autocratic leaders lamenting the interference of Big Tech into national politics (De Gregorio, Stremlau 2020) to the European Union's defence of supposedly shared European values (Braun, Hummel 2023).

To bring clarity into an expanding debate, and account for the unique sets of actors and forces weakening or hardening borders in the digital space, Julia Pohle and Thiel Thorsten have suggested a simple but effective heuristic framework that systematises "digital sovereignty claims by distinguishing whether they address the capacity for digital self-determination by states, companies or individuals" (2021, p. 8).

States are the most obvious actors in the process of renationalisation of digital spaces, seeking to enforce their authority over digital infrastructures and content, in the name of better security, alignment to cultural values, or protection of citizens. Their gains, together with the encroachment of commercial logics onto online interactions (see below), have led to the progressive fading of the ideal of the Internet as a borderless cyberspace, epitomised by John Perry Barlow's fierce challenge to national governments – "I ask you of the past to leave us alone. You are not welcome among us. You have no *sovereignty* where we gather" (Barlow 1996, emphasis added). The project of renationalising cyberspace, once believed at odd with the very nature of the protocols on which the Internet was based (Elmer-Dewitt 1993), has proven more rapid and successful than expected. In the end, most users, including those already online in 1996 when Barlow published his *Declaration of Independence of*

Cyberspace, have spent more years using a version of the Internet incorporating national restrictions and choke-points than in the promised unbounded virtual world imagined by some of the early theorists of the information society, such as Pierre Lévy (1995) or Manuel Castells (1996).

Pohle and Thorsten's second category of digital sovereignty claims – economic autonomy and competition – refers to the ability of domestic players to emerge and contribute to a flourishing national economy in a protected environment. This category, however, acquires its full significance when interpreted negatively, rather than positively, in relation to the dominance of foreign technology and service providers from the US, and increasingly from China in some of the most critical areas of digital economies and societies. In this reading, the overwhelming power concentrated in the hands of few tech giants becomes a threat not only to smaller companies in domestic markets unable to compete with foreign rivals, but also to governments' own ability to exercise their stated functions. "Platforms are weakening states in their regalian domain. They provide a number of essential services that would have been offered under the initiative or at least supervision of governments in the past, while states have become both dependent on and in competition with them" (Grumbach, Zanin 2023, p. 949)

Finally, claims to individual self-determination assert the potential for users, consumers, and employees to "take actions and decisions in a conscious, deliberate, and independent manner" (Pohle, Thiel 2021, p. 58). The emergence of "digitally sovereign subjects" (Dammann, Winkler 2023) is only a faint image of the rise of a virtual class – free to experiment with new modes of being irrespective of their "offline" identities, ties, obligations – imagined in the 1990s. It can still suggest, at least, possibilities for individuals and coalitions to challenge the narratives and unequal power relations generated by dominant state and corporate actors. Digitally sovereign subjects can be thought of as users who, for example, are aware of the extractivism powering up services and applications presented as benevolent supports of everyday life and operations (Chagnon, Durante, Gills, Hagolani-Albov, Hokkanen, Kangasluoma, Konttinen, Kröger, LaFleur, Ollinaho, Vuola 2022; Crawford 2021). Or as gig workers defying the narratives of entrepreneurship, independence, and dignified work articulated by tech giants and data-labelling companies and revealing the exploitative nature of human labour sustaining digital platforms. The apparently unsurmountable challenge in this latter conceptualisation of sovereignty claims, however, is transforming individual tactics seeking to denounce or route around the most dubious practices, services, and applications into broader strategies that can influence trajectories of innovation.

These frameworks, together with richer empirical investigations of how digital sovereignty has emerged in different national and regional contexts (Chander, Sun 2023; Glasze, Cattaruzza, Douzet, Dammann, Bertran, Bômont, Braun, Danet, Desforges, Géry, Grumbach, Hummel, Limonier, Münßinger, Nicolai, Pétiniaud, Winkler, Zanin 2023; Gagliardone 2019) have helped mapping and understanding the material and discursive forces at work in re-aligning national and digital borders. But can the conceptual and methodological tools created to examine digital sovereignty be equally applied to AI sovereignty? My answer is: yes and no.

The motivations for answering "yes" reside in the types of actors involved in negotiating power and influence over the shaping of the new technology. Large tech companies that, after having secured dominance in key areas of the digital ecosystem (from e-commerce – Amazon and Alibaba – to search – Alphabet/Google and Bing – from social networking – Meta and Tencent – to digital infrastructures – Huawei) have amassed capital and expertise to compete in the most advanced segments of the AI ecosystem (from cloud computing and data centres to the training of Large Language Models), trumping or acquiring smaller competitors. National governments or regional institutions that, after having been found unprepared by the diffusion of the global Internet (Mueller 2010) and having had to incessantly react to regulate and seek to control digital innovation and its outcomes, are now scrambling to understand the distinctive qualities and repercussions of AI, aiming to play a more proactive role in its development.

The reasons for answering "no", however, are possibly deeper and more indicative of key transformations that, while not introduced by AI, have been exacerbated by it. They relate to drastic changes in "geopolitics of data flows" (Glasze, Douzet, Dammann, Cattaruzza 2023). While the conception of digital sovereignty has been associated, especially in the early stages of the diffusion of the Internet, with efforts to keep specific data and information outside of a state's jurisdiction, AI sovereignty responds to an almost opposite logic, indicating the ability of a state to access and make use of data that are produced within its jurisdiction. These two strategies – which I refer to as *lock-out* and *lock-in* sovereignty – share some common roots (e.g. the attempt to protect and enhance specific cultural attributes recognised as important by a national community), but they also point to different technical, economic, and political characteristics needed to enforce one or the other type of sovereignty. I discuss them in turn to highlight their similarities and differences.

Lock-out sovereignty. This is possibly the most familiar type of sovereignty, associated with concepts of censorship, protection from external threats, and symbolised by common images of "walled gardens" and "firewalls". The evolution of this type of sovereignty, going from ensuring citizens within a specific territory could not access external content perceived by rulers as destabilising, to strengthening and legitimising practices of censorship of users operating within a country's borders have been well documented in the *Access* trilogy published by Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (2008; 2010; 2011). The technical means required to ensure this type of sovereignty are now in reach to even the most resource strapped governments, and it could be considered a battle of the past if it was not for the complexities later introduced by social networking platforms. Because of their nature of widely popular services used by large portions of the population but owned by private companies and regulated according to their own terms of service, the control and regulation of the content allowed on these platforms has been out of reach for most governments, especially those in countries whose markets account for a very small portion of the companies' revenues. If institutions such as the European Union have progressively developed a strong negotiating power with tech giants, requests from governments or individuals in the majority of countries in the Global South to remove content considered for example hateful or derogatory still tend to be met with inaction and silence (De Gregorio, Stremlau 2020; Paul, Milmo 2021).

Lock-in sovereignty. This, more recent, category of sovereignty claims is related not to what should be kept out of a country's borders but to what should be kept in, or more precisely, to who should have access to and make use of the data that are produced within a specific jurisdiction. Interests in the localisation and accessibility of data predate the hype that followed the popularisation of generative AI chatbots and are rooted in a combination of economic and cultural factors. On the one hand, the increasing awareness of the value that can be derived from accessing large amount of data, and the anger towards tech giants' extractive practices, syphoning data away from the communities where it is produced while preventing the same communities from accessing it in pursuit of their own goals. On the other hand, the aspiration by national and supra-national institutions to inscribe rights and values considered fundamental in their jurisdictions in the mechanisms guiding how public and personal data are handled and utilised.

The strategic importance of generative AI and the exponential proliferation of its applications have given an all new meaning to these claims of sovereignty over data. "Insofar as AI tools depend on large and representative data sets, countries with access to large data sets will be better situated than countries without such access" (Woods 2023, p. 131). If we enlarge the focus from the data layer (e.g. the possibility of accessing vast pools of data to train Large Language Models) to the entire "technology stack and (emerging) ecosystem" (Van Der Vlist, Helmond, Ferrari 2024) on which AI systems rely – including energy-hungry data centres, vast computational power, and proprietary software – the possibilities for countries other than the two AI-superpowers (Lee 2018), the US and China, to assert an independent role in shaping frontier AI applications are practically null.

Access to training data, however, can make a major difference in projects building on top of open-source large language models, in developing bespoke AI solutions, or in creating smaller models tailored to respond to specific tasks. It can allow generating solutions that are better aligned with a country's needs and values, as well as reducing intentional or unintentional forms of influence depending on the reliance on models developed in foreign contexts. An example can help clarifying this aspect.

In April 2024, Taiwan's National Science and Technology Council released the Trustworthy AI Dialogue Engine, or Taide, a LLM relying on Meta's Llama and trained on domestic data, with the majority of parameters consisting of news publications and publicly available government reports. Taide's goal is not just offering outputs that can better align with Taiwanese language patterns and colloquialism. Most critically, Taide is meant at preventing or reducing the political and cultural influence China can exercise on Taiwanese citizens through its own chatbots, especially on hot issues such as the island's independence (Bone 2024). In fact, as Jennifer Creery (2024) reported, when asked who won the 2024 presidential election in Taiwan, Baidu's Ernie Bot first accurately answered "Lai Ching-te", but then added "No matter how the situation in Taiwan changes, the basic fact is that there's only one China".

While Taiwan's case may have few equals across the world, a more generalisable point it raises is the importance of a focused understanding of the goals that can be achieved through accessing specific types of training data and specific technologies. As also stressed in case of South Africa's Data and Cloud Policy discussed below, simply accessing vast amounts of data with a generic hope to be able to extract monetary value from them – just because this is what tech giants do – rather than a strategic understanding of how data can be put to work and towards which objectives, may lead to modest outcomes.

DISTINCTIVE ASSERTIONS OF DIGITAL SOVEREIGNTY IN AFRICA

Similarly to other attributes of African states, sovereignty has tended to be defined in negative terms, "measuring the gap between what Africa is and what we are told it ought to be" (Mbembe 2019, p. 26). Robert Jackson (in)famously explained African sovereignty as part of a framework that opposes real states and positive sovereignty in the Global North and quasi-states and negative sovereignty in the Global South (Jackson 1990; 1986). As Navnita Chadha Behera lamented, this meant erasing pre-colonial pasts and extending the gaze of the West's civilising mission: "the quasi-states in Africa are characterised by a *lack* – an 'absence' of political community, 'lack' of national capability, backwardness and a 'soft' state, characterised by corruption and disorder" (Behera 2020, p. 154). The global diffusion of digital technologies has either reinforced this pathologisation, through indexes and statistics stressing the lack of skills, infrastructure, or adequate policies, or has informed hyped narratives presenting the latest innovations as finally able to address Africa's seemingly intractable development and humanitarian challenges.

The two cases analysed below – one detailing the challenge brought by gig workers in Kenya to Meta, the other the evolution of South Africa's Policy on Data and Cloud – illustrate different forms of contestation of these prevailing narratives. They are indicative of a new conjuncture in Africa's digital transformation, questioning promises of benevolent connectedness and entrepreneurship made by Big Tech and advancing new narratives that seek to inform distinct paths of digital innovation.

ASSERTING AFRICAN WORKERS' DIGITAL RIGHTS

Despite the pledges to act ethically and fairly, the maximization of profits pursued by Big Tech has encouraged companies like Meta, OpenAI or TikTok to exploit imbalances of power and rights in the international division of digital labour. Data workers contracted in the Global South not only receive lower wages than their counterparts in North America or Europe, they also have fewer protections, and their remoteness contributes to the process of invisibilisation engineered to anonymise workers, and conceal the contribution of their work from users' experiences (Gray, Suri 2019). As Muldoon and Wu (2023) stressed, the work required in the training of large language models such as Chat GPT follows a colonial supply chain, reinforcing the legacies of historical colonialism and existing power imbalances. As they point out, "the work is structured in a way to render invisible the contributions of workers in the majority world from the public imaginary of AI's production, preferencing the so-called highly skilled work of engineers" (Muldoon, Wu 2023, p. 13).

For a long time, this unequal distribution of labour, benefits, and responsibilities has gone unchallenged, couched in powerful narratives celebrating disruptive innovation; considered an inevitable feature of global capitalism; or justified through the creation of new practices and concepts such as "impact sourcing". Impact sourcing emerged in the late 2000s in opposition to traditional forms of aid, as a type of outsourcing seeking to give dignified work to the poorest, in ways that can guarantee them a living wage and possibly benefit their immediate communities (Janah 2017). The US company Sama (known until 2021 as Samasource) has pioneered this practice, presenting itself as an 'ethical AI' company, and winning large contracts from companies like Google, Walmart, Microsoft and eBay for data cleaning, annotation, and verification. As they claimed, "Sama is driving an ethical AI supply chain that meaningfully improves employment and income outcomes for those with the greatest barriers to work" (Sama 2023, as cited in Muldoon et al., 2023, p. 2).

This narrative of transformative and compassionate transfer of value was severely questioned, however, when a South African employee of Sama's office in Nairobi, Daniel Motaung, begun revealing the exploitative working conditions under which data workers in Kenya actually operated; and Billy Perrigo, a journalist for TIME magazine, published a damning investigation based on Motaung and other workers' testimonies (Perrigo 2022a). Motaung's accounts were related to the contract Sama signed with Meta to provide content moderation on its Facebook platform in Southern and Eastern Africa and revealed critical information about how both Sama and Meta treated and thought of data workers in Kenya.

After having gained access to Sama's payslips, TIME revealed workers in Kenya received as little as $1.50 per hour, among the lowest fares paid to Sama's employees on the planet (Perrigo 2022a). The calculation of these salaries supposedly responds to the company's mandate to pay a living wage in a way that would not distort local labour markets. However, research on Sama's operations in East Africa revealed circumstances in which the company transgressed its own – widely publicised – commitment to pay these minimum standards, in response to pressures from clients and an increasingly competitive market (Muldoon, Cant, Graham, Ustek Spilda 2023). Also the working regime under which Sama's employees operate seems to contravene the promise of dignified work advertised by the company. Through a digital monitoring system, workers' activities are closely surveilled, determining whether they are 'productive', 'idle', or 'out of focus' (Muldoon, Cant, Graham, Ustek Spilda 2023). Their 10-hour working day amount to an endless series of decisions that are closely monitored and have to be made in seconds in order to meet strict performance targets.

To add to the precarious and taxing nature of the job, for the contract signed by Sama with Meta, data workers were required to moderate highly disturbing content, including graphic images or videos depicting dismemberment, murder, or rape; causing some of them to develop post-traumatic stress disorder (PTSD), anxiety, and depression (Perrigo 2022a). In the summer of 2019, the combination of these factors motivated Daniel Motaung and other content moderators to threaten Sama they would strike within days unless they were given better pay and working conditions. However, as Perrigo (2022a) reported, "Instead of negotiating, Sama responded by flying two highly-paid executives from San Francisco to Nairobi to deal with the uprising. Within weeks Daniel Motaung, the attempted strike's leader who was in the process of formally filing trade union papers, had been fired."

Three years later, through the support of Foxglove, a non-profit organisation providing legal representation to tech workers, and following TIME's exposé, Daniel Motaung took Sama and Meta to court. Motaung's move – and the national and global support it received – is an important indication of changing attitudes among tech workers in the Global South, and more generally, of shifting perceptions about the limits of exploitation and extraction, even if couched under the banners of digital innovation and opportunity. It ties with other experiences seeking to provide new frameworks and processes to protect platform workers and expand their rights (Cano, Espelt, Morell 2023; Graham, Woodcock, Heeks, Mungai, Van Belle, du Toit, Fredman, Osiki, van der Spuy, Silberman 2020), but it the first to emerge from the bottom-up, from a coordinated effort among platform workers in Africa. At the same time, Sama and Meta's responses to Motaung's claims as the legal case unfolded reflect the determination of tech giants not to back down, reaffirming and continuing exploiting existing imbalances of power.

Motaung's requests to the court fell in two categories. On the one hand, being recognised rights similar to those granted to Facebook workers and content moderators operating in Europe or the US, including adequate mental health support and better pay. On the other hand, recognising key provisions of the legal frameworks existing in the countries where data workers operate, including the rights to strike and form unions.

Meta's reaction was at once arrogant and ineffective. The company not only resorted to its usual playbook, arguing it had no registered office in Kenya, did not operate in the country, and it was thus not a party to the legal challenge against worker exploitation. It also filed a request for a 'gagging order' to prevent Daniel Motaung from speaking about the case. The request was later withdrawn, after a coalition of more than eighty organisations and prominent individuals (including whistle-blower Frances Haugen) signed a petition accusing Meta of discrimination towards an African and black employee, treated as a 'second-class digital citizen' (Rashad Robinson cited in Perrigo, 2022b). Similar requests had not been made in the past for other Meta employers turned critics or whistle-blowers (Perrigo 2022b). Finally, following the bad publicity surrounding the case, in January 2023 Meta terminated the contract with Sama and switched to Majorel, another outsourcing company operating in Kenya. Overnight, all Sama employees providing content moderation for Facebook not only lost their job, but, in apparent retaliation for their actions, criticism, and determination to speak to the press, they were covertly barred from gaining employment at Majorel. As Foxglove reported, 'messages between moderators and Majorel recruiters reveal that the recruiters were specifically instructed not to hire any moderators previously employed by Sama. One recruiter said: "Unfortunately they will not accept candidates from Sama, it's a strict no"'(Hegarty 2023a). In response to these revelations, some of the sacked moderators filed a civil application against Meta, Sama, and Majorel.

When asked to adjudicate the cases between the data workers and their employers, Kenya's courts emerged as unanticipated challengers of the status quo. In a series of unprecedented moves, Kenyan judges not only declared Meta a 'proper party' to the case (Dark 2023), but in June 2023 they ruled that Meta, and not Sama, was the 'true employer' of the content moderators in Kenya, meaning it was also legally responsible for them (Hegarty 2023b). This ruling, the first of its kind in the world, has potential game-changing consequences for tech giants, challenging their ability to exploit imbalances of power and rights, while remaining unaccountable for the dire conditions in which their outsourced employees have to operate. It also carries an important message for content moderators and data annotators in Africa and globally, countering the process of their invisibilisation, and illustrating how standing up for better working conditions and the recognition of basic rights, even against some of the world most powerful companies, can find support in an expanding network of institutions, activists, and media.

FROM CONTESTATION TO ADAPTATION

The second case – detailing the shift in the conceptualisation of South Africa's policy on data localisation – follows a trajectory that is almost opposite to the challenge brought by content moderators and data annotators to Big Tech. It narrates how determination to denounce and contest the excessive power of tech giants turned into acceptance of existing imbalances, recognising the limited space for negotiation available to governments and corporations in the Global South in an increasingly concentrated market. It also reaffirms how attempts to alter the geopolitics of data flows, if pursued in isolation and by less powerful actors, have little chances of success.

On 1st April 2021, the Department of Communications and Digital Technologies (DCDT) published the "Draft National Policy on Data and Cloud" (DCDT 2021), a consultation document open to comments from industry, civil society, research centres, and the public at large. The section on localisation and cross border data transfer contained very strong statements, denouncing the dominance of foreign actors and asserting the need for smaller players to benefit from the increasing centrality of data in shaping both economic activities and public services. These went from lamenting the "dominance of North American, European, and Asian technology giant companies [as] shown by the concentration of data centres" (DCDT 2021, p. 28) and the implication that "data generated in Africa and South Africa is mostly stored in foreign lands and, where stored locally, is owned by international technology giant companies" (DCDT 2021, p. 29); to asserting the need that "data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled" (DCDT 2021, p. 30). Assertions like these are quite rare in policy documents, and are reminiscent of critical scholarship on data colonialism, denouncing tech giants' extractivist practices (see Couldry, Mejias 2019; Crawford 2021).

Three years later, however, when the final "National Policy on Data and Cloud" (DCDT 2024) was published, this form of criticism and assertion of national sovereignty over data had all but disappeared. The same section – detailing principles and measures related to data localisation and cross border data transfer – signalled almost a U-turn, reframing South Africa from a potential source of criticism towards Big Tech's extractive practices, to an appealing destination for multinational corporations:

> The free flow of data is an important catalyst for robust internet services and the global exchange and sharing of information and data. Many multinationals, based in South Africa and other countries, rely on an open cross-border data regime to be able to manage their businesses across different jurisdictions. Any restriction to such cross-border flows can have a negative impact on such businesses. South Africa is an investment destination for many multinationals that are supporting local economic growth and jobs required for sustainable livelihoods (DCDT 2024, p. 26).

One may be inclined to read – not without reason – in this dramatic change of attitude yet another example of tech giants flexing their muscles, forcing less powerful players to abandon attempts to set a different course. South Africa, after all, hosts the majority of data centres in Africa. As of 2024, it is the only cloud region including all operators that are in the continent: IBM, Amazon, Microsoft, Google, Alibaba, Oracle, and Huawei (Tugendhat Forthcoming; DC Byte 2024). While claiming greater state control over data stored on servers owned by foreign companies could appear to some an opportunity to cash in on the country's position as the continent's largest data warehouse, for other the same measure could jeopardize South Africa's potential in a fast growing market, where strong competitors – i.e. Kenya, Nigeria, Egypt (DC Byte 2024) – are rapidly emerging.

This reading, however, while not inaccurate, would be reductive and obfuscate a more critical learning point emerging from comparing the two documents. As numerous, publicly available, responses to and analyses of the draft policy (Razzano 2021; van der Berg 2021; Research ICT Africa 2021; Sutherland 2021) highlighted, the types of assertions of sovereignty advanced in the draft policy built on a somehow misleading understanding of what South African institutions could actually do if they owned data produced in South Africa but stored by foreign tech companies. While it is encouraging to see how a policy document could be receptive of arguments made in critical media and AI scholarship, denouncing concentration in the hands of few multinationals and their extractivist practices, the alternative practices the document advanced build on a narrow conception of the value of data, considered mostly as "a tradable commodity" (DCDT 2021, p. 29). As Gabriella Razzano remarked in her analysis of the policy, "the idea that simply gathering more and more data creates economic benefits does not recognise the microeconomic realities of data" (Razzano 2021, p. 3). Owning data, while intrinsically difficult because of the only partially excludable nature of data as commodity (van der Berg 2021), per se, offers very little guarantees to generate significant value when data are sold to third parties. It is the ability of using data, not owning them, that generates value. Because of economies of scale, it is mostly large firms in dominant positions that can extract value from interpreting that data and feeding it into their own products and services (Razzano 2021; Martínez 2019).

More critically, the state centric approach to the data economy proposed in the Draft Policy fell into two distinct, but related, traps. The first is political. The actors the Draft Policy sought to exclude, or whose claims it sought to limit, were not only tech giants. They were also other states. This may seem an obvious goal, and intrinsic to any sovereignty claim. But, in this particular conjuncture – characterised by the overwhelming power of a few multinational companies vis à vis the limited capacity of state and corporate actors in Africa – it unduly heightened competition with other African states in similar positions of subalternity, rather than recognising the potential gains that could be made by experimenting with more coordinated approaches. In this regard, the final National Policy, despite its other shortcomings, tried at least to acknowledge the possibility of establishing stronger ties with other African states, in the framework of African Continental Free Trade Area (AfCFTA).

The second trap is economic. By emphasising the monetary gains that can be made by trading data, rather than seeking to imagine which kind of data could be especially important for achieving specific goals – e.g. better service delivery or preparedness to face emergencies – the Draft Policy implicitly limited considerations on the value of data to market logics, while the ambitions of data governance frameworks can also be social and transformative (Razzano 2021). A comparison with proposals to compensate individual users for their data shows interesting analogies and may help further clarifying this point. As Ulises Mejias remarked:

> First, it's a very neoliberal response, focusing on the individual at the expense of the collective [...] In the end the idea is that the problem is solved once each individual "gets theirs." [...] Secondly, this solution again leaves the fundamental problem of data colonialism, the problem of extraction and appropriation, intact. In fact, it normalizes it, by telling people: "We are going to continue the extraction, but here are a few pennies for your troubles" (van der Spuy, Mejias 2020)

In the absence of creative and concerted efforts, attempts seemingly challenging the overwhelming power of tech giants, but limited in practice to serving narrow individual, national or economic interests, seem condemned to fail or even to reinforce the same logics they initially set to contest.

NETWORKED SOVEREIGNTY?

The two cases examined in this article are significantly different and followed almost opposite trajectories. One was a bottom-up response to exploitation, emerging from individuals who felt deprived of their rights and dignity, and found possibly unexpected backing both from local institutions – Kenyan unions and courts – and international activist networks. Bolstered by this support, many AI annotators and content moderators have progressively become recognisable actors, seeking to oppose the invisibilisation of the work powering up social networking platforms and AI models as well to raise awareness on colonial supply chains exploiting existing power imbalances. The other emerged as a botched attempt to incorporate some of the criticism denouncing tech giants' extractivist practices into policies that could contain or redress some of those practices in actuality. As the policy evolved towards the final draft, these ambitions appeared short-lived, but also revealed the shortcomings of seeking to beat tech giants at their own game, rather than imagining creative ways to make use of data and innovations towards different goals.

Taken together, however, the two cases help making two important points, one empirical and one conceptual. First, an increasing number of actors in Africa – from labourers to governments – have begun to stand up to the exploitative mechanisms introduced by foreign tech companies under the pretence of benevolent innovation and connectedness. These attempts are likely to face opposition by tech giants seeking to protect their image of benign modernisers as well as their profit margins. Or, as the South African case illustrates, they may lack strategy. After all, for a long time Africa has been defined through the lenses of ICT for development – and purportedly new paradigms of AI for good have emerged in its path – framing the continent as a space lacking innovation and depending on external support. Changing these paradigms – making external actors aware of the distinct visions and materialities emerging from Africa; leveraging the increasing geopolitical competition making Africa an appealing frontier for growth – will require time and a strategic understanding of how to turn criticism of exploitative practices into concrete opportunities for charting new paths.

The second point is conceptual and is related to the contradictory nature of national sovereignty in Africa, and how it interfaces with digital innovation. As stated above, states in Africa have tended to be framed for what they lack, when compared to ideal types emerging from Europe. At the same time, authors like Achille Mbembe have accused African leaders of "fetishising" the nation-state, appropriating, rather than challenging colonial tropes. They "borrowed terms like 'national interest', 'risks', 'threats' or 'national security' [which] refer to a philosophy of movement and a philosophy of space entirely predicated on the existence of an enemy in a world of hostility, [while] disregarding [Africa's] long held traditions of flexible, networked sovereignty' (Mbembe 2017, p. 2). As he wrote, describing the functioning of networked sovereignty in precolonial Africa: "At the time, each economic space was part of a vast, more or less coherent regional and multinational ensemble, within which power and commerce often went together. Such regional and multiethnic ensembles were not characterized by stable and precise borders, or by clear figures of sovereignty, but rather by a complex series of vertical corridors, lateral axes, and networks that were often mutually imbricated according to the principle of intertwining and multiplicity" (Mbembe 2019, p. 181). Or, put differently, "Networks, flows and crossroads were more important than borders. What mattered the most was the extent to which flows intersected with other flows" (Mbembe 2017, p. 2).

What if greater efforts could be made to understand how these forms of networked sovereignty could be reappropriated and inform alternative paths of innovations? What if the "lacks" through which African states have been often defined – which in the AI space would amount to not enough data, infrastructures, skills – could be turned into opportunities to explore cooperative ways to reach the scale required to achieve well- and locally- defined sets of goals?

Certainly, African states could gain much greater leverage with tech giants if they were less concerned to display their ability to enforce their individual sovereign rights and were able to create coalitions around specific demands and projects. South Africa's attempts to claim sovereignty over data may lead to better outcomes if requests did not include all data in order to exclusively monetize on them, but targeted specific types of data – in sectors like health, agriculture, indigenous knowledge and languages – whose utility in generating new solutions could stretch beyond the country's borders. Or, in the case of AI annotators and content moderators in Kenya, their potential victory might incur in fewer risks to lead to scarcer job opportunities – as tech giants look elsewhere for less confrontational spaces – if it was able to generate momentum across countries and produce widely shared principles to regulate data work.

These scenarios may appear distant or unattainable, given the still very limited level of cooperation across African states in the digital sector (i.e. the African Union Convention on Cyber Security and Personal Data Protection adopted in 2014 is still inoperative as it lacks enough ratifications from individual states). But it is encouraging to notice how some of the key tenets that characterize the concept and historical practice of networked sovereignty – the intersection of flows generating value at their point of encounter, the possibility of different claims to coexist and the lack of necessity to identify an actor that could claim supreme power – share many similarities with other proposals to create more inclusive regimes of data governance. These include the generation of data pools that would allow access to large aggregation of data that might otherwise be unavailable to AI researchers and developers (Woods 2023), or new forms of "commoning" (De Angelis 2017; Calzati, Van Loenen 2023), as sociotechnical systems that do not include only data, but also communal values and labor processes.

BIBLIOGRAPHY

AI MEDIA GROUP, 2022. *Analysis of the 4IR in Africa – A Foundation for Growth*. Cape Town: AI Media PTY.

ALDEN, Edward, 2022. Washington Raises Stakes in War on Chinese Technology. *Foreign Policy*. Online. 2022. Available from: https://foreignpolicy.com/2022/10/11/us-china-technology-sanctions-semiconductor-chips-geopolitics-cold-war/

BARLOW, John Perry, 1996. *Declaration of independence for Cyberspace*. Online. 1996. Available from: http://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html

BEHERA, Navnita Chadha, 2020. State and sovereignty. In: TICKNER, Arlene, BLANEY, David and HAMATI-ATAYA, Inanna (eds.), *International Relations from the Global South: Worlds of Difference*. Routledge. p. 139–160.

BONE, Alayna, 2024. Taide: Taiwan's Own AI Project Highlights Geopolitical Implications. *Ketagalan Media*. Online. 6 May 2024. Available from: https://ketagalanmedia.com/2024/05/06/taide-taiwans-own-ai-project-highlights-geopolitical-implications/ [Accessed 3 October 2024].

BRAUN, Matthias and HUMMEL, Patrik, 2023. Sovereign Power: Artificial Intelligence and Europe's Digital Sovereignty. *Geopolitics*. 15 March 2023. Vol. 28, no. 2, p. 919–958.

CALZATI, Stefano and VAN LOENEN, Bastiaan, 2023. Beyond federated data: a data commoning proposition for the EU's citizen-centric digital strategy. *AI & SOCIETY*. Online. 21 August 2023.

CANO, Melissa Renau, ESPELT, Ricard and MORELL, Mayo Fuster, 2023. Working Conditions in Platform Work: Testing Digital Platform Workers' Rights on Platform Cooperatives. *SocArXiv*. Online. 2 April 2023.

CASTELLS, Manuel, 1996. *The Information Age: Economy, Society and Culture*. Oxford: Blackwell.

CHAGNON, Christopher W., DURANTE, Francesco, GILLS, Barry K., HAGOLANI-ALBOV, Sophia E., HOKKANEN, Saana, KANGASLUOMA, Sohvi M. J., KONTTINEN, Heidi, KRÖGER, Markus, LAFLEUR, William, OLLINAHO, Ossi and VUOLA, Marketta P. S., 2022. From extractivism to global extractivism: the evolution of an organizing concept. *The Journal of Peasant Studies*. 7 June 2022. Vol. 49, no. 4, p. 760–792.

CHAMPION, Mark, 2019. How U.S.-China Tech Rivalry Looks Like Cold War 2.0. *Bloomberg.com*. Online. 2019. Available from: https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war [Accessed 21 December 2022].

CHANDER, Anupam and SUN, Haochen, 2023. *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.

COULDRY, Nick and MEJIAS, Ulises A., 2019. *The costs of connection*. Stanford University Press.

CRAWFORD, Kate, 2021. *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

CREERY, Jennifer, 2024. Taiwan Builds Own AI Language Model to Counter China's Influence. *Bloomberg.com*. Online. 25 January 2024. Available from: https://www.bloomberg.com/news/articles/2024-01-25/taiwan-builds-own-ai-language-model-to-counter-china-s-influence [Accessed 2 October 2024].

DAHIR, Abdi Latif, 2018. Africa's youngest leader is riding a wave of hope from the young people who got him there. *Quartz*. Online. 30 May 2018. Available from: https://qz.com/africa/1292345/ethiopias-abiy-ahmed-marks-two-months-as-prime-minister/.

DALY, Angela and THOMAS, Julian, 2017. Australian internet policy. *Internet Policy Review*. Online. 14 March 2017. Vol. 6, no. 1.

DAMMANN, Finn and WINKLER, Jan, 2023. Digitally Competent – Digitally Sovereign – Digitally Civic: Geopolitics of Subject Formation in the German Context. *Geopolitics*. 15 March 2023. Vol. 28, no. 2, p. 919–958.

DARK, Martha, 2023. Facebook tried to dodge former content moderator Daniel's case in Kenya – and failed. *Foxglove*. Online. 6 February 2023. Available from: https://www.foxglove.org.uk/2023/02/06/facebook-daniel-failed/

DC BYTE, 2024. *Africa's Key Data Centre Markets*. Online. Available from: http://africadca.org/wp-content/uploads/2023/07/Title_Africas-Key-Data-Centre-Markets.pdf

DCDT, 2021. *Draft National Policy on Data and Cloud*. 1 April 2021.

DCDT, 2024. *National Policy on Data Cloud*. 27 March 2024.

DE ANGELIS, Massimo, 2017. *Omnia sunt communia: On the commons and the transformation to postcapitalism*. Bloomsbury Publishing.

DE GREGORIO, Giovanni and STREMLAU, Nicole, 2020. Internet Shutdowns in Africa| Internet Shutdowns and the Limits of Law. *International Journal of Communication*. 2020. Vol. 14, p. 4224–4243.

DEIBERT, Ronald, PALFREY, John, ROHOZINSKI, Rafal and ZITTRAIN, Jonathan, 2008. *Access denied: the practice and policy of global Internet filtering*. Cambridge: MIT Press.

DEIBERT, Ronald, PALFREY, John, ROHOZINSKI, Rafal and ZITTRAIN, Jonathan, 2011. *Access contested: security, identity, and resistance in Asian cyberspace*. MIT Press.

DEIBERT, Ronald, PALFREY, John, ROHOZINSKI, Rafal, ZITTRAIN, Jonathan and HARASZTI, Miklos, 2010. *Access controlled: The shaping of power, rights, and rule in cyberspace*. Mit Press.

DENARDIS, Laura, 2009. *Protocol politics: The globalization of Internet governance*. Mit Press.

ELMER-DEWITT, Philip, 1993. First nation in cyberspace. *Time*. 1993. Vol. 6, p. 62–64.

ERIE, Matthew S. and STREINZ, Thomas, 2021. The Beijing Effect: China's Digital Silk Road as Transnational Data Governance. *NYUJ Int'l L. & Pol.* 2021. Vol. 54, p. 1.

FISCHER, David, 2022. The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Zeitschrift für Politikwissenschaft*. 2022. P. 1–20.

FOSTER, Douglas, 2012. *After Mandela: The Struggle for Freedom in Post-Apartheid South Africa*. W. W. Norton & Company. ISBN 978-0-87140-479-4.

GAGLIARDONE, Iginio, 2019. *China, Africa, and the Future of the Internet*. London: Zed Books.

GLASZE, Georg, CATTARUZZA, Amaël, DOUZET, Frédérick, DAMMANN, Finn, BERTRAN, Marie-Gabrielle, BÔMONT, Clotilde, BRAUN, Matthias, DANET, Didier, DESFORGES, Alix, GÉRY, Aude, GRUMBACH, Stéphane, HUMMEL, Patrik, LIMONIER, Kevin, MÜNSSINGER, Max, NICOLAI, Florian, PÉTINIAUD, Louis, WINKLER, Jan and ZANIN, Caroline, 2023. Contested Spatialities of Digital Sovereignty. *Geopolitics*. 15 March 2023. Vol. 28, no. 2, p. 919–958.

GLASZE, Georg, DOUZET, Frédérick, DAMMANN, Finn and CATTARUZZA, Amaël, 2023. Emerging Geopolitics of Data. *Geopolitics*. 15 March 2023. Vol. 28, no. 2, p. 919–958.

GRAHAM, Mark, WOODCOCK, Jamie, HEEKS, Richard, MUNGAI, Paul, VAN BELLE, Jean-Paul, DU TOIT, Darcy, FREDMAN, Sandra, OSIKI, Abigail, VAN DER SPUY, Anri and SILBERMAN, Six M., 2020. The Fairwork Foundation: Strategies for improving platform work in a global context. *Geoforum*. 1 June 2020. Vol. 112, p. 100–103.

GRAY, Mary L. and SURI, Siddharth, 2019. *Ghost work: How to stop Silicon Valley from building a new global underclass*. Eamon Dolan Books.

GRUMBACH, Stéphane and ZANIN, Caroline, 2023. Platforms Vs. States: A Sovereignty Conundrum. *Geopolitics*. 15 March 2023. Vol. 28, no. 2, p. 919–958.

HEGARTY, Tom, 2023a. The Facebook-Sama layoffs: union busting disguised as redundancy in Nairobi. *Foxglove*. Online. 24 March 2023. Available from: https://www.foxglove.org.uk/2023/03/24/facebook-sama-layoffs-redundancy-nairobi/

HEGARTY, Tom, 2023b. Huge ruling in Kenyan court threatens global model of outsourced content moderation – and says that Facebook is the "true employer" of its key safety workers. *Foxglove*. Online. 6 June 2023. Available from:

https://www.foxglove.org.uk/2023/06/06/kenyan-court-ruling-outsourced-content-moderation-facebook/

JACKSON, Robert H., 1986. Negative sovereignty in sub-Saharan Africa. *Review of International Studies*. 1986. Vol. 12, no. 4, p. 247–264.

JACKSON, Robert H., 1990. *Quasi-states: sovereignty, international relations and the Third World*. Cambridge University Press.

JANAH, Leila, 2017. *Give work: Reversing Poverty one job at a time*. Penguin.

KWET, Michael, 2020. The City Surveillance State: Inside Johannesburg's Safe City Initiative . 2020.

LEE, Kai-Fu, 2018. *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin.

LÉVY, Pierre, 1995. *Qu'est-ce que le virtuel?* Paris: La découverte.

MARTÍNEZ, Antonio García, 2019. No, Data Is Not the New Oil. *Wired*. Online. 2019. Available from: https://www.wired.com/story/no-data-is-not-the-new-oil/

MBEMBE, Achille, 2017. Scrap the borders that divide Africans. *Mail & Guardian*. 2017. Vol. 17.

MBEMBE, Achille, 2019. *Out of the Dark Night: Essays on Decolonization*. Columbia University Press. ISBN 978-0-231-50059-3.

MBEMBE, Achille, 2020. At the Edge of the World: Boundaries, Territoriality, and Sovereignty in Africa. *Public Culture*. 2020. Vol. 12, no. 1, p. 259–284.

MKOKELI, Sam and COHEN, Michael, 2018. Mandela's Favored Heir Takes Power in South Africa. *Bloomberg.com*. Online. 15 February 2018. Available from: https://www.bloomberg.com/news/articles/2018-02-15/mandela-s-favored-heir-ramaphosa-takes-power-in-south-africa.

MUELLER, Milton, 2010. *Network and states. The global politics of internet governance*. Cambridge, Mass ; London: The MIT Press.

MULDOON, James, CANT, Callum, GRAHAM, Mark and USTEK SPILDA, Funda, 2023. The poverty of ethical AI: impact sourcing and AI supply chains. *AI & SOCIETY*. Online. 20 December 2023.

MULDOON, James and WU, Boxi A, 2023. Artificial Intelligence in the Colonial Matrix of Power. *Philosophy & Technology*. December 2023. Vol. 36, no. 4, p. 80.

MUSIANI, Francesca, 2022. Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*. 26 April 2022. Vol. 25, no. 6, p. 785–800.

PAUL, Kari and MILMO, Dan, 2021. Facebook putting profit before public good, says whistleblower Frances Haugen. *The Guardian*. 2021.

PERRIGO, Billy, 2022a. Inside Facebook's African Sweatshop. *TIME*. Online. 14 February 2022. Available from: https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/

PERRIGO, Billy, 2022b. Facebook Is Attempting to Silence a Black Whistleblower. *TIME*. Online. 1 July 2022. Available from: https://time.com/6193231/facebook-crack-whip-black-whistleblower/

POHLE, Julia and THIEL, Thorsten, 2021. Digital sovereignty. *Internet Policy Review*. 2021. Vol. 9, no. 4, p. 47–67.

RAZZANO, Gabriella, 2021. Policy Brief 06: *Data Localisation in South Africa: Missteps in the Valuing of Data*. Online. Mandela Institute.

RESEARCH ICT AFRICA, 2021. Written submission in response to the Proposed National and Data and Cloud Policy. Online. 2021. Available from: https://researchictafrica.net/wp-content/uploads/2021/06/public-interest-submission-to-dcdt-on-south-africas-proposed-national-data-and-cloud-policy.pdf

SEGURADO, Rosemary, LIMA, Carolina Silva Mandú de and AMENI, Cauê S., 2014. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. *História, Ciências, Saúde-Manguinhos*. 13 August 2014. Vol. 22, p. 1551–1571.

SUTHERLAND, Ewan, 2020. The Fourth Industrial Revolution – The Case of South Africa. *Politikon*. 2 April 2020. Vol. 47, no. 2, p. 233–252.

SUTHERLAND, Ewan, 2021. *South Africa - Response to draft National Policy on Data and Cloud*.. Online. SSRN Scholarly Paper. 31 May 2021. Rochester, NY: Social Science Research Network.

TUGENDHAT, Henry, Forthcoming. Gathering Clouds Over Africa's Digital Sovereignty: An Analysis of Chinese and US Cloud Infrastructure. Forthcoming.

VAN DER BERG, Shanelle, 2021. Policy Brief 02: *Data protection in South Africa. The potential impact of data localisation on South Africa's project of sustainable developoment*. Online. Mandela Institute.

VAN DER SPUY, Anri and MEJIAS, Ulises Ali, 2020. Should we nationalise data? In conversation with Ulises Mejias. . Online. 19 March 2020. Available from: https://researchictafrica.net/2020/04/07/should-we-nationalise-data-in-conversation-with-ulises-mejias/.

VAN DER VLIST, Fernando, HELMOND, Anne and FERRARI, Fabian, 2024. Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data & Society*. March 2024. Vol. 11, no. 1.

WOO, Stu, 2020. The U.S. vs. China: The High Cost of the Technology Cold War. *WSJ*. Online. 2020. Available from: https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438.

WOODS, Andrew Keane, 2023. Digital Sovereignty + Artificial Intelligence. In: CHANDER, Anupam and SUN, Haochen (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.