7

A Modulated Approach to Digital Sovereignty

Exploring Huawei-Led Smart City Initiatives in South Africa and Italy

Stefano Calzati

7.1 INTRODUCTION

This chapter is framed within the broad and multilayered issue of China–Africa relations in connection with Information and Communication Technologies (ICTs). At such a juncture, it becomes particularly relevant to unpack the geopolitical and tech-dependent power relations between two BRICS countries – China and South Africa – in the context of smart city initiatives. The Huawei OpenLab in Johannesburg is chosen for the study, with a similar initiative from Cagliari – the capital of Sardinia, Italy – used as a comparison. The goal is to explore the extent to which bilateral cooperation between China and South Africa in constructing smart cities can be said to empower all actors involved, especially South African actors and citizens, rather than (re)producing power asymmetries within a South–South geopolitical scenario. Further, the chapter offers a better understanding of how Huawei-led smart city initiatives are conceived by scrutinizing their discursive framing, exploring the extent to which the tech giant actions can be deemed as an example of corporate digital sovereignty (see Chapter 1). The chapter also sheds light on the governance model of these smart city initiatives, with particular attention paid to Huawei's partnerships and the management of data lifecycle.

Today, South Africa has one of the most advanced ICT markets in the African continent, largely due to interventions and investments by foreign partners, both Western and Chinese. Chinese tech giant Huawei, in this regard, represents a key actor. Huawei has entered South Africa's ICT market since early 2000s and gained an increasing centrality over the years. In this context, Huawei OpenLab is a paradigmatic example of Chinese-led multi-stakeholder tech initiative whose goal is to conceive, develop, and implement smart city solutions (e.g., face recognition, mobility sensors, diffused Internet of Things (IoTs) for pollutions monitoring, traffic management, and building energy

savings) in and for the city of Johannesburg. For comparison, this initiative is juxtaposed to a similar one, the Joint Innovation Center (JIC) in Sardinia, Italy, of which Huawei is also a key stakeholder. This comparison highlights the similarities and differences between the two initiatives in discourse and governance.

The chapter is structured as follows. First, it briefly discusses methodology and the documents reviewed for the study, followed by an outline of the theoretical framework along three main axes: (1) the role of China in Africa in the context of ICT development; (2) current competing visions about internet (geo) governance through the lenses of "digital sovereignty" and "data colonialism"; and (3) a critical review of the concept of "smart city." Then, the author introduces the two case studies: Huawei OpenLab in Johannesburg and the JIC in Italy, highlighting major discursive and governance-related similarities and differences. Lastly, the chapter draws some conclusions, linking the major findings from the case studies to the theoretical framework (see Chapter 1), highlighting the strains and exchanges when different forms of digital sovereignty – especially state and corporate ones – may clash or converge.

7.2 METHODOLOGY

Huawei OpenLab in Johannesburg and the JIC in Cagliari were chosen as case studies due to three considerations. First, Huawei played a key role in both initiatives as a main actor and provider of technological support. Second, these two initiatives aim to achieve similar goals in smart city solutions. Third, the comparison offers an interesting opportunity to triangulate and explore the activities of Huawei in different settings, notably in a country part of the BRICS and in a country of the "Global North." The study examines a series of documents, reports, and press releases to provide valuable insights into the inner workings of these two initiatives as well as the development models they represent. The analysis helps unveil the discourses surrounding the two Huawei-led initiatives as well as the management of data lifecycle and the smart solutions developed. It should be noted that the analysis here does not draw from direct feedback from Huawei. Despite the author's attempts to interview Huawei representatives for the two smart city projects, the Chinese company did not provide a response.

7.3 THE ROLE OF CHINA IN AFRICA'S ICTS AMONG SOFT POWER, DIGITAL SOVEREIGNTY, AND "SMART" DEVELOPMENT

7.3.1 China in Sub-Saharan Africa

Currently, Africa is the continent with the strongest growth in digital connectivity worldwide: more than 5.2% of annual growth rate in mobile subscriptions and 8.7% in internet users between 2018 and 2019 (We Are Social, 2019). Despite the remarkable advancement, internet penetration in the continent

remains uneven across regions. In North and South Africa, at least 50% of the population have access to the internet. However, in East and West Africa, the percentages of penetration are lower, at 32% and 41% respectively, with Central Africa reaching only 12%.

Sub-Saharan Africa (SSA) represents a crucial crossroad along the New Maritime Silk Road. A set of major techno-infrastructural investments, the New Maritime Silk Road is part of the Belt and Road Initiative, and it aims at connecting Mainland China to Europe via Hong Kong, India, and Africa. Chinese ICT-related investments in SSA span across all African regions (Oreglia, 2012): eastern (e.g., Kenya, Ethiopia, and 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, have initially focused on infrastructures (backbone and last-mile cabling), while over the last decade, they have shifted toward knowledge transfer, cloud computing, artificial intelligence solutions, and smart city projects.

Different from Western powers, China has been said to exert "soft power"[1] on the African continent by promoting investments "with no strings attached" (Gagliardone, 2019). At least in rhetoric, China is committed to developing African infrastructures and services by fostering agreements that keep African business partners, local authorities, and workers involved, tailoring investments for their needs. In various international documents, China's relationships with SSA countries are discursively shaped as peer-to-peer forms of collaboration rather than top-down aids (King, 2013). However, the extent to which China's and Chinese companies' commitment to fostering vibrant ICT markets in SSA aims to empower African actors instead of subjecting these actors to forms of soft colonization is still being debated. For instance, not only do Chinese individuals tend to occupy managerial roles in Chinese–African partnerships, but knowledge transfer to Africa is also contested (Makundi, Huib, & Develtere, 2016). Some scholars have found that effective cooperation on a peer-to-peer basis is limited (Cheru & Obi, 2010; Gagliardone, 2019; Shen, 2013; Taylor, 2006). On the other hand, it is also recognized that China's involvement in Africa does produce sharing and collaboration with local communities, helping to foster a positive perception of Chinese expats by locals (Agbebi, 2018; Anshan, 2007; Musyimi, Malechwanzi, & Luo, 2018). In a more balanced summary, King (2010) notes that "there is recognition by Chinese officials that the transfer of Chinese labor practices can lead to friction, and they provide advice about this. On the other hand, there seems to be a good deal of admiration for the Chinese determination to start and finish a job on time and on budget" (p. 494).

[1] "Soft power" is the term that Chinese authorities adopt when describing their engagement with and in foreign countries, especially low-to-middle-income countries (LMICs). It is a broadly conceived form of power based not much on military force or economic agreements (although economy does play a role), but on diplomacy and culture as keys to establish relations across the world (see, for instance, Bodomo, 2009; Fijalkowski, 2011).

Hence, the idea of a homogenizing "soft power" exerted by China on Africa calls for contextualization. In fact, such label can hardly account for the variety and complexity of Chinese investments in the African continent. It would be too simplistic to consider Chinese companies as the *longa manus* of the Chinese government in Africa, insofar as the diverse, multilayered initiatives put forth by various Chinese actors – diplomats, private companies, state-led companies, trade intermediaries, and so on – can often have competing agendas. For instance, Xu's research (2014) shows that the Chinese Ministry of Commerce and Ministry of Foreign Affairs tend to have different approaches toward their foreign partners. Gu and colleagues (2016), in turn, observe that "the Chinese state has engaged in unprecedented economic diplomacy in Africa" (p. 25), implying a flexible approach of Chinese authorities to African economies and societies, instead of presupposing a uniform top-down relationship. This is in line with Li's argument (2008) that China's paradigmatic approach to Africa has shifted from "economy serving diplomacy" to "diplomacy serving economy," manifest of China's soft power in developing regions of the world.

Besides a pan-Africa diplomacy framework, China is increasingly committed to fostering bilateral agreements with individual African states. Gu and colleagues (2016) note:

> this [diplomacy] has two aspects: multilateral (pan-African) and bilateral (state-to-state) diplomacy. The former is driven through the FOCAC [Forum on China-Africa Cooperation] framework, a dialog and institutionalized 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 (p. 25).

From a Chinese perspective, the goal is to adapt to each context without imposing an agenda, while seeking a convergence between China's own interests and those of local actors. On this point, Gagliardone (2019) 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" (p. 56). For this study, the involvement of the Chinese tech giant Huawei in South Africa is of special interest.

Huawei is the major Chinese ICT actor in South Africa. It entered the country in 1999, just one year after its arrival in Kenya, which marked the beginning of Chinese investments in SSA's ICTs. Huawei's presence in South Africa has grown considerably over the years. Huawei's sales in Africa reached $4 billion in 2012. As for June 2021, Huawei compete with Samsung to be the leading mobile phone provider, after having already overtaken Apple (Statista, 2021). In addition, Huawei has also committed to delivering ICT training through its Huawei Authorized Information and Network Academy (HAINA), which has so far mentored more than 50,000 graduates.

In early 2019, Huawei played a crucial role in the rollout of the first 5G commercial network in South Africa, together with Rain, the country's mobile

data-only network operator. In 2020, following the US ban of Huawei, South Africa's government confirmed its support to the Chinese company. Currently, Huawei is at the center of a project of techno-renovation of the city of Rustenburg, near Pretoria. Famous for its mines, the city has been identified as the target of major investments and deployment of smart city solutions.

7.3.2 Unpacking (Cyber) Power Relations

The genealogy of China–Africa relations in the ICT realm can date back to the 1970s. Riding on the wave of Third-Worldism, commercial and political partnerships between China and states of the Non-Aligned Movement, that is, countries not directly subsumed under either of the two superpower blocs centered around the United States and USSR, thrived. Half a century later, the geopolitical scenario has radically changed, with the eclipse and metamorphosis of the former Soviet Union into Russia and China's rise on the global stage as a leading commercial, technological, and political power. On the other hand, African countries experienced substantial demographical and technology-led economic growth, although uneven across the continent. Today, China, Russia, and South Africa – the most economically developed African country – together with Brazil and India, are part of the BRICS alliance composed of some of the largest emerging economies of the world.

The rise of China and the emergence of the BRICS bloc challenge conceptual frameworks and theories of the Global North and Global South as well as of a world system divided into "the first world," "the second world," and "the third world." It has been contested that such epistemological categories have their limitations and even harmfulness vis-à-vis the goal to account for and put forth a truly inclusive internationalist perspective in which all actors – nations, public institutions, private companies, and people – are granted a proactive (and not only reactive) agency. While such categories might be useful for identifying patterns of socioeconomic imbalances, they nonetheless tend to oversimplify stratifications and tensions cutting through these geographies, thus fundamentally overlooking the unique histories, internal and external power relations, and cultural differences affecting the involved countries. This has become more pronounced in global trade and ICT infrastructures, consolidated around China and the US. For instance, China's involvement in Africa and Europe, via the proxy of Huawei's investments in both continents, requires not only a contextual assessment of technological and geopolitical power relations between the "superior" and the "subaltern" actors but also a paradigmatic rethinking of the theoretical basis of such assessments. As Wen (2021) writes in his book *Huawei's Model*, "the development of the global economy has been characterized by the transition toward transnationalized digital capitalism, within which information and communications technologies have increasingly played a pivotal role in restructuring the global capitalist system" (p. 12). To foster generative

discussions and debates and institute practical policies, it is important to subject the new global map of power relations to a critical examination.

This entails the undoing of dichotomies such as global–local, especially when it comes to issues of "data colonialism" (Couldry & Mejias, 2019) and "digital sovereignty" (Belli, 2017) as well as conceptual binaries such as "multi-stakeholderism–multilateralism" (Nonnecke, 2016) in the realm of internet governance. In this respect, Wasserman (2018) observes that what is at stake is 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' in communications" (p. 448). What has emerged bears resemblance of federated forms of technological globalization – contested internally as much as externally – in which the circulation of data, tech expertise, innovation, and policies can be prompted or hindered by competing discourses, actors, and agendas part of different ecologies *at once*.

Elsewhere (Calzati, 2020a), I have noted that any discussion on data colonialism can be fruitful only to the extent it is contextualized and historically thickened. Otherwise, the risk lies in reifying the same power asymmetries that the notion of data colonialism aims to uncover. For instance, while US corporations tend to dominate internet services and software, the "ownership" of the internet infrastructure's components sees an imbrication of actors. A case in point is the transpacific FASTER cable system between the United States and several cities in Japan, China, and Korea. This is a major infrastructure jointly developed by Chinese, American, and South Asian private companies, including Google, China Mobile, China Telecom, SingTel, KDDI, and Global Transit. It is evident that within such a multilayered, entangled scenario, the very concept of digital sovereignty risks losing its epistemological validity if it is not anchored to the ground: each "North" contains its "South," each node exists as an extension of its edges, each network is traversed and repeatedly remolded by contingent (data) interests.

When ICTs are framed within a geopolitical North–South perspective, the risk of new forms of power asymmetry emerges. Studies have shown the "misalignment" between the internet as a commons infrastructure and the legitimacy of sovereign powers (Mueller, 2019) as well as the shifting toward a multipolar scenario (Winseck, 2017) in internet governance. Traditional categories such as "market" and "state," "national" and "international," and multi-stakeholderism vs. multilateralism may no longer be sufficient to account for such changing and complex realities. For instance, as Yu and Goodnight (2020) 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" (p. 13). Hence, digital sovereignty, data colonialism, and also digital self-determination can be best regarded as macro-entangled dimensions that contest and resist linear (agent-structure) readings.

SSA's digital transformation is increasingly associated with a new "scramble for Africa" (Taylor, 2013) aimed at controlling the deluge of

ICT-derived data from the continent. There exists a grave risk due to the lack of agency provided to African institutions and African peoples when it comes to their own digital transformations. Studies have shown a colonially tainted asymmetry between Africa and the developed countries (Mohan & Lampert, 2013; Taylor & Broeders, 2015), which relegates African countries and people to a subaltern role. Given the power asymmetry, scholars have emphasized the urgent need to "Africanize technology" (Mutsvairo & Ragnedda, 2019, p. 22) to empower African actors and ICT users. However, it remains to be seen whether such asymmetry also affects South–South power relations, such as those among BRICS countries. Thus, this study seeks to investigate the tensions informing the smart city initiatives led by Huawei in Johannesburg and compare them with similar projects developed in the Global North, of which Italy is part traditionally. More broadly, the study assesses the indigenous *and* transnational entanglement of digital sovereignty and data colonialism and how such double-sided articulation impacts an effective emancipation of African (and Italian) actors.

This brings us to explore the concept of "digital sovereignty," deeply intertwined with "data colonialism." Historically, the notion of sovereignty emerges at the intersection of exclusive authority and territoriality. This chapter will show that, when contextualized, the concept can be usefully adopted to understand Huawei's initiatives across the globe.

According to Kushwaha and colleagues (2020), "digital sovereignty" is a concept that is midway between the broad idea of "technological sovereignty" and the narrow idea of "data sovereignty." In her speech in February 2020, the President of the European Commission Ursula von der Leyen defined digital sovereignty as the capability "to make its own choices, based on its own values, respecting its own rules" in the field of tech (von der Leyen, 2020). At the heart of the matter is control over data and/or tech infrastructures (Hummel et al., 2021). More concretely, to assess the soundness of the concept, it is necessary to put it in context. Apart from those countries able to chart their own course of economic and technological developments – those which can "consider creating a national programme to foster and promote nationally headquartered companies to invest in creating and offering CSP services within their country" (Kushwaha, Roguski, & Watson, 2020, p. 60) – for the majority of countries around the world, especially LMICs, the risk of being co-opted by major global powers, private or public, in their infrastructures and services is extremely high. As de Nardis (2014) pointed out, technology governance becomes part and parcel of geopolitics when power relations heavily influence how a technology is developed, implemented, controlled, shared, and used. Such technology, in turn, impact people's lives – both individually and collectively – in creating or eroding values at social, economic, cultural, environmental, and institutional levels (Cardullo & Kitchin, 2019; Micheli et al., 2020).

This type of cyber-geo-governance has peculiar features. One such feature is the increasingly federated forms of transnational technologization, with China gaining a central role in shifting global power relations. Thus, it should

not surprise anyone that the European Union (2019) warned against the "digital dependency on non-European providers and the lack of a well-performing cloud infrastructure respecting European norms and values." This also means that "states will increasingly face difficult policy decisions with regard to deciding how best to balance competing sovereign interests" (Kushwaha, Roguski, & Watson, 2020, p. 58). For instance, Wu (2021) notes that the US *Cloud Act*, passed after China's adoption of its *Cybersecurity Law*, is a typical example of a law that, under the guise of data localization and protection, has an eminently transnational character. Yet, such a law might also have undesirable commercial repercussions, especially for the US's European allies.

Given such scenario, it is certainly insightful to examine the power relations binding two BRICS countries – China and South Africa – through the lens of digital sovereignty (and colonialism), as applied in studying a smart city project in Johannesburg (and one in Cagliari for comparison). The way in which the Chinese tech giant Huawei approaches different contexts and fosters multi-stakeholder partnerships for developing smart city solutions sheds light onto how the concept of digital sovereignty gets challenged and rearticulated differently in reality.

7.3.3 Smart Cities: A Critical Review

Despite the fuzziness, multiple interpretations, and sometimes abuses of the term "smart cities," the notion has come to signify primarily the fostering of highly efficient urban spaces based on ICTs and the gathering of IoT-related data. Plus, the development of smart cities has occurred at a time of increasing responsiveness to the need for sustainability of the whole built environment. The International Telecommunication Union (ITU)'s Focus Group on Smart Sustainable Cities (FG-SSC 2016) defines smart cities as follows: "A smart sustainable city is an innovative city that uses ICTs and other means to improve the quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects."

With nuances from report to report, such a definition has become the standardly accepted idea of what a smart city should be and do, ideally. However, what counts as "quality of life," "efficiency," and "competitiveness" and whether such features are desirable, compatible, and truly beneficial to citizens remain open questions. Many smart city initiatives have increasingly been shaped by a techno-optimism ethos that tends to overlook the realpolitik behind the implementation of tech-based solutions in the urban environment. As Angelidou (2017) notes in her critical review of several case studies, "most smart city strategies fail to incorporate bottom-up approaches, are poorly adapted to accommodate the local needs of their area, and consider issues of privacy and security inadequately."

The hyperefficiency that the smart city is meant to realize conflates "easiness of use" with "living wellbeing." The idea that a city is good to live in when it is easy to navigate betrays the underlying technological rationale of

an urban space "founded on the basis of utopian 'clean and orderly' pervasive computing" (Viitanen & Kingston, 2014, p. 807). Things, however, are more complex. Oftentimes, how, where, and what smart technology is deployed contributes to widening socioeconomic disparity, precisely because technology is already epistemologically loaded with the same principles and rationalistic logics that guide its development and which, in turn, technology reinforces.

Secondly, the idea of a city's smartness often conceals economic drives and interests. Turning a city into a clean and orderly space on the ground of an accrued attention to citizens' needs also implies shaping the city as a space to be *used*. The smart solutions adopted in cities are often offered by private companies and co-opted by market forces (Mann, Mitchell, Foth, & Anastasiu, 2020), which then take the lead in defining the normative ideas of what counts as "smart," that is, something that they can profit from. It is no surprise that given tech innovation is primarily led by private firms, the underlying business model of today's smart cities is one that produces power asymmetries at various levels: not only does it subordinate public spaces and actors to private ones, but it also turns citizens into consumers.

Thirdly, it is not rare to find the concept of smart city coupled with that of "safe city," via the creation of a network of diffused technological solutions, among which video cloud, facial recognition, and tracking sensors, which overlaps to the citizen's being-in-the-city as a ghostly shadow. A safe city, then, can be realized above all as a "monitored city" in which technology can be used in exploitative (and often lucrative) terms. In this sense, "safe city" is to be found somewhat in the middle between "care" and "control" (Lyon 2007): the extent to which safety morphs into surveillance rather than enhances people's wellbeing is an economic-political matter closely linked to how smart technologies are developed, deployed, by whom and for which purposes. As Deleuze (1992) acutely points out by distinguishing between an old "disciplinary" city governance from a new "control" one: "the disciplinary man was a discontinuous producer of energy, but the man of control is undulatory, in orbit, in a continuous network" (p. 4). The citizen of smart cities is metamorphosed into a trace-leaver. "Any one of us," Bratton writes (2016), "is (or could be, or should be) less a political subject of this one city – London, Mumbai, Shanghai – but of the City, of the globally uneven mesh of amalgamated infrastructures and delaminated jurisdictions" (p. 152). The smart city is an agglomeration that transcends borders and specificities to impose a new layer of global technologized living space that demands to be unpacked in all its internal complexities.

7.4 HUAWEI OPENLABS IN SOUTH AFRICA AND THE JOINT INNOVATION CENTER IN ITALY

Over the last few years, Huawei has launched a number of OpenLabs around the world. Except the OpenLab in Suzhou, Mainland China, which opened in 2012, the others are all abroad, for example, in Johannesburg (April 2017),

Istanbul (December 2017), Paris (April 2018), Moscow (April 2018), and New Delhi (October 2018).

These initiatives are conceived as hubs where, based on shared infrastructures and facilities provided by Huawei, various stakeholders can converge for developing and testing innovative technological solutions for the "smartening" of the urban environment. It is significant to delve into the governance model that regulates the relations among the OpenLab's stakeholders in order to understand how data are put to use, by whom, for whom, and for which purposes.

More specifically, while the vision of sharing hardware, software, and tech know-how is clear, it is worth exploring how the data lifecycle is managed as well as how the tech solutions developed address issues of cybersecurity and local actors' empowerment. This same approach also applies to the second case study – the JIC in Cagliari, Italy – of which Huawei is also one of the leading actors in constructing tech infrastructures, facilities, and know-how.

7.4.1 The OpenLab in Johannesburg

The OpenLab in Johannesburg is interesting as it was one of the first hubs to be opened by Huawei outside Mainland China and it remains the only one of its kind in SSA. The initiative hopes to bring together various stakeholders to create a synergic model of tech innovation with an impact at the urban level.

As stated in the press release published at the occasion of the launch of the OpenLab (Huawei, 2017), "Huawei will provide the data centre facility, hardware and software infrastructure and technical team while the partners will contribute ideas, products and human resources" with the goal to "test and customise a broad range of solutions under the umbrella of safe cities and smart grids." Here the equation of smart city *as* safe city returns, a *leitmotif* in Huawei's discourses on technological solutions applied to urban environments.[2] On its website,[3] Huawei elaborates:

> The center focuses on four capacities: joint innovation, partner development, solution development, and industry experience. Johannesburg OpenLab works together with global, regional, and local partners, concentrating on Safe City, Smart Grid, and

[2] In a 2020 white paper issued by Huawei specifically dedicated to smart cities, the term "safe city" appears seventeen times over nineteen pages. The concept is deeply entrenched with that of "smart city" and is considered de facto as a driver to realizing the latter. More to the point, the document unfolds an all-monitoring characterization of "safe city" as that which "uses ICT to predict, prevent, and reduce crime; address new and emerging threats; improve emergency/disaster planning and response. (…) Safe Cities us[e] a variety of tools such as advanced analytics, social media, collaboration and information sharing tools, and mobile technologies to support (…) local law enforcement and policing, and the justice and corrections system including local courts, locally operated jails and prisons, probation, community corrections, and parole." The wide and diverse application of smart solutions raise concerns over their impact on individual rights and freedoms, especially when the "implementer" is a private company in a foreign context.

[3] See https://e.huawei.com/en/partner/openlab/johannesburg.

Smart City solution [sic] to develop competitive solutions for industrial customers. Johannesburg OpenLab supports the demonstration of Safe City converged command, video cloud, and facial recognition scenario.

Overall, the presentation of the OpenLab is rather minimal and factual. The description of the smart city projects is kept at a high level of abstraction and any form of qualitative assessment is avoided. While the Lab is open for "cooperation/consultation," Huawei's representatives declined to respond to this researcher's request for interviews. Such an approach seems symptomatic of a corporate strategy that, while leaving the doors open to a wide spectrum of partnerships, remains problematically vague over the concrete projects and the effective results of the Lab toward a broader audience. In fact, the stress on "industrial customers" is indicative that the smart city's solutions developed, albeit having an immediate impact on the local communities, are kept among a small cohort of actors.

Further, the concept of "safe city" is projected to be realized through a network of tech solutions that include video cloud and facial recognition. "Safe city," therefore, can be intended above all as "control city" to the extent to which the restriction of access to the OpenLab mainly to industrial customers and lack of community presence cast doubt on the public agency and publicly beneficial impact of the solutions developed by the Lab.

After operating in Johannesburg for six years, the OpenLab provides few details about the extent tech solutions developed within the Lab have been deployed. Nor has it openly addressed concomitant issues of privacy and data protection as well as other potential unintended consequences such as different forms of bias and discrimination. While there is no legal obligation for any private tech company to explore and account for these concerns outright, from a cyber-geopolitical perspective, these issues remain front and center of large-scale public projects and beg for more transparency.[4]

Such technological side effects are of particular relevance in a multiracial context such as South Africa, to the point that Kwet (2019) speaks of the risk of "AI-powered apartheid." Yet, Huawei does not openly address such concerns related to the activities and solutions of its OpenLab. Instead, it tends to favor a purely technically optimistic presentation of the smart city initiative, seemingly oblivious to the intrinsic social facets of technology and its governance. In the words of Arsène (2018), "the very sensitive character of these technologies and the geopolitical stakes paradoxically lead to a certain level of secrecy around the technologies that are supposed to bring more transparency" (p. 58).

More information on the smart city solutions envisioned and developed by Huawei can be found in its 2018 Corporate and Social Responsibility

[4] Not rarely, Corporate Social Responsibility initiatives are adopted by companies as brand-enhancing strategies for compensating the lack of approach to the development of on these issues and present the companies' goodwill to the population see (King, 2013; Makundi, Huib, & Develtere, 2016).

(CSR) report, which describes the ambitious project in the mining city of Rustenburg to be turned into a smart city:

> A world-class city where all communities enjoy a high quality of life, and one that is interconnected, energetic, healthy, green, friendly, secure, smart, prosperous, efficient, and sustainable. (…) To efficiently implement this project and build a smarter Rustenburg, the municipal government has picked a number of partners, including South Africa's ICT and financial technology company Electronic Connect, Sanchuan Water Meter Co., Ltd., intelligent transportation system provider Xiamen Lenz Communication Inc., and Huawei (p. 34).

Unlike the limited information about such smart city projects made available on its OpenLab's website, Huawei's CSR report puts forth an overinflated discourse on smart cities. It presents the upcoming renovation of the city of Rustenburg as an all-encompassing masterplan that will significantly uplift the quality of citizens' life, characterizing the "smart city" as the "optimal city" with such intrinsic qualities as "security," "interconnectedness," "prosperity," and "sustainability." Yet, no further insights are provided in support of these projected values or how they are realized through specific technological solutions.

To put things into perspective to assess a smart city's socioeconomic-ethical implications, it is worth looking at a similar project initiated in 2015 by the Chinese Development Group Zendai, which proposed a plan to turn the neighborhood of Modderfontein (east of Johannesburg) into a smart city. After two years, the project fell into disgrace due to the conflicting visions between the company and the municipality of Johannesburg. The city required at least 5,000 affordable homes to be included in the plan, while Zendai insisted on building luxurious housing, offices, and venues.

This case pulls aside the curtains, allowing a glimpse into the realpolitik behind smart cities. The label of "smart city" often conceals rather than reveals how the smartening of a city can lead to diverging interests among the actors involved, thus raising concerns about the socioeconomical sustainability of the solutions proposed. In other words, the benchmark against which to assess smart city solutions cannot be solely their tech feasibility or efficiency, but also their concrete economic, cultural, and social impacts on the local communities. The Modderfontein case epitomizes the extent to which smart initiatives, especially those led by private companies only, risk reinforcing or exacerbating existing socioeconomic inequalities and demand a thoughtful assessment involving all parties before being implemented.

One further aspect to be stressed is that both cases – Modderfontein and Rustenburg – entail a synergy of local and foreign actors, both public and private, concretizing the idea of cooperation among Chinese and African actors discussed earlier. However, the scenario is much different when it comes to Huawei OpenLab that provides few details about its "global, regional, and local partners." Among the publicly listed partners involved in

the OpenLab are[5]: (1) a French and a Chinese company focused on railways infrastructures, (2) a UK firm that offers consulting digital services (both business-to-consumer and public-to citizens), (3) three Chinese tech companies focused on smart city solutions and smart grids for energy efficiency and facial recognition; (4) a German and a Danish company in the field of surveillance and tech safety solutions; (5) a Swedish IT company that provides smart city solutions; (6) two US tech companies; and (7) a French company involved in digital identity and security solutions.

On the one hand, the OpenLab clearly can attract an array of private partners. On the other, the glaring absence of South African partners, either public or private, is significant. This is particularly striking because the focus of the Lab on smart city solutions by default bears a local outreach. The lack of local community representation is thrown into sharp contradiction considering South Africa's Minister of Communications and Digital Technologies, Stella Ndabeni-Abrahams' recent remarks: "South African initiatives are likely to be successful only if they happen in an integrated manner" (SA News, 2019). Lacking integration with local stakeholders, Huawei OpenLab risks compromising the digital sovereignty of South Africa and its citizens, severely limiting the potential beneficial effects of its tech solutions.

Overall, it is possible to identify four major actors leading tech innovation initiatives in South Africa: (1) foreign ICT companies (mainly Western and Chinese); (2) South African ICT companies; (3) South African governmental bodies; and (4) South African universities. While a number of tech hubs and incubators witness the collaborations among these four types of actors (e.g., The Innovation Hub in Pretoria and Thsimologong Precint in Johannesburg), Huawei has favored a proprietary, corporate approach to the development of the OpenLab, which makes the development of the solutions potentially disempowering for South African actors.

7.4.2 The Joint Innovation Center in Cagliari

For comparison, this chapter also examines the JIC launched in Cagliari, the capital of Sardinia, at the end of 2019. A comparative analysis aims to produce more insight into the governance models of Huawei's smart cities initiative around the world. Similar to the OpenLab, the JIC focuses on the collaborative development of tech solutions to turn the Italian city of Cagliari into a smart city. In this case, too, Huawei is the leader of the initiative, together with CSR4, the Centre for Advanced Studies, Research and Development of Sardinia, which is an interdisciplinary pole of technological innovation whose sole public shareholder is the regional agency Sardegna Ricerche. In this case, Huawei joins forces with the main public actor in the region in technological R&D. Beyond that, other partners of the JIC include:

[5] https://openlab.huawei.com/portal/en-us/pages/earth/johannesburg.html.

(1) an Italian company that develops core IT infrastructures through cloud computing; (2) an Italian company that offers hardware and software solutions for the IoTs including cybersecurity services; (3) an Italian company that develops network and connectivity solutions; and (4) an Italian firm focused on IT projects and installations.

Although neither Huawei Italy nor CSR4 were available for interviews before the end of the partnership (expected at the end of 2021), on the JIC's (2020) website,[6] the media section provides valuable information from the stakeholders involved in the initiative. As Massimo Carboni, coordinator of the JIC for Sardegna Ricerche, states: "the project is a collaborative venture of three main actors: CSR4, which provides skills and know-how, Regione Sardegna, which defined the vision and mission of the initiative, and ICTs companies, among which Huawei is the main partner, plus other six SMEs." From this perspective, the initiative has a "indigenous" component, especially in comparison with Huawei OpenLab in Johannesburg. This, however, does not provide a clear indication of the governance behind the initiative, that is, the power relations among the actors when it comes to the data lifecycle's management. The JIC website states:

> The objective of the project is the realization of an experimental infrastructure with which new technologies will be developed for widespread connectivity on a metropolitan scale (…) aimed at solving problems related to smart cities, the experimentation of widespread sensors for the acquisition of large amounts of data that will be managed through the development of architectures for Open Data and Big Data, the testing of systems for city safety (safe city) and the study of new generation e-LTE systems.

Resonating with the mission of Huawei OpenLab in Johannesburg, here too the stress is on "smart city" as "safe city." Mentioned on the JIC's website is the development of an array of sensors for vast collections of data: video cameras and distributed urban tracking systems such as "face recognition, plate recognition, intrusion detection, behavioural analysis, etc." The idea of amassing large amounts of data by means of innovative tech solutions is again framed within a techno-optimistic discourse of "improvement of citizens' quality of life" and even of "increase [of] both cultural and educational mutual knowledge" for all the companies involved. Hence, the discourse supporting the initiative tends to present a win-win situation, which echoes the idea of peer-to-peer cooperation typical of Chinese companies' "going out" efforts. As Lidia Leoni in charge of strategic partnerships at CSR4 points out, what counts the most is the ultimate goal rather than the means: "it is extremely important to have an idea of what is happening everywhere (…) by connecting data which would remain otherwise unrelated." While such a functionalistic approach of the tech cooperation between Huawei and CSR4

[6] www.jicsardegna.it/en/. If not differently specified, all subsequent quotes are taken from the website.

adheres to an understanding of the city as a space to be mapped in real time for increased control and efficiency, overlooked are issues of realpolitik and people's safety and security behind data lifecycle. Missing from JIC's public discourse is clear communication of which actors and under which obligations are responsible for the management and security of data and potential data breaches.[7]

What we do know, via the media releases, is that through the deployment of these smart city solutions, the JIC aims to build an intelligent operation center (IOC), that is, a centralized platform on which all data converge for the formation of what is called the "data lake." Vincenzo Strangis, director of smart cities and innovation at Huawei, defines the IOC by resorting to the human–machine metaphor: "the IOC is like the brain of the human body connected to the nervous system, for us the nervous system is that which comes from all the sensors that are present in the city." The platform is based on open-source technologies on which vertical applications can then be implemented. The open-source choice favors the potential arrival of (new) partners by lowering barriers to access and enhancing interoperability. Namely, the IOC is based on a logic of federation of the data, which maximizes data's capitalization through the creation of the data lake by an array of different actors. On this point, Strangis specifies that "the infrastructure gravitates around the data center, that is, the storage technology that allows for the emergence of the data lake, to which all the various stakeholders will contribute by making available *to us* the data coming from their applications [emphasis added]."

The fact that the JIC is led by a public stakeholder should prioritize, in principle, the public interest in using data to tackle social and environmental issues in the urban context instead of profit-only objectives. In a way, data are expected to be repurposed for the benefit of the local community. On the other hand, however, the network through which these data run is owned by Huawei, making the Chinese company an inalienable actor of the whole initiative (the "us" used by Strangis is emblematic). And this does raise concerns over the risk of tech dependency voiced by the European Union recently. To borrow the well-established and somewhat questionable metaphor of data as "the new oil," the IOC could be seen as the public-led data refinery and Huawei as the owner of the pipeline through which the oil runs. On the JIC's website, it is also reported that the goals of the initiative are:

[7] On this point, it is worth highlighting the results of a longitudinal qualitative analysis about Huawei's communication on social medial platforms (Calzati, 2020b). From the study, it emerges that the company's lack of responsiveness to users' comments on Facebook and Twitter is the results of a precise communicative strategy rather than the lack of monitoring of interactions. In fact, once the company feels the need to rectify/preserve its online image (such as when accused of being owned by the Chinese's government), it shows a very proactive attitude in creating online interactions.

To experiment and demonstrate on the field the effectiveness in the implementation of a private network, which exploiting a high data transmission capacity, allows the study of new solution for the benefit of the city community and of public and private institutions. We will then proceed with the experimentation of sensors able to detect data that will be processed by other parts of the project. Prototypes of mobile devices operating on the frequencies of the private e-LTE network provided by Huawei will be tested in the field.

E-LTE networks are also at the core of the OpenLab initiative in Johannesburg. The corporate-based conception of the "pipeline," which makes the collection of data possible, puts Huawei in a privileged position, whether the solutions developed will concretely and beneficially impact on the community and/or other partners or not. At stake, it is not to contest such conception – these solutions might really improve the quality of citizens' life – but rather to shed light on the trade-offs in terms of digital sovereignty that the governance model of these initiatives entail. Notably, compared to the South African case where the joint venture capitalized exclusively on foreign actors, the JIC enacts a multinational approach that sees Huawei establishing not only commercial ties but also institutional partnerships (e.g., the CSR4) with local actors. However, such multinational approach should be dutifully scrutinized from a cyber-geopolitical perspective, considering that, as Wen (2021, p. 31) notes, Huawei's activity "has been closely entangled with the Chinese government's (…) attempt to extend China's control over transnational network infrastructures." The stake is eminently sociopolitical, that is, accountability of the extent to which technology and data use/ownership create socioeconomic value and for whom.

7.5 CONCLUSION

By comparing Huawei's OpenLab in Johannesburg and the JIC in Cagliari, the chapter scrutinized the discursive framings of these initiatives with regard to the normative tech-centered conception of smart city solutions, and assessed the different governance models and partnerships supporting the initiatives in terms of their potential (dis)empowerment for local actors and citizens.

Both initiatives put forth a techno-optimistic vision that presents them as win-for-all projects. This framing avoids an in-depth characterization of actual implementations of smart city solutions and their impact on local communities. In this regard, the discourses surrounding both initiatives adhere to the normative understanding of smart city solutions as ICT-based endeavors to enhance decision-making efficiency and quality of life, by default rather than proven. Of particular significance is the coupling of smart city with the concept of safe city, that is, increasingly controlled spaces. From this perspective, socioeconomic considerations are eschewed as if the smartening of the city were an inevitable tide uplifting all actors involved. The analysis also revealed differences in the ways in which these initiatives have been publicly communicated.

While there is more publicly available information in the Italian case, very minimal exists in the case of Johannesburg's OpenLab. In both cases, however, Huawei refrained from delivering any statements upon request about the workings and outcomes of its initiatives.

In terms of governance, the OpenLab is heavily based on foreign private stakeholders. In fact, no South African stakeholders, either private or public, are officially part of the Lab. Instead, the OpenLab includes Western and Chinese private ICT companies alike. Running against the call by South African authorities to fuel tech initiatives in an integrated manner, the foreign-led nature of the OpenLab frustrates the development of local stakeholders and hinders the emergence of South Africa's digital sovereignty. This unbalance emerges even more vividly when comparing the OpenLab with the JIC in Italy. Although Huawei is the main private stakeholder, the JIC is nonetheless led by CSR4, an Italian public research center. However, in this case too, the cyber-geopolitical tensions surrounding the technology governance of the initiative cannot be overlook in that they do represent a potential threat to digital sovereignty as underscored by the European Union.

To an extent, Huawei shows high contextual flexibility when establishing its investments and partnerships abroad. The proprietary approach Huawei favors in South Africa undoubtedly gives the company more discretion with regard to the type of projects developed. The diversity of stakeholders with whom Huawei partners, particularly in Italy, does highlight the extent to which its smart city initiatives rework the concept of digital sovereignty and how, beyond theory, such diversity fosters a *certain* real-political form of digital sovereignty based on contextual opportunities. Beyond a domestic and foreign dichotomy, these smart city initiatives rearticulate the concept of digital sovereignty according to a transnational approach, underscoring Huawei's modulated interventions across the globe.

For both case studies, further field research is needed to substantiate the discursive analysis with ethnographic findings. Indeed, the assessment of the extent to which digital sovereignty is a contested arena along the Global North–Global South axis, *as much as* the South–South axis cannot do without the direct engagement with stakeholders. This, in turn, requires putting pressure on all ICT actors for demanding a more transparent and accountable communication concerning how the data fueling their smart city projects are managed, especially considering that digital sovereignty is an increasingly entangled transnational geo-governance issue.