‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs

a document review on Kenya

Calzati, Stefano

DOI
10.1080/02589001.2022.2027351

Publication date
2022

Document Version
Final published version

Published in
Journal of Contemporary African Studies

Citation (APA)
Calzati, S. (2022). ‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya. *Journal of Contemporary African Studies*, *40*(2), 270-285. https://doi.org/10.1080/02589001.2022.2027351

Routledge
Taylor & Francis Group

Journal of Contemporary African Studies

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cjca20

‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya

Stefano Calzati

To cite this article: Stefano Calzati (2022) ‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya, Journal of Contemporary African Studies, 40:2, 270-285, DOI: 10.1080/02589001.2022.2027351

To link to this article: https://doi.org/10.1080/02589001.2022.2027351

Published online: 03 Feb 2022.

JOURNAL OF CONTEMPORARY AFRICAN STUDIES
2022, VOL. 40, NO. 2, 270–285
https://doi.org/10.1080/02589001.2022.2027351

Routledge
Taylor & Francis Group

'Data sovereignty' or 'Data colonialism'? Exploring the Chinese involvement in Africa's ICTs: a document review on Kenya

Stefano Calzati

Department of Urbanism, TU Delft, Netherlands

ABSTRACT

Information and Communication Technologies (ICTs) have become a crucial sector of China–Africa relations. As scholars have noted, Africa's 4th Industrial Revolution (4IR) risks transforming into a new 'scramble' with foreign actors harnessing Africa's data. The present article explores this issue at a discursive level, i.e. delving into policies, bilateral agreements, and laws. The focus is specifically on Kenya in that it is one of the most developed ICT markets in Africa and it is here that the Chinese tech giant Huawei began its investments in 1998. Via a document review, the article provides a preliminary discursive assessment of the extent to which Kenyan actors are effectively (dis)empowered with regard to their own 4IR. The analysis shows that both pan-African and bilateral agreements remain at a high level of abstraction: while this is the typical Chinese way of framing discourses on technological innovation, it also leaves room for political manoeuvring and potential forms of data colonialism.

ARTICLE HISTORY
Received 9 July 2020
Accepted 4 January 2022

KEYWORDS
China–Africa relations; ICTs; Kenya; data colonialism; data sovereignty

1. Introduction

This article is framed within the broad and multi-layered issue of China–sub-Sahara Africa (SSA) relations in the context of Information and Communication Technologies (ICTs). Today, many ICT companies operating in SSA are foreigners and some scholars have denounced the lack of African agency in matter of tech- and data-related policies, investments and socio-economic benefits (Mohan and Lampert 2013; Mutsvairo and Ragnedda 2019; Taylor and Broeders 2015). Beyond these warnings, little research has been conducted on how the relations binding China and ICT Chinese companies to African authorities and ICT actors are discursively framed, with particular regard to the lifecycle of data, i.e. the collection, storage, access, use, and distribution of data.

Following the work of Friederici, Ojanperä, and Graham (2017) methodologically, this article provides a critical review of the documents – i.e. agreements, policies, laws – surrounding and regulating China–Kenya cooperation in ICTs. The article focuses specifically on Kenya because it is here that the main Chinese private ICT company – Huawei – anticipating Western actors, launched its investments in Africa in 1998.

CONTACT Stefano Calzati s.calzati@tudelft.nl Department of Urbanism, Room 540, TU Delft

Through the lenses of the concepts of 'data colonialism' (Couldry and Mejias 2019; Calzati 2021) and 'data sovereignty' (Hummel et al. 2021; Kushwaha, Roguski, and Watson 2020), the document analysis aims to bring to light how the 'data knowledge' on the lifecycle of data is distributed across the network of identified Chinese and Kenyan actors. This is propaedeutic to highlighting the emergence of a 'data divide', characterised as the (potential) unevenness affecting the data knowledge distribution among the actors. The analysis provides a preliminary discursive assessment of the extent to which China is effectively involved in a new (data-related) scramble for Africa, or whether it is fostering a sovereign-based cooperation with African actors.

The article is structured as follows. Section 2 accounts for the rise of SSA as an ICT pole, mainly due to the investments of foreign actors; section 3 introduces the concepts of data colonialism and data sovereignty, and pinpoints literature on Asian-specific discursive and rhetorical strategies; section 4 is dedicated to unpacking the method of the analysis, presenting the actors and documents surveyed; section 5 analyses the main pan-African document, that is, the Forum on China Africa Cooperation (FOCAC); section 6 delves into bilateral China–Kenya agreements, involving both public and private actors; section 6 offers a comparative analysis between Kenya's Data Protection Act (DPA) and other similar laws in the European Union, South Africa and China; in section 7 some conclusion and further research lines are outlined.

2. The boom of ICTs in SSA and China's role

According to recent statistics on connectivity and digital growth (We Are Social 2019), Africa is currently the continent with the strongest annual digital growth worldwide: +5.2% in mobile subscriptions and +8.7% in Internet users between 2018 and 2019.

In this scenario, Chinese ICT-related investments in SSA have become pervasive (Oreglia 2012) spanning all regions: eastern (e.g. Kenya, Ethiopia, Zimbabwe), western (e.g. Ghana and Nigeria), central (e.g. Cameroon), and southern (mainly in South Africa). These investments, often in the form of financial loans, focused first on the building of infrastructure (backbone and end-mile cabling) and, over the last decade, shifting towards knowledge transfer, cloud computing, artificial intelligence (AI) solutions, and smart city projects. On the other hand, after a gradual increase since early 2000s, from 2015 onwards the United States has reduced its foreign direct investment (FDI) in SSA (Statista 2018). Only in 2019 did Trump's administration declare that the United States International Development Finance Corporation (DFC) would put forward a US$60 billion investment plan in Africa, with the precise intention of 'providing a robust alternative to the Chinese debt-heavy model that can leave developing countries worse off.'[1]

Differently from Western powers, China has been said to exert a 'soft power' on Africa, by promoting investments 'with no strings attached' (Gagliardone 2019). This means that China is committed to developing African infrastructure and services by fostering agreements that do keep African parties in business and involve local authorities and workforces, tailoring investments to their needs. While the extent to which China's and Chinese companies' commitment to fostering solid ICT markets in SSA is also empowering African actors and not simply indebting them is still being debated, the idea of a homogenising 'soft power' exerted by China on Africa nonetheless calls for contextualisation.

In fact, such a label can hardly account for the variety and complexity of Chinese investments on the continent. It would be too simplistic to consider Chinese companies as the

longa manus of the Chinese government in Africa, insofar as the diverse, multi-layered initiatives put forth by Chinese actors – diplomats, private companies, state-led companies, trade intermediaries, etc. – frequently follow mutually competing agendas. Existing literature (Xu 2014) shows that China's Ministry of Commerce and China's Ministry of Foreign Affairs tend to have different approaches to their foreign partners, often leading to contrasts between how they function. In this regard, according to Li (2008), the paradigm has shifted from 'economy serving diplomacy' to 'diplomacy serving economy'.

In the words of Gu et al. (2016, 25) 'this [diplomacy] has two aspects: multilateral (pan-African) and bilateral (state-to-state) diplomacy. The former is driven through the FOCAC framework, a dialog and institutionalised process for cooperation established in 2000. The latter is driven by extensive tours of African states by Chinese state and party officials and bilateral cooperation agreements.' Most interestingly, in the 2015–2018 plan which followed the 6th Forum on FOCAC, it was announced the strategic decision to turn the Forum on China–Africa Media cooperation into an official sub-forum of FOCAC. This shift highlights the extent to which both China and African countries consider ICTs as a crucial sector of their mutual cooperation.

At the same time, beyond this pan-Africa framework, China is increasingly committed to fostering bilateral agreements with individual African states. The goal is to adapt to each context without imposing an agenda, but rather seeking a convergence between China's own interests and those of local actors. On this point, Gagliardone (2019, 56) claims that 'a continental overview of China's engagement (…) corroborates the impression that China is not trying to impose a blueprint (…) Rather, [it] has produced specific and individual responses in different African countries.'

This means that China–SSA relations in the ICTs are multi-layered and call for contextualisation – here the focus is on Kenya and the role of the Chinese tech giant, Huawei – as well as for a critical unpacking of their discursive framing. This is the first necessary step towards a cognisant assessment of the extent to which agreements between China (and Huawei) and Kenya in the matter of tech innovation can be said to empower all actors involved – especially Kenyan actors and citizens – or rather tend to (re)produce power asymmetries within a South-South geopolitical context. In other words, at stake is Kenya's data sovereignty over its own 4IR.

2.1. The role of Huawei in Kenya

China's presence in Kenya's ICT sector has become crucial over the last two decades (Oreglia 2012; Gagliardone 2019). Here, Huawei – the major Chinese private ICT company – provides both backbone and last mile solutions (Oreglia 2012). Indeed, it was in Kenya that Huawei began its African investments in 1998, anticipating the advent of other American and European actors. At present, Huawei is in charge of the phase two of the National Optic Fibre Backbone Infrastructure (NOFBI): the project is expected to link all 47 counties by implementing an extra 1600 km of fibre. Beyond that, Huawei has gradually expanded its investments in the country, encompassing not only infrastructure and products but also corporate social responsibility (CSR) projects. Among these, the company is committed to promoting knowledge transfer through its ICT academy programmes. The long-lasting and diversified presence of Huawei in Kenya, and its partnership with the strong local subsidiary Safaricom, has given the

Chinese company an edge over competitors such as Airtel Networks Kenya (owned by Indian Bharti Airtel) and Telkom Kenya (owned by Orange France).

As King (2013) notes, these CSR initiatives are framed within a logic that moves beyond economy and comes to encompass the cultural sphere of mutual understanding between China and Kenya. However, the impact of that training on Kenyans, as well as the effective (social) return Huawei gets from such initiatives, remain to be seen. This lack of certainty is reflected in the fact that not only are managerial roles in Chinese ICT companies in Kenya still heavily occupied by Chinese people (Makundi, Huyse, and Develtere 2016), but the knowledge transfer that such training provides is debatable, depending on the companies involved and the countries studied (Agbebi 2018; Musyimi, Malechwanzi, and Luo 2018).

3. Unpacking data sovereignty and its underpinning epistemologies

3.1. (Cyber) power relations

The genealogy of China–Africa relations in the ICTs can be dated back to the 1970s, on the wave of third-worldism's commercial and political partnerships between so-called 'non-aligned' countries.

Today, the scenario has radically changed. With the consolidation of global trade and ICT infrastructure, it has becomes necessary not only to extend discussions on technological and geopolitical power relations to 'subalterns' – especially in the context of South-South relations – but also to rethink these same discussions, shifting from an international to a transnational perspective whereby the global mapping of power relations is accompanied by a critical questioning of how these relations rework borders, sovereignty and coloniality. As Wen (2021, 12) writes in his *The Huawei's Model* 'the development of the global economy has been characterised by the transition towards transnationalized digital capitalism, within which information and communications technologies have increasingly played a pivotal role in restructuring the global capitalist system.' This entails, in other words, undoing dichotomies such as 'global-local', especially when it comes to issues of 'data colonialism' and 'data sovereignty'. In this respect, Wasserman (2018, 448) correctly notes that at stake is the assessment of the remaking of global power relations that 'have prompted different ways of thinking about categories such as the "South," the "global," the "local" and the "transnational".' As Calzati (2021) points out, what we are witnessing is the emergence of federated forms of technological globalisation – contested internally as much as externally – in which the circulation of data, tech expertise, innovation, and policies can be favoured as much as hindered by competing discourses, actors, and technologies belonging to and traversing different networks of power *at once*.

Studies have shown the 'misalignment' between the Internet as a common infrastructure and the legitimacy of sovereign powers (Mueller 2019), as well as the shifting toward a multipolar scenario (Winseck 2017) in Internet governance. The European Commission (2020) has also acknowledged these concerns, warning against the 'digital dependency on non-European providers and the lack of a well-performing cloud infrastructure respecting European norms and values.' As Yu and Goodnight (2020, 13) note with specific regard to China, 'cast in light of the cybersphere, China's so-called Intranet also reveals entanglements with foreign capital, foreign technology, foreign markets, and foreign labor.' Hence, tech and data sovereignty (and their implied possibility for self-

determination of countries and people) can be best regarded as macro-entangled dimensions which, to begin with, contest and resist linear (agent-structure) readings. This is why discursive and geopolitical approaches heralding competing visions of ICTs (e.g. multistakeholderism vs. multilateralism, see Nonnecke 2016) might no longer be sufficient. It is in this respect that Kushwaha, Roguski, and Watson (2020, 60) remark that, while the report by the UN Expert Governmental Group[2] affirms that 'states have jurisdiction over the ICT infrastructure located within their territory', this 'did not form a consensus view as to jurisdiction over data stored within that ICT infrastructure.' This leaves the door open to forms of disguised data expropriation, which demands contextual assessment.

3.2. Emerging discourses

As soon as SSA's 4IR is explored through the lenses of geopolitical tech and data sovereignty, a new 'scramble for Africa' (Taylor 2013), aimed at controlling the deluge of ICTs-derived data of the continent, becomes apparent. Of particular significance is the lack of agency to which Africa, African institutions and African people are subjected, when it comes to their own digital transformation. Studies show a colonially-tainted asymmetry with developed countries (Mohan and Lampert 2013; Taylor and Broeders 2015), which relegates African countries and people to a subaltern role. This means that Africa is often objectified, i.e. considered as a mere recipient of top-down ICT-related investments and policies. Mutsvairo and Ragnedda (2019, 22) claim, on this point, that: 'we do not think policies should be drafted in Washington or Brussels'. Building on that, the present article explores how tech partnerships between China and Chinese companies, on the one hand, and Kenya actors, on the other hand, are discursively presented, while aware of the fact that language always embeds socio-political and ideological salience (Fairclough 2003; Van Dijk 2008).

On this point, it is worth noting that a growing body of studies in socio-linguistics, with a specific focus on the intercultural dimension of communication, shows that Asian people tend to pay attention to contextual cues and the whole scenario, while Westerners zoom in on the most relevant pieces of information in an analytical way (Masuda and Nisbett 2001). Moreover, from the point of view of rhetoric, while Asians adopt circular discursive strategies to gradually arrive to the point, Westerners unfold linear argumentative structures (Kaplan 1983).

For the present discussion, these ideas find support in how China has fostered its own discourse on tech development and AI. For instance, the document "New Generation of Artificial Intelligence Development Plan"[3] is characterised by some precise economic goals and more abstract conceptualisations of the social impact of these goals. As researchers (Roberts et al. 2021, 72) have noted, the document is 'limited to high-level principles, lacking implementation'. Far from evidencing inaccuracy, this can be regarded as a typical 'Chinese way' of framing policies and agreements, whereby high-level abstract visions involving the whole of society are favoured over step-by-step linear narratives.

4. Method

While relations between China and SSA are usually presented to public opinion in the form of peer-to-peer collaborations (King 2013), the unpacking of the power relations

that traverse official documents, agreements, and laws in matter of ICT cooperation remains uncharted. This article aims to remedy that situation by conducting a two-layer – pan-African and state-level (i.e. Kenya) – document review. Based on exiting literature (Gu et al. 2016; Xu 2014), the following relevant actors are identified: China's Ministry of Foreign Affairs (MFA), China's Ministry of Commerce (MOFCOM), Kenya's Ministry of ICT and Youth Affairs, Kenya's Communication Authority (CA), Huawei and Safaricom (i.e. Huawei's subsidiary in Kenya). Lastly, the case of South Africa is brought into the discussion for a comparison between this country's law on data protection (Protection of Personal Information Act – POPI Act 2013),[4] Kenya's recent Data Protection Act (DPA 2019)[5] – which is heavily inspired by Europe's General Data Protection Regulation (GDPR 2016)[6] – and China's Cybersecurity Law. This will allow a better understanding, through and beyond discursivities, of the extent to which Kenyan actors are able to (re)appropriate the data produced indigenously, or whether they are still mainly subjected to foreign agency and data expropriation.

5. China-Pan African framework: the Forum on China–Africa cooperation

By delving into the analysis of the latest FOCAC document (for the years 2019–2021), it is possible to see that this document does contain references to ICT- and tech-related synergies. For example, the article 3.3.5 states that:

> The two sides will, in recognition of the strategic and far-reaching impact of information and communication technology (ICT) on economic and social development, enhance exchanges and cooperation between competent authorities, share good practice in each other's ICT development, seize the opportunity presented by the digital economy.

The wording remains at a very general level. No specifications, for instance, are given about what a 'good practice' in the ICTs consists of, or how the sharing of 'each other's ICT development' should be intended and concretely pursued. Something more can be found in the subsequent article 3.3.6, dedicated to the 'far reaching impact of ICTs':

> The two sides will actively explore and advance cooperation in the application of new technologies including cloud computing, big data, and the mobile Internet. China will support African countries in building 'smart cities' and enhancing the role of ICT in safeguarding public security, counter terrorism and fighting crime and work with the African side to uphold information security.

Here, after a prelude that reaffirms the 'cooperation' between the two sides, it is clearly stated that it is China that will take the lead in supporting African countries. Most interesting is the mention of the sharing, among parties, of cloud computing technologies (which will also return in other documents) and big data. The flourishing of cloud computing and its dislocation by private tech giants around the globe, is what really constitutes, today, a new form of contemporary (data-related) colonialism. Sometimes – as we will see in the next section – even governments and public services rely on private foreign data centres, literally forfeiting their tech-dependent sovereignty to foreign private ICT companies. Against this backdrop, the level of discursive abstraction complied with is significant; no further insight is provided regarding, for instance, where and for which purposes could computing technologies will be implemented, or which data will be collected, stored and circulated, how, and among whom.

Overall, the FOCAC is meant to outline very broad guidelines along which subsequent bilateral agreements can be based. Moreover, the document follows the Chinese way of communication, reaming rather elusive on the realpolitik surrounding these agreements. Hence, from the FOCAC document, it is difficult to assess concretely the data knowledge distribution across the actors involved or any potential data divide among them. At the same time, considering China's long-lasting involvement in SSA's ICT markets, this discursive elusiveness – however culturally loaded – is hardly accidental and might come in handy for leaving the door open to interpretation and political manoeuvring.

6. China–Kenya bilateral agreements

In this section, the review of the most important documents in matter of ICT cooperation released over the last three years (September 2016–September 2019) by Chinese public and private actors – the MFA, the MOFCOM, Huawei – and Kenyan public and private actors – Ministry of ICT and Safaricom – are discussed, putting the stress on how the lifecycle of data is discursively framed.

6.1. China's ministry of foreign affairs and China's ministry of commerce

Through the analysis of the press releases published on the website of the China's MFA, the technological cooperation between China and SSA emerges as a chiefly diplomatic matter, without really digging into the specifics of the projects. A case in point is the "Joint Communiqué of the Leaders Roundtable of the Belt and Road Forum for International Cooperation" (16 May 2017).[7] This document, which reflects the state of the art about the development of the Belt and Road Initiative, resonates with the discursive ethos of FOCAC's document. In fact, both the objectives and the measures of cooperation contained in the communiqué are described in very broad terms, without further substantiation, time schedules, or implementation phases.

Differently, the press releases of China's MOFCOM are more tech-focused. For instance, in a document published on 11 May 2017 and titled "Harnessing the China–Africa ICT Opportunities",[8] it is stated that 'the two principles that should beguiding [*sic*] investments into ICT are safety and sustainability, where three major types of ICT are likely to play an instrumental role: surveillance cameras, light emitting diodes (LEDs) and geographic information systems (GIS).' The same document overtly mentions the example of Kenya, a country in which Huawei and its subsidiary, Safaricom, collaborated to Kenya's 'safe city' solutions in order 'to deal with terrorism in Nairobi and Mombasa, [by installing] 1,800 surveillance cameras.'

A further document published on MOFCOM website on 27 July 2017[9] states, with particular attention to Kenya, that 'Huawei has invested in supportive infrastructure and technical expertise to facilitate faster integration of cloud computing in key operations. Kenya's President Uhuru Kenyatta during his trip to China in May signed an agreement with Huawei to help develop government cloud services.' It emerges from here that also Kenyan governmental bodies resort to technological solutions provided by Huawei for 'key operations' which – it is reasonable to assume – have a public outreach and, as such, concern the whole Kenyan population.

More broadly, in the digital transformation of African governmental services are involved not only Chinese firms but also Western ones, as clearly stated in a document published on 27 November 2017.[10] According to this document, the Chinese company Inspur is at the lead of an international consortium including 'Cisco, IBM, Diebold Nixdorf, and Ericsson' whose goal is 'to integrate their cutting-edge IT products, technologies [i.e. datacenters and cloud services] and solutions to accelerate the construction of the Digital Silk Road.' The document continues as follows: 'projects will first be launched in South Asian and African countries, such as Thailand, Bangladesh, Malaysia, Nigeria, Ethiopia, Tunisia, Tanzania, Zambia, and Kenya.' Although it is not specified (or precisely because of that), it is not audacious to assume that the Digital Silk Road has to do, among other aspects, with the harnessing by Chinese (and Western) actors of the fruits of SSA's 4IR. Legal and procedural constraints to which the actors involved would be subjected are overlooked. In this sense, tech and data sovereignty become a field of tensions, since such sovereignty gets contested and distributed across a number of private foreign actors which cannot be said to be directly responsible for Kenyan national interests.

6.2. Huawei Kenya and Safaricom

Since Huawei and Safaricom are two of the major ICTs companies in Kenya, it is interesting to look at their most recent CSR reports to see if and how issues connected with the life-cycle of data are addressed.

Huawei Kenya latest report (2018)[11] consists of 48 pages divided into 6 sections: 'About Huawei Kenya'; 'Huawei Sustainability Strategy'; 'Bridging the Digital Divide'; 'Supporting Stable and Secure Network Operations and Protecting Users Privacy'; 'Promoting Environmental Protection'; and 'Building a Healthy Ecosystem'. For the present discussion, the most relevant section is the fourth one, which is also the most concise, consisting of only two pages. Here, on the one hand, Huawei Kenya does stress its commitment towards cybersecurity, as well as its proactivity in fostering corporate awareness as far as data protection is concerned: 'fostering a company-wide climate and culture of cybersecurity awareness helps ensure that every employee accounts for cybersecurity and privacy protection.' On the other hand, however, the report does not go into any detail about how such practices are put forth, i.e. how data protection is performed and how corporate awareness on this issue is fostered. While it remains to be seen how such claims can align to tech and data sovereignty, the document works primarily for securing for the company an image of trustworthiness.

Safaricom's report[12] is more detailed and approaches data protection and cybersecurity by contextualising them within Kenya's ICT sector and society. Safaricom, in other words, shows signs of an indigenous approach to these issues.

To begin with, data protection is introduced not from a systemic or policy-driven point of view, but rather connecting it to ethics and individual behaviour. It is this stance, in the words of Safaricom's CEO Bob Collymore, 'to inform how we address issues like customer privacy and concerns regarding customer data collection and use, which are sensitive areas that companies like ours are going to have to navigate carefully in the near future.' The framing of data protection and use in terms of ethical behaviour moves the attention away from the company itself towards the individual and considers the

tackling of these issues as the sum of a collective socio-moral endeavour, rather than a legally bounded theme which puts the company's liability at the centre of the stage.

It is also interesting to remark that 'costumer data collection and use' are presented as not today but tomorrow's concerns. This same outlook towards the future is underlined further on in the document with a list of 'future focus areas pertaining to the regulatory environment', among which we find 'ensuring data privacy and protection [and] building a culture of transparency.' These two latter points are unpacked as follows:

> Robust data protection standards have come strongly into focus for the mobile industry. We seek to maintain its high standards of transparency to ensure that customer rights are placed at the centre of our product development and service delivery.

Beyond that, Safaricom's CSR report integrates the discussion on data protection and cybersecurity by connecting it to the recently approved DPA: 'We have reviewed and developed our data security and protection policy in line with the European Union (EU) General Data Protection Regulations (GDPR), as well as the proposed Kenyan legislation, which governs the management of data going forward.' To refer to Kenya's legislation evidences an insider perspective, which in Huawei Kenya report was absent.

Last, it is worth noting that in Safaricom's report, Huawei – albeit being its major partner – is rarely mentioned, as though Safaricom strives to disjoin its image from that of the Chinese tech giant. In fact, when Huawei is mentioned, it is with reference to its training programmes, likely in the attempt to present a more benevolent partnership.

6.3. Kenya's Ministry of ICT Innovation and Youth Affairs

The website of Kenya's Ministry of ICT is the richest source of documents concerning China–Kenya ICT cooperation. As a preliminary note, it is worth highlighting that within Kenya's government ICTs are linked with youth affairs. This connection underscores the government's objective to make ICTs development crucial to youth's education. In fact, the government has launched and funded various initiatives in recent years: the Digital Literacy Programme (DLP), which is meant to make education an equaliser of digital opportunities for all Kenya children; the Presidential Digital Talent Programme (PDTP), which trains Kenyan young people to harness digital knowledge; and the Ajira Digital Programme (ADP), which mentors and encourages young people to take up online jobs, thus connecting jobs offer and demand. These initiatives are frequently heavily funded and supported by foreign ICT actors such as Huawei (for the PDTP programme) or other Western partners.

The press releases contain a variety of announcements, memoranda, guidelines and bills. The analysis focuses particularly on: (1) partnerships between the Ministry and Chinese authorities or companies, as part of the BRI; (2) projects aimed at building and transferring ICT-related knowledge and skills; and (3) documents addressing data protection and cybersecurity.

Even from a preliminary survey of all documents, the renewed importance played by US companies and administration in Kenya's ICT sector emerges, especially when contrasted with China and Chinese companies. In fact, no mention at all is made of the BRI. On the one hand, Chinese ICT companies are mentioned only twice over three years and always with regard to projects of knowledge transfer (rather than infrastructural

investments). For instance, a document dated 26 April 2017[13] deals with the Ajira Digital Platform: 'Huawei technologies and e-monitoring Africa sponsored the training. […] The Chinese ambassador to Kenya Dr. Liu Xianfa said his country provided 200 scholarships to Kenyan youth last year to pursue ICT training in China.'

On the other hand, the US administration and US companies do enter the picture more often. A communiqué concerning Facebook, released on 1 September 2016,[14] is a case in point, as it reflects, more broadly, the interests of US ICT companies in making business in Kenya and likely their willingness to contend the market to the Chinese influence. The document states that 'Zuckerberg said part of Facebook's overall strategy for Africa and Kenya is to understand what is happening on the continent and establish an entry point into the African economies for development. He said Facebook is committed to investing in connectivity.' This very general statement betrays the extent to which even a tech giant like Facebook seems to have long overlooked (for almost a decade) the potential of the whole SSA region, and Kenya's ICTs in particular. At the same time, it also shows Facebook's intention of making Kenya an entry point into the continent for its business, similar in manner to what Amazon recently announced (following the DPA approval).

As for the US administration, a document issued on 22 June 2017[15] states clearly Kenya's willingness to 'collaborate with the US in cybersecurity': 'We see the United States as key partner in the implementation of our ICT sector policy, and collaboration in areas of mutual interest such as mobile first which aims at availing ICT access to all Kenya.' So, while China and Chinese companies seem to have shifted out of focus, the US administration is enmeshed more directly in Kenya's ICT infrastructures and cybersecurity-related issues, even though this can be read as an attempt to pair with China protracted involvement in the region.

Overall, these documents attest to Kenya's proactivity in fostering bilateral synergies in matter of data protection and cybersecurity. At the same time, it is important to stress that Kenya is the only African country that has so far drafted a detailed assessment of blockchain and AI technologies. The report titled "Emerging Digital Technologies for Kenya: Exploration and Analysis" (2018)[16] is a comprehensive report edited by a taskforce of the Ministry of ICT, which details a possible roadmap for the adoption of these technologies. In this report, both the importance of building a 'National Digital Infrastructure' as well as, conjointly, the need for the Kenyan Parliament to 'pass the Data Protection Bill before the system is fully operational' are acknowledged. To this, the report adds the necessity of fostering a synergy between the government and FinTech players in order to 'understand how data are being collected and processed and enhance data sharing frameworks.' This shows the awareness of Kenya's authorities of the potentialities and risks connected with 'data knowledge', 'data divide' and related forms of data colonialism, as well as their intention to create a sovereign ecosystem of public-private cooperation at the head of which must remain the Kenyan government.

7. DPA, GDPR, POPI Act and China's cybersecurity law

The drafting of Kenya's DPA was open to suggestions and comments from stakeholders and foreign actors. The final version was approved in November 2019. These suggestions and comments will be analysed further below. To begin with, a high-level comparison

between the DPA, the GDPR, South Africa's POPI Act and China's Cybersecurity law is advanced.[17]

In many articles the DPA is very similar to the GDPR. These two documents put the physical individual at the centre of the legislative framework, by making the protection of his/her data their main concern. The primary differences between the two documents have to do not so much with the articles themselves (which are frequently taken verbatim in the Kenyan version) as with the existing legislative frame within which these same articles will be interpreted and applied. In particular, the GDPR is built upon existing laws both at European and national levels. Because of that, the document is enriched with a variety of case-by-case examples that aim at providing an operative interpretation of the most contentious articles. On the other hand, the DPA is the first law of its kind in Kenya. As a consequence, having drawn heavily from the GDPR, some concepts remain in a vacuum and need further contextualisation so that they are not open to arbitrary interpretation. This is the case, for instance, with the notions of 'legitimate interest' and that of 'exceptional circumstance'. Most of the time, these notions do not have any specific characterisation; they are definitional by default which makes their understanding and application more difficult. As signalled in one of the comments to the Act by the US Chamber of Commerce:[18]

> The EU's GDPR includes a provision allowing processing based on legitimate interest, which must be demonstrated through a rigorous, documented analysis of privacy risks and mitigations that confirms the controller's legitimate interest. The current approach is a concern from an operational perspective, and will debilitate Kenya's ability to do business globally.

Hence, the DPA could be strengthened, on the one hand, by clearly identifying cases of 'legitimate interest' in the processing of personal data and, on the other hand, by subsuming 'exceptional circumstances' under the 'legitimate interest' (indeed, this latter suggestion has been taken up by Kenyan legislators).

It is also interesting to note that in January 2020, a Kenyan court stopped the ongoing census of the Kenyan population led by public authorities (the census also included the collection of biometric data and DNA samples) due to the fact that the effective implementation of the DPA was still at an initial stage and the protection of data could not be fully guaranteed. On this point, the report on blockchain and AI by the taskforce of Kenya's Ministry of ICT also signals that 'there are fears of government intrusion. To allay such fears, [Kenya's] parliament must pass the Data protection Bill before the system is fully operational.'

On its part, the POPI Act presents some key differences from both the GDPR and the DPA. Despite contrasting views concerning the efficacy of the POPI Act, this law certainly represents a step forward in the protection of personal data within South Africa (Botha et al. 2017). Differently from the DPA and GDPR, the POPI Act is state-centric more than subject-centric. In fact, it extends towards legal persons and it only involves (physical and legal) persons within South Africa. In other words, the POPI Act is relevant to South African persons and businesses in South Africa. The GDPR and the DPA, by contrast, cover individual European and Kenyan citizens' data, extending its applicability to all businesses outside of the EU and Kenya which do business within the EU or which deal with European and Kenyan citizens' data, regardless of where the business is located.

At the same time, while in the GPDR the national authorities in charge of enforcing the law are called into question in a limited number of cases, in the POPI Act a wider spectrum

of action is granted to the information regulator. For instance, South Africa's information regulator must be notified of all data breaches, regardless of whether or not there is a high risk for the infringement of the data subject's rights and freedoms. In fact, the POPI Act considers all personal data types equal in terms of risk and importance.

As for China's Cybersecurity Law, it is stricter than the other laws concerning in particular which Chinese data can be sent out of China. Article 37 states that 'critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China.' As Belli (2017) points out, this course of action can be read as a response to 'US-dominated CBPR framework, which mandates lower levels of personal data protection for cross-border data among participating APEC countries, favour[ing] the extraction and circulation of personal data instead of empowering data subjects in other APEC countries.' More generally, while China's law limits private companies' power to collect, process and use people's data, these restrictions do not apply to the government, which, in fact, enjoys a wide spectrum of privileged lanes in monitoring the Chinese population.

To conclude this section, it is worthwhile offering an overview of the comments and suggestions received by Kenya's CA during the drafting of the DPA. These documents are publicly accessible from the website of the CA. First of all, by skimming through the documents, it is possible to see that comments and suggestions come from a variety of actors: international stakeholders (e.g. GSMA), Kenyan organisations and experts (e.g. Kenya National Commission on Human Rights, Research ICT Africa) as well as foreign actors, especially US (e.g. Amazon Cloud Service, Facebook, IBM, Microsoft, the US Chamber of Commerce, the US government). No comments and suggestions come from either Chinese companies or Chinese authorities, signalling the politics of sovereign non-interference that connotes China's approach to the development of Kenya's ICT sector.

For the sake of analysis, the comments and suggestions made by the US Chamber of Commerce and by the company Safaricom are discussed. We have already seen that the US Chamber of Commerce noted the inconsistency of the notion of 'legitimate interest' and its incongruence with that of 'exceptional circumstance'. While the formulation of 'legitimate interest' remains largely decontextualised, 'exceptional circumstance' has been taken out from the final version of the Act. Kenyan legislators have also followed the suggestion according to which 'data breaches that do not involve any material risk or harm to the individual should not need to be reported to the regulator.' In fact, now only major data breaches that put the data subject at risk need to be reported. While the earlier formulation was closer to the POPI Act, the latter aligns the DPA more closely with the GDPR.

In contrast, one major suggestion by the US Chamber of Commerce which remained unaddressed has to do with the request to get rid of 'the need for prior approval from competent authorities for international data transfer [which] is a heavy burden and is not adequate in the context of a global economy.' Such comment responds to a deregulated understanding of data flow characterising the US approach to data protection, which has not been accommodated by the Kenyan legislator.

When it comes to Safaricom's comments and suggestions,[19] it is noticeable that the company strives for a greater transparency as well as space for manoeuvring in dealing

with the lifecycle of data. Concerning the rights of the data subject, Safaricom notes that the statement contained in an earlier draft of the law, according to which 'there may be limitations on data rights of data subject when required by the law or when there are competing rights and therefore would require an assessment based on the facts and circumstances' is not detailed enough. Hence, the company proposes that the law addresses 'instances where limitations of data rights can be applied [in order to] avert ambiguity or any potential abuse of this clause.' This has in fact been done in the final version of the DPA.

On the other hand, one comment that was not taken up by Kenyan legislators has to do with the request to have more clarity over the periodical audits that the data commissioner is allowed to carry out for checking that both data controllers and data processors abide to the law. More specifically, Safaricom's suggestion that the Act should indicate: 'how often the audits of the systems will be carried out; how much notice will be given to data controllers or data processors before the audit is conducted; and the information that will be subject to audit' has been dismissed and the final version of the Act has remained unaltered on this point, leaving greater discretionally to the commissioner.

The analysis highlights how different actors defend different stakes and put forth different data interests and visions. As such, the decision of Kenya's CA to open the preliminary draft of the DPA to public assessment is certainly valuable considering that such law is the first of its kind in Kenya. At the same time, the negotiation between accepted and dismissed comments and suggestions manifests a clear institutionalised vision about how data protection should be intended in Kenya. It is then surprising, if not ironic, that the state-led census of the Kenyan population had to be suspended by a judge's decision, due to the lack of certainty about the effective implementation of the DPA.

8. Conclusion

This document review, which involved various Kenyan and Chinese actors, brought to light contrasting findings with regard to possible forms of data colonialism. Overall, Chinese actors – whether institutional or businesses – tend to withdraw from the direct provision of guidelines on data-related matters to Kenyan authorities. It remains to be seen, however, if such non-interference at the discursive level also finds a reflection in how Chinese ICT companies perform their role in the matter of tech and data sovereignty as transnational actors.

At the same time, in several documents issued by China's MOFCOM, China's leading role in the implementation of cutting-edge technologies in SSA clearly emerges, sometimes as part of international consortia. These technologies also involve data of African governmental institutions. While it is not clear who will have access to and control over these data – in other words, it is not possible to advance claims concerning a potential 'data divide' – it is a fact that the delicate issue of the storing of these data has been delegated to private foreign actors, bringing to light a contested supra-sovereign data knowledge distribution which moves beyond Kenya's direct national interests.

Although further ethnographic research is needed in order to substantiate these findings, it is noteworthy to highlight how China and Chinese companies tend to frame their international synergies in terms of cooperation and, above all, to maintain their discourses at a high level of abstraction and generality. Although complying with Asian

linguistic and rhetorical strategies, this approach can also be seen as a way for leaving room for political manoeuvring that, while not necessarily indicating opacity, could signal reticence.

From a legal point of view, Kenya's authorities have drafted and approved a solid data protection law, inspired by the EU's GDPR. And yet, it is evident that the GDPR risks becoming outdated soon, overtaken by the rapid development of those same technological means that the law aims to regulate. Moreover, the tendency seems to go in the direction of a sovereign understanding of data 'expatriation', a vision heralded primarily by China, to which other countries will be compelled to align.

Funding

This work was supported by EU Astra Program: [Grant No. 4.01.16-0032].

Notes

1. "US Ups Investment in Africa to Counter China's Influence." https://www.aljazeera.com/ajimpact/ups-investment-africa-counter-china-influence-190618203434468.html
2. *UN Document*. A/70/174 paras 26, 27, and 28(b), "How International Law applies to the use of ICTs."
3. "A New Generation of Artificial Intelligence Development Plan." https://flia.org/wpcontent/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf
4. *Protection of Personal Information Act*. https://www.gov.za/documents/protection-personal-information-act
5. *Data Protection Act*. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
6. "General Data Protection Regulation." https://gdpr-info.eu/
7. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1462012.shtml
8. http://english.mofcom.gov.cn/article/newsrelease/counselorsoffice/westernasiaandafricareport/201705/20170502573606.shtml
9. http://english.mofcom.gov.cn/article/counselorsreport/asiareport/201707/20170702617180.shtml
10. http://english.mofcom.gov.cn/article/newsrelease/counselorsoffice/westernasiaandafricareport/201711/20171102675929.shtml.
11. https://www.huawei.com/minisite/explore-kenya/pdf/huawei_kenya_csd_report.pdf.
12. https://www.safaricom.co.ke/images/Downloads/Resources_Downloads/Safaricom2019_Sustainability_Report.pdf.
13. https://ict.go.ke/innovate-ict-applications-and-software-youth-told/.
14. https://ict.go.ke/facebook-founder-call-on-ict-cabinet-secretary/
15. https://ict.go.ke/kenya-to-collaborate-with-us-in-cyber-security/.
16. https://www.ict.go.ke/blockchain.pdf.
17. It must also be remembered that in 2018 Kenya approved the Computer & Cybercrime Act, which complements the DPA.
18. https://ca.go.ke/wp-content/uploads/2018/10/US-Chamber-of-Commerce-US-Africa-Business-Center.pdf.
19. https://ca.go.ke/wp-content/uploads/2018/10/Safaricom-PLC.pdf.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Stefano Calzati is currently a postdoc researcher at TU Delft with a project on the ethics in data-driven cities. Before that, he worked at Tallinn University of Technology and as a teaching fellow at Polytechnic Institute of Milan, researching social datafication and teaching new tech literacies.

ORCID iD

Stefano Calzati http://orcid.org/0000-0002-4590-6709

References

Agbebi, M. 2018. "China in Africa's Telecom Sector: Opportunities for Human Capital Development? A Case of Huawei in Nigeria." *Human Resource Development International* 21 (5): 532–551.

Belli, L. 2017. "The scramble for Data and the Need for Network Self-determination." Viewed 10 June 2021, https://www.opendemocracy.net/en/scramble-for-data-and-need-for-network-self-determination/.

Botha, J., M. M. Grobler, J. Hahn, and M. Eloff. 2017. "A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws." *International Conference on Cyber Warfare and Security*. https://www.researchgate.net/publication/311495321_A_High-Level_Comparison_between_the_South_African_Protection_of_Personal_Information_Act_and_International_Data_Protection_Laws.

Calzati, S. 2021. "Decolonising 'Data Colonialism': Propositions for Investigating the Realpolitik of Today's Networked Ecology." *Television & New Media* 22 (8). doi:10.1177/1527476420957267.

Couldry, N., and U. Mejias. 2019. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20 (4): 336–349.

European Commission. 2020. "Policy and Investment Recommendations for Trustworthy AI." Viewed 1 June 2021, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence.

Fairclough, N. 2003. *Analysing Discourse: Textual Analysis for Social Research*. London: Routledge.

Friederici, N., S. Ojanperä, and M. Graham. 2017. "The Impact of Connectivity in Africa: Grand Visions and the Mirage of Inclusive Digital Development." *The Electronic Journal of Information Systems in Developing Countries* 79 (2): 1–20.

Gagliardone, I. 2019. *China, Africa, and the Future of the Internet*. London: Zed Books.

Gu, J., Z. Chuanhong, A. Vaz, and L. Mukwereza. 2016. "Chinese State Capitalism? Rethinking the Role of the State and Business in Chinese Development Cooperation in Africa." *World Development* 81 (May): 24–34.

Hummel, P., M. Braun, M. Treffer, and P. Dabrock. 2021. "Data Sovereignty: A Review." *Big Data & Society*. Advance online publication. doi:10.1177/2053951720982012.

Kaplan, R. 1983. "Contrastive Rhetorics: Some Implications for the Writing Process." In *Learning to Write: First Language/Second Language*, edited by A. Freedman, I. Pringle, and J. Yalden, 139–161. New York: Routledge.

King, K. 2013. *China's aid and Soft Power in Africa: The Case of Education and Training*. Cambridge: Boydell & Brewer.

Kushwaha, N., P. Roguski, and B. Watson. 2020. "Up in the Air: Ensuring Government Data Sovereignty in the Cloud." *Proceedings of the 12th International Conference on cyber conflict*. Tallinn: NATO CCDCOE Publications.

Li, A. 2008. "China's New Policy Towards Africa." In *China Into Africa: Trade, Aid and Influence*, edited by R. I. Rotberg, 22–50. Washington DC: Brookings Institution Press.

Makundi, H., H. Huyse, and P. Develtere. 2016. "Cooperation Between China and Tanzania on ICT: Fish, Fishing Tackle or Fishing Skills?" *Journal of Chinese Economic and Business Studies* 14 (2): 129–149.

Masuda, T., and R. Nisbett. 2001. "Attending Holistically vs. Analytically: Comparing the Context Sensitivity of Japanese and Americans." *Journal of Persoanlity and Social Psychology* 81: 922–934.
Mohan, G., and B. Lampert. 2013. "Negotiating China: Reinserting African Agency Into China-Africa Relations." *African Affairs* 112 (446): 92–110.
Mueller, M. 2019. "Sovereignty and Cyberspace: Institutions and Internet Governance." Viewed 1 April 2020, https://www.intgovforum.org/multilingual/sites/default/files/webform/week13-cyberspacesovereignty.pdf (last accessed 10 June 2021).
Musyimi, C., J. Malechwanzi, and H. Luo. 2018. "The Belt and Road Initiative and Technical and Vocational Education and Training (TVET) in Kenya: The Kenya-China TVET Project." *Frontiers of Education in China* 13 (September): 346–374.
Mutsvairo, B., and M. Ragnedda, eds. 2019. *Mapping the Digital Divide in Africa: A Mediated Analysis*. Amsterdam: Amsterdam University Press.
Nonnecke, B. 2016. "The Transformative Effects of Multistakeholderism in Internet Governance: A Case Study of the East Africa Internet Governance Forum." *Telecommunications Policy* 40 (4): 343–352.
Oreglia, E. 2012. "Africa's many Chinas." Viewed 1 April 2020, http://www.ercolino.eu/docs/Oreglia_Proj_AfricasManyChinas.pdf.
Roberts, H., J. Cowls, J. Morley, M. Taddeo, V. Wang, and L. Floridi. 2021. "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation." *AI & Society* 36: 59–77.
Statista. 2018. "Direct Investment Position of the United States in Africa from 2000 to 2018." Viewed 1 April 2020, https://www.statista.com/statistics/188594/united-states-direct-investments-in-africa-since-2000/.
Taylor, L. 2013. "The Scramble for Africa's Data." Available at: https://www.oii.ox.ac.uk/news-events/news/the-scramble-for-africas-data-2/.
Taylor, L., and D. Broeders. 2015. "In the Name of Development: Power, Profit and the Datafication of the Global South'." *Geoforum; Journal of Physical, Human, and Regional Geosciences* 64 (August): 229–237.
Van Dijk, T. 2008. *Discourse and Power*. Houndsmills: Palgrave.
Wasserman, H. 2018. "Power, Meaning and Geopolitics: Ethics as an Entry Point for Global Communication Studies." *Journal of Communication* 68: 441–451.
We Are Social. 2019. "Global digital report in 2019." Viewed 1 April 2020, https://wearesocial.com/global-digital-report-2019.
Wen, Y. 2021. *The Huawei Model: The Rise of China's Technology Giant*. Urbana: University of Illinois Press.
Winseck, D. 2017. "The Geopolitical Economy of the Global Internet Infrastructure." *Journal of Information Policy* 7: 228–267.
Xu, Y.-C. 2014. "Chinese State-Owned Enterprises in Africa: Ambassadors or Freebooters?" *Journal of Contemporary China* 23 (89): 822–840.
Yu, H., and T. Goodnight. 2020. "How to Think About Cybersovereignty: The Case of China." *Chinese Journal of Communication* 13 (1): 8–26.