Global Campus Europe

University of Coimbra

European Master's Programme in Human Rights and Democratisation
A.Y. 2019/2020

# A Digital Scramble for Africa

## US, EU and Chinese Influences on Internet Regulation in Africa and their Effects on Freedom of Expression and the Right to Privacy

Author: David Fischer
Supervisor: Jónatas Machado

**Abstract**

Divisive Internet regulation is fragmenting the formerly worldwide web into numerous shards that follow their own rules. The US, the EU and China are influential in shaping regulation even beyond their own jurisdictions, with consequences for human rights, particularly in Africa.

This paper argues that, as of 2020, the Western post-9/11 security agenda and uncontrolled digital capitalism had a more detrimental impact on Internet regulation in Africa than the authoritarian Chinese concept of Internet sovereignty, seriously affecting freedom of expression and the right to privacy online. However, particularly authoritarian governments in Africa use China's economic and political agenda to their advantage, leaving civil societies at the mercy of digitally empowered states.

Direct ways of impacting Internet regulation in Africa include loans, development programs or influential laws, whereas indirect means include engagement in multilateral and multi-stakeholder fora. Besides the political and economic interests of states, the datafication agendas of ICT corporations shape Internet landscapes in Africa. An emerging data protection framework pushed by the EU has the potential to mitigate their impact. Other means of protecting human rights require a united approach by the African Union and a deconstruction of digital capitalism and dependence relations between African states and the Global North.

**Table of Contents**

## 1 Introduction

In August 2020, after years of Western politicians criticising China's Internet censorship, US President Donald Trump took a page out of the Chinese Communist Party's (CCP) strategy book and announced the bans of WeChat and TikTok, two of the world's largest Internet platforms, from doing business in the US (Swanson). Going even further, his administration called on US allies to create "Clean Networks", disconnected from the "CCP's surveillance state and other malign entities" (Pompeo). The US call for ideological alignment and, effectively, polarisation of Internet governance is phrased in a rhetoric that reflects an emerging technological cold war and makes the idea of a truly *worldwide* web seem like a relic from the past. Internet governance has entered the realm of foreign policy and particularly social media platforms and their regulation are becoming geopolitical arenas (Brühl).

African states without a domestic information and communication technology (ICT) sector that can compete globally are in danger of becoming a battleground for international stakeholders looking to access new markets and increase their influence on Internet governance (Mihr 65). As a countermeasure to a perceived lack of regulation by platform operators, many African governments have resorted to blocking access to these platforms or to the Internet altogether (Mutsvairo & Ragnedda 18). Authoritarian administrations arrested Internet users and censored websites, violating the rights to freedom of expression and privacy (CIPESA 3, 6).

Internet regulation in Africa is often influenced by interactions with foreign stakeholders. Historically, US and European development and security agendas shaped Internet governance in the Global South (Arora). Since the rise of China to an economic powerhouse, its political influence grew and its restrictive domestic Internet policy sparks fears among Western democracies that it could export cyber authoritarianism as "an alternative ideology and governance structure to the prescribed democratic template of the United States and Europe" (Arora). From an African perspective, on the other hand, China emerged as a new partner for reaching development goals without the conditionality clauses in European and US agendas, which notoriously include the "imposition of neoliberalism through structural adjustment programmes and democratization promotion" (Alden 88).

Three main research questions inform this paper. Firstly: What approaches to Internet regulation do the US, the EU and China take and how do they promote them in interactions with African stakeholders? Secondly: How do these interactions affect Internet regulation in

the case study states Ethiopia, Ghana, Kenya, Nigeria and Zimbabwe, particularly with regards to the human rights to freedom of expression and privacy? And thirdly: Which steps should stakeholders involved in Internet regulation take to secure the rights to freedom of expression and privacy?

This paper argues that, as of 2020, the Western post-9/11 security agenda and uncontrolled digital capitalism had a more detrimental impact on Internet regulation in Africa than the authoritarian Chinese principle of Internet sovereignty, seriously affecting freedom of expression and the right to privacy online. However, power balances are shifting and particularly authoritarian governments in Africa use China's economic and political agenda to their advantage, leaving civil societies at the mercy of digitally empowered states.

Specifically, this paper demonstrates that US ICT corporations' monopolies allow them to shape online communication in Africa while collecting personal data that fuels the public and private surveillance sector. African governments are overwhelmed and some view platform blocking or Internet shutdowns as their only means of regulation. A Western multi-stakeholderism approach to global Internet regulation that includes voices from civil society and corporations is losing momentum, because these actors pursue different economic and political interests and authoritarian governments push for the exclusion of non-state actors. An emerging data protection regime spearheaded by the EU's General Data Protection Regulation (GDPR) is expanding its influence into parts of Africa, but still faces much pushback.

On the other hand, it will be shown that China's influence on Internet regulation in Africa is based on long-term strategies that synchronise the actions of the government, financial investors and ICT corporations. By almost unconditionally supplying incumbent African governments with the means of establishing a restrictive Internet, negative effects on freedom of expression and the right to privacy prevail even after governments change. Since China mostly provides loans rather than aid, it reproduces and intensifies existing relations of dependence. Rather than exerting direct political pressure on African states to adopt its restrictive version of the Internet, China impacts global Internet regulation by gaining influence in multilateral fora where debtor states are loyal to Beijing. Stakeholders in media, education and academia complement the government's foreign policy with soft-power.

For the African states examined as case studies in this paper, China as an alternative partner creates new forms of agency, an aspect that is often undervalued in scholarship dealing with Internet development in the Global South. As Iginio Gagliardone found necessary to remind readers, China, the US, and – it must be added – Europe are "*interacting with*" African institutions, not "*doing something to* Africa" (11). Another preconception must

be abandoned, one that is often held by Western states who fashion so-called Africa policies, lumping together the continent's 55 independent countries (Mutsvairo & Ragnedda 17). While there are similarities that make African states comparable within the boundaries of the Internet policy framework (e.g. membership in the AU, colonial histories or a tertiary role in creating global Internet governance), it is vital to see them as individual actors. The case study states in this paper are selected to cover a broad spectrum of authoritarian and democratic states, a variety of relations to external stakeholders and different stages of big data readiness (see chapter 5.1).

To address its research questions this paper draws on the analytical tools of dependency theory, securitization and datafication. This interdisciplinary approach helps to discern the motivations of the various stakeholders involved in the disorderly process of shaping Internet governance in Africa. Chapter 2 establishes these theories in greater detail and defines terminology before chapter 3 briefly introduces the mechanisms of Internet regulation. Chapter 4 outlines US, European and Chinese principles of Internet governance and analyses their different methods of influencing it on a global scale. Special attention is devoted to the role of China which has changed global power dynamics over the last years and is controversially discussed in the academic discourse surrounding Internet regulation. Chapter 5 transfers the discussion to the realm of Internet governance in African states, analysing the influence of external powers as well as human rights effects in Ethiopia, Ghana, Kenya, Nigeria and Zimbabwe. An additional focus is laid on the African Union as the connecting legal and political organisation and its function in upholding digital human rights across the continent. Chapter 6 engages with the debate on recommendations to the stakeholders involved and discusses ways to improve Internet regulation in African states with regards to human rights. Chapter 7 concludes and outlines areas of further research.

Methodologically, this paper will make use of theory-testing process tracing as described by Beach and Brun Pedersen (14-16) and built upon by Stokke (n.p.). It posits the approaches of the US, the EU and China and their respective ICT corporations to influence Internet regulation in the Global South as an independent variable. Accordingly, the effects on Internet regulation in the case studies of African states constitute the dependent variable against which the hypotheses established above are probed.

Fig. 1: Variables and causal mechanisms of foreign influence on Internet regulation in African states, structured according to Kristian Stokke's model of process tracing.

| | **Independent variable** | **Causal mechanism** | **Causal mechanism** | **Dependent variable** |
|---|---|---|---|---|
| **Theoretical level** | Dominant actors' approaches to Internet regulation | Direct political influence on African states | Indirect political influence through multi-lateral and multi-stakeholder fora | Internet regulation in case study states and effects on human rights |
| **Empirical level** | States: Legislation on freedom of expression, privacy and data protection, political statements, foreign policy<br><br>Corporations: intra-platform regulations, cooperation with governments | Investment, debt-relations, foreign aid, joint development projects, bilateral treaties, party-to-party relations, shared ideologies | Agreements at AU and UN level<br><br>Agreements in ITU, WSIS | Infrastructure: Internet penetration, ICT landscape, market structures<br><br>Legislation: Laws affecting freedom of expression, privacy, data protection<br><br>Executive: Internet blocking, censorship, arrests |

Source: The author; Stokke.

Due to the nature of international relations, finding irrefutable empirical evidence to support a causal relation between Internet visions of the US, the EU and China and regulation in African states is difficult. Not only are political deals often non-transparent, but data concerning the human rights effects of Internet regulation in Africa is often incomplete (Joubert et al. 109). To overcome these challenges of operationalisation, this paper moves beyond traditional data sources and includes political statements and interview excerpts from stakeholders to support its argument. The five case studies can be considered straw-in-the-wind tests intended to increase the hypotheses' plausibility without being decisive on their own (Collier 826). In conjunction, however, they provide a benchmark for an initial assessment of the claims regarding external influences on Internet regulation in Africa.

Two caveats with regards to focal areas: While Internet regulation expands far beyond the sphere of social media, this paper devotes special attention to this form of communication, which is vital for political and social movements in the Global South who depend on

platforms as an essential way to spread messages (Mihr 52). The temporary focus stretches from the securitization of online communication in the post-9/11 era, over the emergence of China as a digitisation partner for African states in the 2000s and 2010s, until the recent platform bans in mid-2020. However, current power dynamics cannot be seen detached from historical developments dating back into the times of colonialism, as the following chapter will demonstrate.

## 2 Theoretical Background

The main theoretical background for this paper is provided by dependency theory and it is supplemented by ideas emerging from securitization and datafication. Dependency theory establishes the framework for analysing power structures between states in the field of digital development from the perspective of the Global South. Securitization is mainly employed to explain the rationales of governments within their domestic spheres. Datafication accounts for the role that ICT corporations play in amplifying dependency relations by deconstructing the dynamics inherent to digital capitalism. Thereby, the paper expands its foundation in international relations (IR) to an interdisciplinary approach that include voices from economic and media studies.

### 2.1 Dependency Theory

The Brazilian sociologist and co-founder of dependency theory Thetônio dos Santos defines dependence as

> a situation in which the economy of certain countries is conditioned by the development and expansion of another economy to which the former is subjected. The relation of interdependence between two or more economies, and between these and world trade, assumes the form of dependence when some countries (the dominant ones) can expand and can be self-sustaining, while other countries (the dependent ones) can do this only as a reflection of that expansion, which can have either a positive or a negative effect on their immediate development. (231)

The school of thought emerged as a counter-position to developmental theories of modernization, criticising the assumptions of a linear economic development in the Global

South and exposing the capitalist interest of industrialised states in maintaining relationships of dependence (Ferraro). There are several different strands of dependency Theory, but their common ideas include 1) the division of states into dominant and dependent groups, 2) the importance of external forces representing dominant states' interests in dependent states, including multinational corporations, economic institutions, communications and foreign aid, and 3) a continuous reinforcement and intensification of the power imbalance between dominant and dependent states through the system of international capitalism (Ferraro).

A core concept within the Marxist strand of dependency theory is underdevelopment, which is viewed as intrinsic to international capitalist relations between dominant and dependent states. Accordingly, underdeveloped states make use of local resources, albeit not for the advancement of their own population, but for the benefit of dominant states (Ferraro). For dependency theory pioneer André Gunder Frank "underdevelopment and exploitation happen not through exclusion from the economic system of capitalism but as a consequence of being included" (qtd. in Musa 82).

Dependency theory enriches the debate on Internet regulation in Africa by structuring economic and power relations between dominant actors like the US, EU and China and dependent actors such as African governments through a critique of capitalist implicitness. It is relevant when contrasting development programmes based on conditionality or non-conditionality by tracing the aims of donor countries back to their own economic and political agendas. While most dependency theorists acknowledge that short-term advancements can be achieved in the Global South through investments from dominant states, they point out the perpetual replication of power constellations: "The development that it produces benefits very narrow sectors (...) and leads to the progressive accumulation of balance-of-payments deficits, which in turn generate more dependence and more superexploitation" (Dos Santos 235).

Although the intention of this paper is explicitly to analyse African governments as actors, rather than passive institutions acted upon from the outside, applying dependency theory shows that the scope of actions for dependent states is limited, especially in negotiations with economic superpowers. Particularly with regards to providing basic Internet infrastructure, African legislators face a pressure to 'catch up' with technological standards coming from their own civil society, the domestic private sector and international global players.

## 2.2 Securitization

The IR theory of securitization deals with the process of turning a non-political or political matter into a security issue. Buzan et al. explain that securitization is "constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" (25). The authors identify three components to successful securitization: "existential threats, emergency action, and effects on interunit relations by breaking free of rules" (26). When securitization is achieved, the securitizing actor, often the state, is able to go surpass existent rules to tackle the alleged existential threat.

While securitization theory traditionally focused on processes in liberal democracies, it has since been applied as an analytical framework to other forms of government as well. Indeed, Wæver claims that the theory is potentially "systematically Western-sceptic" in its view of relations between traditionally strong Western actors and other rising powers (476). Securitization critically assesses the creation and consolidation of threats, a discourse that, when seen globally, has been historically dominated by Western states.

The Post-9/11 War on Terror is a popular subject matter that has repeatedly been deconstructed by applying securitization theory. This paper shows how online communication has been annexed into this securitized area, as calls to regulate the Internet are commonly framed as a matter of national security, particularly in states dealing with armed groups. On an international level, securitized communication has long informed relations between the Global North and the Global South, with colonisers surveilling and strategically undermining resistance movements (Arora). This historical experience continues to shape the use of modern ICTs by African governments to control oppositional voices.

## 2.3 Datafication

Complementing the classical IR approaches of dependency theory and securitization, datafication provides rationales for the actions of ICT corporations. With a more narrow scope than the theories above, it adds a crucial perspective on the motivations of global players such as Google and Facebook or Tencent and Alibaba.

In his autobiography *Permanent Record*, US whistleblower Edward Snowden identifies a tipping point in the historical development of the Internet when

> companies realized that people who went online were far less interested in spending than in sharing, and that the human connection the Internet made possible could be monetized. If most of what people wanted to do online was to be able to tell their family, friends, and strangers what they were up to, and to be told what their family friends, and strangers were up to in return, then all companies had to do was figure out how to put themselves in the middle of those social exchanges and turn them into profit. (4-5)

Datafication describes precisely this process by which corporations restructure social spaces in a manner that makes them readable, manageable and above all, monetizable (Couldry and Meíjas 4-5). Indeed, Couldry and Meíjas speak of data colonialism "the reconfiguration of human life around the maximisation of data collection for profit" (3). Their theory views data as a resource which is generated through datafication of interpersonal interaction.

This capturing of communicative territory connects the theory of data colonialism to historical colonialism. Mutsvairo and Ragnedda draw an analogy between the installation of European communication systems like telegraphs and telephones during colonialism and the expansion of modern ICT, both of which replace existing forms of communication controlled by Africans through technology that generates profits for foreign investors (19). African states are becoming increasingly more dependent on digital infrastructure and services that multinational companies provide strictly for the aim of monetizing data (Musa 70). The fact that these private actors often possess more economic power than the states they operate in gives them leverage to influence the political process of regulation in their favour.

The long term effects of datafication and data colonialism on communication are still unpredictable, but have already been subject to much scholarly debate. Harsin fears that political movements in the newly fenced territories of communication will be limited to a "managed spectacle of claiming, sharing, liking, debunking and refuting" (6). For big data corporations the contents of this spectacle have no relevance whatsoever, as any contribution or interaction is just as monetizable as another (Dean 179). What matters for the bottom line is the quantity of engagements. Despite their ambitious mission statements, big data corporations register the erosion of democracy or the division of societies merely as unwanted side-effects of this utterly successful business model (Kreye).

### 2.4 An Interdisciplinary Normative Approach

Despite their different foci, dependency theory, securitization and datafication are all able to highlight the power imbalances immanent in the process of Internet regulation. This paper draws on them individually and in combination to explain the motivations of the multitude of actors involved in this process. While there are contradictions between the theoretical approaches, their intersections are more relevant.

All three theories include a normative stance. Dependency theorists' recommendations cover a spectrum from reforming trade and aid relations to complete autarky for dependent states (Flanders 306-07). Wæver admits outright that securitization theory is politically biased towards "desecuritization" (469). And in their discussion of datafication and data colonialism, Couldry and Meíjas point out the need to "challenge corporate data collection as such" (6). Taken together, these positions inform this paper's approach to the field of Internet governance in Africa and expand its scope beyond analysis into the field of criticism and recommendations.

## 3 Conceptualizing Internet Regulation

Over the last two decades the anarchical phase of the pre-datafication Internet transitioned into a continuous restructuring by states and private actors. Between these two classes of actors and among themselves arose a normative competition to impose regulations that guide interactions. This paper draws on Julia Black who defines the process of regulation as

> the sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification. (qtd. in Leenes 12-13)

Leenes argues that regulation becomes necessary when a problem causes market failure, human rights violations or stands in the way of conflict resolution (13). In the case of the unregulated Internet, an argument can be made that human rights are at risk, however, they are also on the line when regulators intervene too much. In 2013, the UN General Assembly agreed to resort to human rights as the "key benchmarks for regulating the online world" (Mihr 63).

In many cases this stands in opposition to the aims of states and corporations who benefit from regulating or deregulating online spaces according to their own goals. In their discussion of power structures and technological development, Michael Allen and Gabrielle Hecht argue that regulating technology shapes values that inform future developments (qtd. in Gagliardone 16), a long-term process that affects society and cannot be reversed simply by updating a law or the terms of agreement of an online platform. Both states and corporations bear responsibilities in their role as regulators since their decisions often have consequences that reach far beyond their countries or platforms.

### 3.1 Private Corporations as Regulators

In the scholarly discourse on Internet regulation, Lessig's dogma that "code is law" is widely accepted as the starting point for discussion (5). However, code is written by private actors rather that elected legislators. In the contemporary Internet, which is structured around the services of large platform operators, the first step in setting a regulatory framework is usually done by ICT companies. This happens in two ways: Firstly, by coding the technical framework of interaction, i.e. defining which formats of content platform users can publish, whether content is published directly or redacted, whether content is accessible only to (paying) members or everyone, etc. Secondly, platform operators establish rules on content itself through the terms of agreement, which can be guided by thematic constraints, social norms, political and security guidelines and more. These terms of agreement are usually in accordance with the platform operators' home state's legal code and their violation can lead to censorship of individual communications, as well as suspension or deletion of user accounts.

While private actors pursue their own economic goals when regulating users on their platform, they also face pressure from government and civil society (PoKempner 232). In the case of multinational big data corporations, however, the power imbalance vis-à-vis states with GDPs amounting to only a fraction of companies' budgets allows for much leeway in regulating communication without external oversight.

Even though the framework of business and human rights is continuously adjusting, Internet regulation by corporations must be viewed under the caveat that private actors cannot be held directly accountable for human rights violations. While their terms of agreements usually correspond to a legal framework in their country of origin, this does not necessarily reflect the laws in the *user's* country. Even when they were willing to, corporations rarely have the capacity to adjust their platform to each country's regulatory system, much less to

distinguish between legal and illegal usage according to the local laws and enforce compliance (PoKempner 233).

Indeed, it can be argued that, in practice, the sheer amounts of content created are not realistically manageable. On the world's leading video streaming platform YouTube, users averagely uploaded 30,000 hours of video content during every hour of the month of May 2019 and the numbers are steadily increasing (Clement). Under pressure from governments and users, in 2017, Facebook increased the number of content moderators from 4,500 to 7,500, however, the number of worldwide users they had to administrate – usually without legal training – was two billion (PoKempner 234).

To date, the enforcement of a platform's terms of agreements still involves a human component and is a questionable business at the ground level. For their documentary *The Cleaners*, directors Hans Block and Moritz Riesewieck interviewed content moderators contracted by US big data corporations in the Philippines. They are in charge of deciding whether or not to delete texts, images and videos, assessing footage of terrorist beheadings, (child) pornographic material, live suicide streams and any other content reported by users or otherwise filtered for review (Block and Riesewieck). An interviewee describes the crucial responsibilities of her team: "Our task is to monitor and moderate the user based content. ... I stop the spreading of child exploitation. I have to identify terrorism. Have to stop the cyberbullying. Algorithms can't do what we do" (qtd. in Block and Riesewieck). The film shows content moderators judging footage within a few seconds, with one interviewee saying he goes through about 25,000 pictures per day. Another moderator claims her superiors ensure the quality of her team's decisions by double-checking about three percent of her evaluations (qtd. in Block and Riesewieck). Whether or not higher level employees have more legal training qualifying them to review cases is not revealed.

Even despite their use of external contractors in low-wage countries, big data corporations are looking to reduce costs at the crucial stage of content regulation. Rather than resorting to "expensive" human reviewers which many cannot or do not want to afford, private actors program algorithms to analyse and judge communications that violate their terms of agreements (PoKempner 234). Within platforms, these algorithms serve as proxies for the law, enforcing penalties from censorship to bans and deletions of user accounts. Depending on their coding, they censor communications within seconds, minutes or hours, or block communication before it ever reaches its intended addressee (Ogunlana 95). Facebook CEO Mark Zuckerberg claimed in 2020 that his company's algorithms were "able to proactively identify 98 percent of the hate speech ... before it's even seen by other people"

(CNET). Since corporations traditionally keep these algorithms non-transparent, there is little possibility of external actors to scrutinize them for their potential to violate freedom of expression.

Whether through human or algorithmic judgement, according to PoKempner it is "not realistic to expect private companies to reproduce judicial-quality distinctions between protected and free speech" (234). On the contrary, as shown in *The Cleaners*, the decision-making processes are nowhere close. While corporations increasingly find themselves under much pressure from states to make regulations in accordance with national laws (PoKempner 233), this process is reciprocal: by funding lobbying and political advocacy, private actors invest heavily in influencing regulations made by states (Leenes 15).

### 3.2 The Role of the State

In the absence of a functioning framework of global Internet governance, the most important regulating actors are states. Like corporations, they pursue different interests when shaping Internet regulation. Particularly with regards to social media platforms, governments are confronted with their "dyadic nature" of being able to promote democracy but also authoritarianism (Oginni & Joash 161).

Unlike platform operators, states have the technological capacity to regulate, surveil and censor Internet communication on a level above the platforms, but usually not within them (Ogunlana 83-84). This led some governments to perceive external platform operators as a threat to their sovereignty. In return, they rely more on the means of control they have left, which include penalizing users for individual communications on a platform, outlawing the platform entirely or restricting Internet access altogether.

While the technical possibilities for states to regulate the Internet are extensive, International Law sets clear boundaries, particularly in article 19 of the International Covenant on Civil and Political Rights which protects the human right to freedom of opinion and expression. As paragraph 3 states, restrictions to this right are only allowed if they are "provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals" (UN General Assembly). In 2011 UN General Comment 34 added several details including specifications regarding the limits of Internet regulation by State parties:

> Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to

> support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government." (UN Human Rights Committee, para. 34)

The General Comment also encourages state parties to ensure access to the Internet for individuals and foster the independence of new media, promote plurality and prevent media monopolies by the State or private actors (UN Human Rights Committee, paras. 15, 40).

Except for China which signed the ICCPR in 1998 but has not ratified it, all other states central to this paper ratified the convention (UN Treaty Collection, "ICCPR") and none made any noteworthy reservations or declarations with the exception of the US, which will be discussed in chapter 4.1. The First Optional Protocol to the ICCPR allowing individual complaints to the Human Rights Committee was signed by all EU member states and Ghana; the US, Ethiopia, Kenya, Nigeria and Zimbabwe are not State Parties (UN Treaty Collection, "Optional Protocol to the ICCPR").

In practice, Internet regulation by states takes many forms that push or break the limitations set forth by human rights treaties. On the most basic level, states are able to control who has access to the Internet by setting up the infrastructural necessities such as cables, satellites etc. Where access is provided by states, they are also capable of taking it away. African governments have repeatedly shut down the Internet nationwide or selectively in specific parts of their countries for instance as a tool to suppress protests as the case studies in chapter 5 show.

Besides these drastic measures, states use legislation to impose restrictions to freedom of expression. A typical example are anti-terrorist laws emerging after UN Security Council Resolution 1373 (passed unanimously just 17 days after the attacks of 9/11), which called for more information exchange on "communication technologies by terrorist groups" (para. 3a). Ten years later, the UN clarified that

> [s]uch offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly

> defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. (UN Human Rights Committee, para. 46)

Other laws affecting freedom of expression online criminalise blasphemy, criticism of government institutions or the expression of opinions about historic facts, all of which have been deemed incompatible with the ICCPR (UN Human Rights Committee, paras. 38, 48, 49).

Nevertheless, states often make full use of their surveillance capacities to enforce these laws, often pressuring platform operators to comply with law enforcement by granting access to user data, or even accessing data without their approval (PoKempner 233). The reluctance of states to pass effective data protection legislation can be considered a way of regulating the Internet by deregulating it, allowing platform operators to collect data on their users which then in turn can be used by state authorities. This is in violation of article 17 of the ICCPR, which constitutes "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks" (UN General Assembly). This right to privacy is also violated when states pass data protection laws that are targeted specifically at private actors, while including loopholes for law enforcement or intelligence agencies (PoKempner 225).

To guarantee access through government agencies and increase regulatory possibilities, some states are looking at possibilities of forcing platform operators to store data on servers within their borders (Kriebitz & Lütge 21). Data localization is controversially discussed for its impact on data protection, with supporters pointing out more local control over foreign ICT corporations and others fearing exploitation by states without functioning data protection.

### 3.3 From Sovereign Regulation to Multilateralism and Multi-Stakeholderism

Until here, the discussion of the state as a regulator has been informed by national sovereignty, i.e. the assumption that states have the power to regulate the Internet by themselves. Due to the web's transnational nature, however, most states recognise a need for basic international agreements on standards and principles. International fora dedicated to finding agreements approach the issue either through multilateralism or multi-stakeholderism. This paper draws on Ruggie's definition of multilateralism as "an institutional form which

coordinates relations among three or more states on the basis of 'generalized' principles of conduct" (571). It can be contrasted with Raymond and DeNardis' definition of multi-stakeholderism, which involves "two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules" (20).

In practice, the lines between multi-stakeholderism and multilateralism are blurred. International organisations (IOs) tend to set up multi-stakeholder platforms, but authoritarian governments push for the exclusion of non-state actors (Gagliardone 145). The most important organization with regards to setting technical standards and regulatory norms for the Internet is the International Telecommunication Union (ITU). The UN specialised agency hosted the controversial 2012 World Conference on International Communications (WCIT) as well as the World Summit on the Information Society (WSIS) in 2003, 2005, 2015 and 2020. The 2012 WCIT was intended to find common ground for regulating the Internet, but ended without consensus, exposing the rift between overarching policies promoted by Western states and the principle of Internet sovereignty which most other participants supported (Gagliardone 147). The stand-off resulted in civil society stakeholders finding themselves "flattened on the position of hegemonic powers and large corporate agents" (Gagliardone 147). The 2005 WSIS saw more results, sparking the mandate for the UN's Internet Governance Forum (IGF) (Mihr 65). The annual meetings are informed by a multi-stakeholder approach and include experts from NGOs and corporations, but final decisions are made by governments (Mihr 65-66). Regional and national IGFs exist across the world, including in all the case study states except Ethiopia (UN Secretariat of the Internet Governance Forum).

A multitude of other multilateral and multi-stakeholder organisations is also engaged in influencing Internet policy. The WTO and the World Bank push a liberalisation agenda to open markets for privates actors. The OECD published Guidelines on Multinational Enterprises, Corporate Social Responsibility (CSR) and Foreign Direct Investments (FDI) to set soft law standards for its member states' engagement in the Global South and promotes principles such as limited data collection, purpose specification, data security and transparency (Kontargyris 62).

Raymond and DeNardis compiled a comprehensive table of responsibilities in Internet regulation. An excerpt that focuses on regulating freedom of expression is reproduced in figure 2. The numerous actors involved in just this sub-section prove that Internet regulation

is de facto a process distributed over several classes of stakeholders which are not necessarily in coordination.

Figure 2: Excerpt of Raymond and DeNardis' table "Disaggregated Internet Governance Taxonomy" (29-30).

| **Functional Area** | **Tasks** | **Primary Institutional Actor** |
|---|---|---|
| Access and interconnection coordination | Setting end-user access and usage policies | Private network operators |
| | Regulating access (such as net neutrality) | National governments/agencies |
| Cyber-security governance | Designing encryption standard | Standard-setting organizations |
| | Cyber-security regulation/enforcement | National statutes/multilateral agreements |
| Information intermediation | Commercial transaction facilitation | E-commerce sites and financial intermediaries |
| | Mediating government content removal requests (discretionary censorship) | Search engines, social media companies and content aggregation sites |
| | App mediation (guidelines and enforcement) | Smartphone providers (such as Apple) |
| | Establishing privacy policies (via end-user agreements and contracts) | Social media, advertising intermediaries, email providers and network operators |
| | Responding to cyberbullying and defamation | Content intermediaries |
| | Regulating privacy, reputation and speech | Statutory and constitutional law |
| | Mediating government requests for personal data | Content intermediaries and network operators |

Source: Raymond and DeNardis (29-30).

Although states are the duty bearers ultimately accountable to international law, particularly democratic governments pressure corporations to "assume the burden of censorship" rather than providing a judicial framework in which cases can be tried (PoKempner 232). The perceived ambiguity of responsibilities has lead to a lack of regulation concerning hate speech and other illegal communications and an insecurity among Internet users about who can be held accountable when a website or platform is abused for racism,

religious hatred, sexism or homophobia and who is accountable for guaranteeing freedom of expression. This insecurity is fertile ground for populists who mobilise followers against state censorship when they are in the opposition or against big data censorship when they are in office.

Van Dijk et al. surmise that the Internet will never be as controlled and regulated as the offline world (775). This paper argues the opposite. Even though the amounts of data currently appear unsurmountable, the data-based nature of the Internet allows any interactions to be read, evaluated and subjected to regulation by states and private actors much easier than offline activities through automated decision-making. Algorithms' potential to regulate interactions online by far exceeds human capacities to exert control over the offline world. More and more of our everyday lives is pushed into the datafied space of online communication where it can be subjected to automated regulation (Couldry & Meíjas 4). It is crucial to be aware which powers set the standards that algorithms use and to what extent their values are informed by human rights.

## 4 US, EU and China as Dominant Norm-Shapers on Internet Governance

Academic discussions of Internet regulators often draw a line between Western and non-Western states. However, this devaluates internal differences within both groups which is why this paper focuses on three more narrow actors: the US, the EU and China. These economically dominant powers promote their approaches to Internet regulation, leading to a normative competition in international fora and in economically dependent states where untapped markets promise profits for ICT corporations. Particularly African states, where the digital communications sector has experienced the largest worldwide growth in the years since 2005, are targeted (Srinivasan et al. 3). This chapter outlines the principles informing Internet regulation for of each of the three dominant actors before respectively analysing their strategies to influence Internet governance worldwide and in Africa.

### 4.1 US

Among the three dominant powers promoting their vision of Internet regulation, the US is the most difficult to pinpoint for two reasons. Firstly, it features striking ideational divides between civil society, big data corporations and the state. Particularly the role of big data corporations in this constellation has been changing with increasing concerns about

disinformation, hate speech and data protection. Secondly, the current Trump administration has turned the global role of the US on its head with his withdrawal from several international organisations, treaties, fora and investments. Nevertheless, US concepts of Internet regulation remain a highly influential actor, even though many efforts to promote them have become undone since 2016. In Internet regulation the US essentially pursues a libertarian approach with strong rights for non-state actors – a multi-stakeholder approach tilted towards the interests of private corporations.

### 4.1.1 A Libertarian Internet

The US considers a libertarian interpretation to the right to freedom of expression as central to its self-conception. This is expressed in a declaration regarding restrictions to article 19 of the ICCPR as set forth by paragraph 3, which implies that the US constitution guarantees additional protection to freedom of speech that the government does not intend to limit:

> For the United States, article 5, paragraph 2 [of the ICCPR], which provides that fundamental human rights existing in any State Party may not be diminished on the pretext that the Covenant recognizes them to a lesser extent, has particular relevance to article 19, paragraph 3 which would permit certain restrictions on the freedom of expression. The United States declares that it will continue to adhere to the requirements and constraints of its Constitution in respect to all such restrictions and limitations. (UN Treaty Collection, “ICCPR”)

Additionally, a reservation to the ICCPR was filed regarding article 20 which prohibits propaganda for war and “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence” (UN Treaty Collection, “ICCPR”). The state party notes that this “does not authorize or require legislation or other action by the United States that would restrict the right of free speech and association protected by the Constitution and laws of the United States” (UN Treaty Collection, “ICCPR”).

The US approach to freedom of expression is established by the First Amendment to the US Constitution that states “Congress shall make no law ... abridging the freedom of speech, or of the press” (US Constitution). The 1791 amendment can be seen as a foundational pillar for the right to freedom of expression worldwide. Unlike the ICCPR, however, the First Amendment creates no room for restrictions to this right and is thereby

problematic in an information society where corporations acting as intermediaries to individuals' speech claim the right to freedom of expression for themselves. Thus, many of the world's largest ICT companies which are based in the United States are assigned a unique role, as Kessler and Pozen analyse:

> Even though they control the infrastructure of digital communication and function as the "new governors" of the digital public sphere, companies like Facebook and Google are generally assumed to not be bound by the First Amendment because they are not state actors. Instead of empowering users to challenge their policies, the First Amendment empowers the companies themselves to challenge statutes and regulations intended to promote anti discrimination norms or users' speech and privacy, among other values. First Amendment law not only fails to check the internet's new governors and the inequalities that pervade their platforms but also stands in the way of legislative and administrative correctives. (1973)

The impact of these rights granted to corporations far exceed the country's borders since US platforms provide essential communication services in large parts of the world. The leeway they enjoy is not just evident in the area of freedom of expression, but also in data protection laws.

Kontargyris contrasted EU and US law on privacy and data protection and finds "the US approach is incoherent, sectoral-based, and with legislative protections that are largely reactive, driven by outrage and at particularly narrow practices" (60). A main property of American privacy law, the author argues, is that it lacks an omnibus law comprehensively covering the private sector, instead "scattered pieces of legislation" create a legal setting in which companies operate without much interference by the state (60, 66). As a result, big data corporations grew enormously and their economic and social impact is now at a level that makes them much harder to regulate.

Over the years the goals of big data corporations have slowly become aligned with the state's. Extracting data from social communications and monetizing it through advertising is accepted as one of the main business models of ICT companies. Ruth Porat, CFO at Google's parent company Alphabet, expressed this position, claiming "data is more like sunlight than oil" (qtd. in Gosh and Kanter, 2019). Couldry and Meíjas see this ideology as a means of disconnecting data from the people it is extracted from, positing it instead as an "owner-less resource" and establishing datafication as the legitimate status quo (12). While this principle

remains largely untouched, a fresh concern for data protection is largely based on the fear that foreign ICT corporations, such as China-based ByteDance, which owns the social media platform TikTok, could cooperate with their home country's intelligence service by granting them access to user data.

There is a certain hypocrisy to this, since particularly US intelligence agencies, which have increased in importance since the securitization of online communication after 9/11, profit heavily from unrestricted data collection by platform operators. Kontargyris points specifically to the PATRIOT Act and the Foreign Intelligence and Surveillance Act as obstacles for creating stronger data protection and privacy laws (75). Edward Snowden's revelations that US agencies' use of technologies like PRISM allow them to spy on Internet users worldwide have not led to a domestic reassessment of the relationship between privacy and surveillance (PoKempner 227). However, the inconsistency of promoting an open Internet and then exploiting it for espionage has changed the way US Internet policies are perceived internationally.

Recent political developments in the US have led to new dynamics between corporations and the state as regulators. As Lamer puts it, "it is starting to become clear that the Internet and social media in particular are not the best arbiters of what constitutes information, misinformation, or disinformation" (133). The 2016 presidential election campaign and Donald Trump's administration have shown that the populist President profits from a lack of content regulation concerning misinformation and disinformation. This relation changed in 2020 when Trump claimed mail-in ballots were inherently fraudulent and Twitter added a link to fact-checking articles with information from NBC, CNN and the Washington Post (Twitter, "Unsubstantial Claim..."). The President fired back, writing: "Republicans feel that Social Media Platforms totally silence conservatives voices. We will strongly regulate, or close them down, before we can ever allow this to happen" (Trump). One day later he signed the Executive Order on Preventing Online Censorship suggesting a revised interpretation of section 230(c) of the Communications Decency Act which would give online platforms the role of publishers, including increased judicial liability for content (United States, Executive Office). Trump used the opportunity for a broad attack on online platform's general political stance, claiming one of the them had "created a search engine for the Chinese Communist Party that would have blacklisted searches for 'human rights,' hid data unfavorable to the Chinese Communist Party, and tracked users determined appropriate for surveillance" without going into specifics (United States, Executive Office).

In isolation, the feud between the President and Silicon Valley tech corporations is merely a populist manoeuvre positing ICT corporations as liberal elites who fact-check the peoples' *volonté generale* as expressed by their elected leader. However, political calls for reforming Internet governance are increasing from all parts of the political spectrum, whether Trump threatens Twitter or naked activists protest inequality on the censorship of male and female nipples on Facebook (Paul). At the same time, users demand solutions for a wide variety of undesired communications associated with 'fake news' and hate speech, including racist and extremist content. The multitude of demands without a clear allocation of regulating responsibilities has led to a vague anger at a 'system' that censors too much where it should not and fails to censor where it should. This became evident in July 2020, when the CEOs of Google, Amazon, Facebook and Apple testified before congress on accusations of abusing their monopolies for manipulating public discourse, privacy breaches and more (CNET). If the current developments culminate in new legislation for regulating platform operators, it remains to be seen whether an empowerment of the state leads to more efficient protection of freedom of expression and the right to privacy or whether it opens the door to a more authoritarian version of the Internet, as some critics fear (Gagliardone 156).

### 4.1.2 US Methods of Influencing Internet Regulation

In 2010 Secretary of State Hilary Clinton articulated the US vision of a world wide web: "We stand for a single internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it" (Clinton). While this Internet vision is much less the romantic library Clinton describes and more of a corporate data bonanza, the crucial point is the idea of a unified Internet and the awareness that the US has the power to shape it. Henry Farrell and Martha Finnemore argue that liberal principles need to remain at the core of US foreign policy to maintain its legitimacy as a shaping power for the world order, even if these principles are not respected in domestic regulation (qtd. in Gagliardone 65). Thus, the US pushes for an Internet that is constructed around freedom and liberty, while implying that corporations have the liberty to shape this space in the way they find most useful i.e. profitable. Foster and Azmeh's findings in their analysis of digital trade companies is true for the entire ICT sector: "[T]heir agendas … [have] become part of national trade goals" (15).

In 2017, the US Department of State released a fact-sheet titled *Internet Freedom* outlining paths to influence global Internet governance:

> Promote & Protect: Fostering implementation of international human rights law and developing commitments in the global Internet freedom space with key stakeholders
> Convene & Facilitate: Creating a space for emerging and critical issues to be debated among relevant stakeholder groups
> Develop & Implement: Establishing tools, training and guidance for U.S. government officials to be more effective envoys on Internet freedom (n.p.)

The US intent to push human rights and developmental aims through a multi-stakeholder approach has been viewed more sceptically abroad, especially among non-Western critics. Li Yan claims "this model is often seen by other countries, especially emerging powers as well as developing countries, as one which favors the economic and security interests of the U.S." (3). Indeed, besides shaping foreign relations to accommodate the agenda of ICT companies pursuing datafication, the securitization of terrorism is a major ideological export impacting Internet governance worldwide. Particularly the approach to development projects in the Global South is informed by security concerns, a perspective promoted at all levels of governance from private policy contractors to international institutions (Gagliardone 128).

A game-changer in this regard was UN Security Council Resolution 1373, signed after 9/11 and calling on states to strengthen information exchange on "use of communications technologies by terrorist groups" (para. 3a). By including communication technologies into the bundle of securitized threats, the US effectively exported a securitization of digital development, creating room for states to strive for a controlled Internet as a weapon in the 'War or Terror'. This securitization prepares an argumentative ground particularly for autocratic governments to legitimize oppressive Internet governance and deny human rights online indicating more urgent security and stability needs (Gagliardone 9f, 127). Edward Snowden's exposure of the American surveillance apparatus resulted not in US scaling it down, but rather to other governments catching up (PoKempner 229).

Although the US advocates for the inclusion of civil society stakeholders into Internet regulation, it also promotes its views through inter-state relations, including bilateral agreements, engagement with like-minded groups of states such as the Freedom Online Coalition or multilateral fora such as G7/G8, and G20 (US Department of State, "Internet Freedom"). However, under Trump, interactions with African states to promote democracy and human rights saw a roll-back while the emphasis on the anti-terror agenda remained (Gagliardone 162). The President's open disdain towards African states – reportedly referring

to them as “shithole countries” (qtd. in Kendi) – is symptomatic for the administration’s disengagement with the continent. The fact that China emerged as a competitor increasingly investing in Africa has not yet caused much change. The UNCTAD World Investment report shows that FDI from the US to Africa have decreased between 2013 and 2017 “as a result of divestments and profit repatriations” while China’s FDI to Africa increased by 50 percent in the same time frame (38-39).

Compared with Chinese companies, big data corporations from the US are almost on their own when taking to Africa. However, reduced government investments also open up opportunities for private corporations which, according to the Department of State, “play an important role in making Internet freedom a reality” (U.S. Department of State, “Internet Freedom”). Despite their size it is difficult to argue that Google, Facebook or others are national champions in the way that Tencent and Alibaba are for China. Instead, Arora describes them as “technological oligarchies” (n.p.) that have the economic power to interact with African states without the support of the US government.

Not unlike the government’s hypocrisy of simultaneously promoting a free Internet and securitized communication, big data oligarchies are caught between their flamboyant mission statements and their investment-drivenness. From start-ups to big data giants like Google and Facebook, “making the world a better place” through their technology is the essential mantra shaping the Silicon Valley jargon (Ester 41). Indeed, some of the projects by ICT corporations in Africa have large effects on online lives of local citizens, particularly at the stage of access. A recent project. in which Facebook participates, is 2Africa, a 37,000 kilometers subsea cable intended to bring “an open and inclusive internet ecosystem” by providing access to 4G, 5G and broadband to “hundreds of millions of people” (Facebook, “Building...”). However, investments like this are primarily based on rate of return which is usually boosted by access to new markets.

The US approach to influencing global Internet governance is shaped by its internal inconsistencies. The state proclaims free and open Internet for everyone while exporting surveillance ideology and corporations are caught between pushing their mission-driven agendas and maximizing profits to please shareholders. Competing with other stakeholders that influence Internet regulation in Africa, the historically powerful US position has grown weaker under the current administration, which is evident in a retreat from multilateral institutions and uncoordinated action in multi-stakeholder fora. Through their economic power and communication monopolies, however, big data companies are still able to effect

change on their own mainly by shaping technical infrastructure. Chapter 5 shows how this too has the potential to impact Internet regulation in African states.

## 4.2 EU

Unlike the United States, the EU's approach to Internet regulation is not divided for political reasons, but for structural reasons. While the Union increasingly provides regulatory frameworks, its member states and European ICT companies follow their own agenda. Interactions with African states continue to be informed by historical relationships between former colonizers and colonies, particularly in investment and development politics. As a whole, the Union shows more commitment to a human-rights based approach to digital development than the US, while sharing the same goal of promoting an "open, free and secure Internet" (European Commission, *Digital4Development* 3-4). With less influence from big data corporations, the EU developed the GDPR as a data protection framework with massive effects on global Internet governance and is developing its next big project in the Digital Services Act (DSA). A multi-stakeholder approach informs EU actions on the global stage, but its human rights agenda often lacks assertiveness when economic pressure from the US or China grows and European companies fear market exclusion.

### 4.2.1 Fundamental Rights and Data Protection

Freedom of expression is constituted by both major European human rights documents, the Charter of Fundamental Rights of the EU (CFR) and the Council of Europe's European Convention on Human Rights (ECHR). The CFR, which applies directly to the "institutions, bodies, offices and agencies" of the Union itself, declares in article 11.1 that "[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers" (European Parliament). Although the wording "regardless of frontiers", which also appears in the 1950 ECHR, predates the dispersion of the Internet, it is vital to the premise that the protection of online communication does not end at the national borders even if jurisdiction does. This informs the EU's approach to Internet regulation which is often directed at the large US tech corporations dominating online communication in Europe. The more important document for individual member states is the ECHR, which formulates the right to freedom of expression in article 10, largely overlapping with the CFR.

The European Court of Human Rights found violations of article 10 in the case of blocking of services from Google (Ahmet Yıldırım v. Turkey 2012) or the video platform YouTube (Cengiz and Others v. Turkey 2015) (1-2).

The EU struggles with ways to directly affect the regulation of freedom of expression within platforms. However, it developed comprehensive data protection legislation ensuring free speech by setting barriers for surveillance and enabling users to hide content from platform operators themselves e.g. via end-to-end encryption. Among these, the 2018 GDPR stands out prominently as a challenge to US "big data exceptionalism", which assumes that extracting data is "just what corporations and markets do" (Helen Nissenbaum qtd. in Couldry & Meíjas 6).

As stated in article 1, paragraph 2, the GDPR "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (The European Parliament and the Council of the European Union). Critics interpret this as an effort to establish data protection as a human right (Kontargyris 71), directed at states as duty bearers. However, the complications of enforcing compliance are exponentially larger when dealing with big data companies protected by their home state's lenient approach to regulation. Contrasting legal systems between the US and EU, Reidenberg comments that US regulation is "based on liberal norms and market forces" while in the EU "data privacy is a political imperative anchored in fundamental human rights protection" (qtd. in Kontargyris 66). While the data protection legislation continuously evolves, the functionality of these rights in practice remains complicated. Couldry and Meíjas point out the issue of user consent as the legal basis on which data is shared, questioning whether informed consent is possible when the algorithmic mechanisms creating a user's "data double" operate beyond human control (7). Kontargyris suggests that the EU needs to focus "on complementing it [the GDPR] with laws that will realistically regulate" Internet platforms where privacy is violated (74-75).

Of course, the EU's push for increasing users' rights online is not directed solely at violations through US corporations, instead, its own member states are often in need of limitations with regards to surveillance and attacks on encryption (PoKempner 236). In some countries, lawmakers also apply pressure to corporations to filter communications in their place. In Germany, for example, legislation constitutes high fines when platform operators do not remove "obviously illegal content" from their sites within 24 hours (Lamer 141). As established in part 3.3, this can be problematic since the responsibility to distinguish between legal and illegal communication is allotted to private actors. Lamer refers to DeNardis and

Hackl in her evaluation that the German approach raises issues of a potential "privatization of human rights" (141).

Two recent developments are likely to influence the EU's approach to Internet regulation in the future. Firstly, in July 2020 the Court of Justice of the EU struck down the Privacy Shield agreement between the US and the EU, which allowed data transfers from technically European companies (like subsidiaries of Facebook or Google) to the US as long as European data protection standards were guaranteed. The Court agreed with the plaintiff, who considered personal data exported to the US unsafe from intelligence agencies, ruling that

> the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, (...) are not circumscribed in a way that satisfies requirements (Court of Justice, para. 185)

The political message emerging from this rulings is that global standards on data protection need to adjust to the high bar set by the GDPR.

Secondly, the EU Commission is preparing a Digital Services Act (DSA), which is still in the planning stage as of August 2020. The DSA is intended to provide a legal framework for supervising large online platforms, setting responsibilities, guaranteeing user rights and dissolving monopolies by regulating the market to the disadvantage of current platforms acting as gatekeepers (European Commission, "The Digital Services..."). In its position paper the advocacy group European Digital Rights (EDRi) describes the DSA as "a unique opportunity to fix the structural problems of today's centralised platform economy and promote an accountable and transparent internet platform regulation system" (Berthélémy and Penfrat 34). The paper makes several suggestions including the regulation of content moderation to prevent over-censorship and the establishment of dispute settlement bodies for cases where the legality of communications on a platform is contested (29, 31-32). A DSA with these provisions could have effects far exceeding the scope of the EU.

### 4.2.2 EU Strategies and their Global Effects

In 2017 the EU agreed on its Digital4Development agenda that aims at "providing access to affordable broadband connectivity for all, creating relevant content and globally competitive

services enabled by an open and free Internet and protecting human rights, including privacy" (European Commission, *Digital4Development* 15). The development outline identifies a particular challenge in companies restricting the right to freedom of expression and violating privacy and data protection laws without legislative safeguards and seeks to promote human rights standards in the ICT sector (13-14). This human rights-based approach to development sets the general context for EU attempts on influencing global Internet governance.

The main difference in comparison with Chinese and US attempts to shaping Internet regulation is the EU's focus on data protection as a foundation to ensure further rights. In multilateral fora, the EU has pressured businesses and government agencies in China and the US to comply with privacy standards (Greenleaf 28). In 2018, this led the UN to encourage states to adopt legislation similar to the GDPR (Couldry & Meíjas 6). The EU is also committed to ensuring net neutrality i.e. equal access to online content independent of the platform it is available on (European Commission, *Digital4Development* 12). These regulations are already difficult to uphold in its member states, but face additional challenges in the Global South where many service providers operate from abroad and are unwilling to comply with local legislation.

In practice, digital cooperation between the EU and Africa revolves mostly around aid and investment. The Commission's plan lays out four key focus areas regarding digital development:

> i. promote access to affordable and secure broadband connectivity and to digital infrastructure, including the necessary regulatory reforms;
> ii. promote digital literacy and skills;
> iii. foster digital entrepreneurship and job creation; and
> iv. promote the use of digital technologies as an enabler for sustainable development (European Commission, *Digital4Development* 4)

One pillar directed at ensuring Internet access is the EU-Africa Infrastructure Trust Fund. However, according to the most recent report covering 2018, the ICT sector received by far the lowest funding with €18.3 million or 2.4% of the €752 million total sum invested since the fund's creation in 2007 (13). The EU is increasingly including the private sector into its development projects through blending mechanisms. These incentivise loans by leveraging them with financial securities for private investors that would otherwise refrain from entering

the African market (European Commission, *Digital4Development* 4). In line with these developments, there is a push for liberalizing African markets to foreign investment and creating conditions favourable to private corporations. A goal expressed in the development plan is to

> create opportunities for European companies to extend their presence in new markets. Policy approximation between the EU and Africa in particular will also contribute to developing business relationships in the fast growing markets of the developing world. (European Commission, *Digital4Development* 15)

The EU's push for better Internet access and regulation reflecting EU policy should thus be seen not only in the light of the human rights that it promotes in public, but also as an economic decision.

Furthermore, the EU has a political interest in encouraging private and public actors to advance the datafication of African citizens that is related to its migration policy, an area continuously securitized by populists across Europe. The push towards limiting migration from Africa into the EU affects the entire field of aid and development including digitisation efforts, and reduced migrant numbers are used as an indicator for successful strategies (Fine et al. 21). The Commission's plan explicitly refers to digital technologies as a way to "reduce and/or manage migration flows" (19) and promotes digital identification schemes as means to "support the governments' efforts to enhance cooperation on legal migration with the EU" (22). Populists in the EU managed to shift the discourse on migration so far into the area of a threat that policymakers now address it as a securitized issue with the potential to override the original intentions of the digital development agenda.

As established, human rights are not the only maxim mainstreamed into the EU's push to influence global Internet regulation. Just like the US and China, it acts as a facilitator to its domestic companies and supports digitisation projects in line with its security agenda. Nevertheless, the EU's resolute data protection stance influences Internet regulation worldwide, enabling secure communication and strengthening the rights to privacy and freedom of expression worldwide. Emerging legislation to advance this agenda can be seen as a force with the potential to shift power balances on the Internet from datafying companies towards individual users.

### 4.3 China

The emergence of China as an economic powerhouse altered the discourse on digital development, which was long dominated by Western stakeholders, by providing an alternative world view (Alden 87). In terms of Internet regulation, this world view is shaped by the authoritarian rule of the Chinese Communist Party (CCP) and its regime of censorship and surveillance. In contrast to the EU and the US, China does not promote a human rights-based approach to regulation, although some of its policies line up with a collective right to development. The government strictly limits the scope of civil society participation in its decision-making process, championing a multilateral approach to Internet governance agreed upon between states without the inclusion of other stakeholders. The principle of Internet sovereignty rejects any outside influence on domestic regulation. Besides multilateral fora, China brings its Internet vision to the world through big data corporations with strong ties to the CCP (Arora). Due to China's game-changing role this paper devotes additional attention to its effect on the global political landscape.

#### 4.3.1 Internet Sovereignty, Censorship and Surveillance

Internet governance in China is first and foremost a reflection of the CCP's authoritarian rule. The Party structured the political landscape without a functioning system of checks and balances that ensure political participation and human rights (Alston). Instead, the government fostered a paternalistic relationship to the people (Arora), which makes use of ICT as a central means of enforcing it. Control over the Internet is not just a tool for the Party, but a pillar on which it stands, which makes it essential to uphold against alternative Internet ideologies from abroad.

While China has not ratified the ICCPR, it is a state party to the International Covenant on Economic, Social and Cultural Rights (ICESCR) as well as several other human rights treaties. However, their effect on the state has been compromised, firstly, through a cultural relativist approach to human rights (controversially referred to as 'Asian values') and, secondly, through the lack of rule of law. What Brooks calls a "human rights system with Chinese characteristics" (175), is essentially an approach to the international treaty system that subordinates it to the Party's national economic and development goals. Among the many concerns raised by a lack of a rule is the fact that judicial proceedings of citizens against the state are unlikely to be judged independently. The World Justice Project's 2020 report

evaluating rule of law rates fundamental rights in China the third-worst among 128 examined states, particularly raising concerns regarding freedom of expression and the right to privacy (58).

De jure, China's 1982 Constitution protects citizens' freedom of speech and freedom of press in article 35 (Constitution of the People's Republic of China). Article 40 establishes the "freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law" (Constitution of the People's Republic of China). Zhou points out more recent legislation like the 2009 Tort Liability Law, the 2016 Cyber Security Law and the 2017 Personal Information Security Specification, but none of these has succeeded in protecting the rights of Chinese Internet users, particularly not against the state (40).

Internet regulation in China reflects the Party's stance towards human rights in that its main characteristic is Internet sovereignty. Scholars struggle to agree on a precise definition, but for this paper, Gagliardone's suggestion will be applied, which describes Internet sovereignty in China as "the reassertion of physical borders into the digital realm, allowing nations the freedom to choose their own conceptions of the Internet, based on cultural, social, and political factors" (Gagliardone 18). This captures the ideas of cultural relativism and a disdain for the international human rights regime interfering with state policies. The government expresses its idea in a white paper on "The Internet in China", writing:

> The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security. (State Council of the People's Republic of China)

Importantly, this White Paper does not imply a Chinese exceptionalism, but rather the legitimacy of *every* state to exercise Internet sovereignty, thus attempting to normalize China's non-compliance with human rights (Gagliardone 97).

For President Xi, regulating the Internet is also a didactic project, as he points out in a 2015 speech:

> [G]reater efforts should be made to strengthen ethical standards and civilized behaviors in cyberspace. We should give full play to the role of moral teachings in guiding the use of the Internet to make sure that the fine accomplishments of human civilizations will nourish the growth of cyberspace and help rehabilitate cyber ecology. (n.p.)

This means that the rights to freedom of expression and privacy are ignored, when they are used to share what the party considers "unethical" or "uncivilized" behaviour. Four examples show how China enforces this approach to Internet governance.

Firstly, the so-called 'Great Firewall' functions as a technical censorship of many of the worlds largest Internet platforms including US based Google, Facebook, Twitter or YouTube, but also international media outlets like *The New York Times*, *BBC*, *Le Monde* or the agency *Reuters* as well as human rights websites from Amnesty International, Reporters Without Borders and many more (VPN Mentor). Users cannot access these sites from China without using proxy or VPN technology which simulates a foreign IP address. In recent years, however, the government intensified its crackdown on commercial VPN providers (Ryan).

Secondly, platforms that are available in China apply heavy censorship on individual communications through human or algorithmic review. TikTok's operator ByteDance employs 6,000 censors, while Weibo, a Chinese version of Twitter, works with an automated system deleting 30 percent of posts considered contentious within 5 to 30 minutes and 90 percent within 24 hours after publication (Weber 76). Public discourse online is additionally guided by the so-called '50 Cent Army'. These paid users and moderators of platforms selectively introduce disinformation and propaganda or control conversations by directing them according to Party guidelines, with some scholars counting thousands (Arora) and others claiming there might be millions (Weber 77). This uncertainty is not coincidental. Both blocking of complete websites and censorship of individual communications are based on non-transparent filtering rules (Drinhausen 4). Equally, the extent to which paid commentators shape public opinion is not visible for ordinary users. The effect of this uncertainty is an increase of self-censorship to comply with what the society or government might consider unwanted communication (Gagliardone 108).

Thirdly, China is continuously perfecting online surveillance. Government bodies and private corporations are currently creating "the most comprehensive profiling of a population" (PoKempner 235-236). The developmental stages for an extensive social credit system that rates citizens' behaviour and assigns rights accordingly are expected to culminate in a

nationwide roll-out within 2020, as projected by the “Planning Outline for the Construction of a Social Credit System (2014–2020)”. Social credit systems, which are already applied to individuals and corporations in the preliminary stages, are intended to “shape a thick atmosphere in the entire society that keeping trust is glorious and breaking trust is disgraceful, and ensure that sincerity and trustworthiness become conscious norms of action among all the people” (State Council of the People’s Republic of China, *Planning Outline...*, para. I.3.).

Finally, China is making use of all of the mechanisms above by applying them to securitized topics, often framed by an argument of counter-terrorism. The most prominent example is the treatment of the ethnic and religious minority of Uyghurs in the region of Xinjiang. People in the predominantly Muslim region are required to download surveillance apps to their smartphones tracking behaviour on social media (Arora). Under the guise of “de-extremification”, users that are not in compliance with Party views, e.g. through certain forms of expressing their religion, are detained and brainwashed in re-education prisons resembling concentration camps (Arora; Kriebitz & Lütge 19). Not only is freedom of expression not guaranteed, unwanted communications are intercepted and citizens are punished and deprived of their ethnic, religious and political identity.

For the CCP, this comprehensive process of Internet regulation and its enforcement is not manageable without the compliance of companies. While Internet governance in the EU and the US is strongly influenced by the dynamics between legislators and private corporations, the economy in China is organised in a top-down manner (Przychodniak 5). Drawing a line between the largest ICT companies and government bodies is difficult, since many of them have party members in influential board positions (Jili 41-42). Thus, corporations act as an ally for the state to regulate their users, amplifying the governments possibilities to influence and censor online communication.

In return, the government invests heavily in its domestic technology sector, providing infrastructure, specialized education and a protected market. The CCP layed out long-term strategies which aim at being at the forefront of ICT innovation in 2030 (Kania 9) and holding enough power to shape global Internet governance by 2035, an attempt to spearhead the ongoing technological transformation after lagging behind on the last two industrial revolutions (Drinhausen 3-4). For China under Xi Jinping, ICTs are the key to continued economic development with a strong base in China and an element of foreign policy to accompany global investment (Przychodniak 5).

The Chinese market itself presents a unique situation for corporations, with the largest world population forming an enormous potential user base. Domestically, Chinese companies

are allowed to compete freely with each other, fostering innovation and technological advancement (Weber 79). Through strong protectionist measures the market is shielded from foreign competitors (Drinhausen 2). These are discouraged by demands such as the government's mandate to localize data in China, ensure access for government agencies and cooperate with inquiries aiming at obtaining personal data (PoKempner 230, 235). On the other hand, when Chinese companies grow large enough to expand abroad, the state increases its investment and control, building up corporations as national champions, a model that Lewis describes as a "bifurbication of state capitalism" with "one set of rules for Chinese companies in China, another set for Chinese companies as they compete in the rest of the world" (18).

Rachel Odell views China's authoritarian control over the Internet as a weakness, claiming

> the CCP's reliance on performance-based legitimacy also imbues it with a paranoid fear that if it somehow fails to perform, it will be faced with massive unrest that could topple the regime. This paranoia has led Beijing to grasp at technological levers of power (...) to manipulate the population into quiescence. (124)

Indeed, China managed to securitize the entire sphere of online communication, positing free speech and access to services outside the 'Great Firewall' as existential threats to national security and economic development. With each subsequent year of economic growth and a continuing emphasis on development in public discourse, the oppressive regulation of the Internet gains more legitimacy and acceptance as a protective measure that succeeds in contributing to development goals. Xi Jinping made this connection clear in a 2015 speech, claiming: "Security and development are like the two wings of a bird or the two wheels of a cart. Security ensures development, and development is what security is aimed at" (n.p.). With China's economic success increasingly on display on the international stage, the question is how other emerging economies react to the securitized development model it presents.

### 4.3.2 Multilateralism and China as a Game-Changer

Particularly Western democracies voice fears that China's influence on Internet governance will lead to a more authoritarian web. At the 2015 World Internet Conference (WIC) in

Wuzhen, Xi Jinping sent mixed messages regarding his vision of the future of global Internet regulation. A major point included Internet sovereignty:

> The principle of sovereign equality enshrined in the *Charter of the United Nations* is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. (Xi)

Although the speech later goes on to praise multilateral cooperation, Xi makes clear that he will not tolerate interference with China's Internet governance and is not supportive of overreach into other states' governance. At the same time, he stresses the importance to "formulate global Internet governance rules, so that the global Internet governance system becomes more fair and reasonable and reflects in a more balanced way the aspiration and interests of the majority of countries" (Xi). This apparent contradiction can be explained by the complexity of China's strategy of influencing global Internet regulation. The government recognized that efficiently regulating the Internet is only possible by continuously adjusting global standards (Cave et al. 8). China aims to strengthen relations between states at the expense of non-state actors and integrating Internet sovereignty into this multilateral framework. Aligning the interests of its stakeholders active abroad with the CCP's agenda, China influences global governance on several levels including through IOs, multilateral and bilateral agreements, party-to-party relations, investments and loans. The decisive advantage towards other actors is that these actions are coordinated and thereby much more effective, as a detailed analysis demonstrates.

A central means for China to increase its status as a norm-shaper in Internet politics is gaining influence in IOs, where the government sees a platform for multilateral discussions without non-state actors. With the US withdrawing funds and political leadership from IOs, China fills the power vacuum carried by clientelistic relationships to other countries that are indebted to it. Effects can be seen in the review procedures of human rights treaty bodies, where China advocates for less participation of non-state actors, particularly human rights NGOs (Brooks 172). Investigators like the Special Rapporteur on Freedom of Opinion and Expression David Kaye are chastised for their critique of non-practicable legislation and pointing out the role of Chinese companies in censoring free communication; the UNHCHR is

denied funding after meeting with non-governmental activists; and China leads a movement to shut out stakeholders from civil society from the Economic and Social Council (Brooks 172-73). China applying pressure to reshape procedures in IOs with the aim of excluding non-government views shows that its concept of multilateralism as a restructured version strictly among acting governments. This would create a toothless world order without the means of holding states accountable to human rights.

Besides transforming existing fora at the UN or other IOs, China also forms new groups with like-minded states, often narrowed down to specific fields of cooperation, such as the Shanghai Cooperation Organization, the International Code of Conduct for Information Security or the World Internet Conference, all of which can be seen as alternative models to the formerly inevitable Western multi-stakeholder approach to global Internet governance (Gagliardone 101-02). China's proposals tend to resonate with governments of the Global South because they demand less compliance with the reform goals of human rights treaties, NGOs and corporations that are often perceived as Western interference. Rather than having to deal with European or US unilateralism, overpowering corporations from the ICT sector or monitoring NGOs, authoritarian governments in particular see the Chinese model as a validation of sovereignty that otherwise finds little acknowledgement.

To change global institutions, China focuses on collaborations with incumbent governments rather than oppositions or civil society stakeholders, which is exemplified by party-to-party relations. Hackenesch investigated relations between African parties and the CCP finding "that in some countries China has indeed already become an alternative cooperation partner for African governments, not only in terms of economic cooperation, but also as a partner to cooperate on African governments' survival strategies" (218). While Hackenesch admits that the exact effects of party-to-party relations are difficult to trace, she cannot exclude that the CCP plays a role in supporting authoritarian governments in their use of coercion or narrowing down the possibilities for political contestation (215). As chapter 5 discusses in greater detail, this was particularly the case in Ethiopia where cooperation with China was key to enabling the government's monopoly as an Internet provider.

China's guiding principle in relations with the Global South is that it directs its cooperation and support almost entirely at governments, regardless of whether they are democratic or authoritarian. Gagliardone refers to this as an "actor-based approach" rather than an "issue-based approach" that is preferred by most Western states (43). This becomes evident in digital development programmes, where decisions are informed by intergovernmental cooperation and multi-stakeholderism is dismissed (Gagliardone 63).

Development interactions between China and African states are based on a conditionality different from projects emerging in the West. China's aid is not issued in the form of traditional official development assistance (ODA), but through loans and aid that support Chinese investments related to African development goals (Gagliardone 42). For instance, funding for African states made available through the government-owned China Exim Bank is tied to provisions to that Chinese contractors be given preference in tenders (Cave et al. 10). The CCP sees these investments as an important element of growing China's ICT sector by expanding to new markets and providing an ideational alternative to the Western conditionality of classic ODA (Gagliardone 37).

Unlike aid by the EU or the US, which is often tied to good governance conditions such as compliance with human rights, China provides loans to democracies and autocracies alike. This policy was explained by president Xi during a 2018 speech at the Forum on China-Africa Cooperation (FOCAC):

> We follow a "five-no" approach in our relations with Africa: no interference in African countries' pursuit of development paths that fit their national conditions; no interference in African countries' internal affairs; no imposition of our will on African countries; no attachment of political strings to assistance to Africa; and no seeking of selfish political gains in investment and financing cooperation with Africa. (n.p.)

While this approach is a welcome boost for any governments following China's model of Internet sovereignty, the lack of distinction between projects that comply with human rights and those that fail to do so has been noted by the UN. The UN Committee on Economic, Social and Cultural Rights pointed out that several supported projects "resulted in violations of economic, social and cultural rights in the receiving countries" and called on China to "adopt a human rights-based approach to its policies of international cooperation" (4).

Development cooperation with Chinese participation must be viewed foremost as financial investments. According to Chris Alden, China became the leading source of foreign investment in Africa in 2013, when funding to the continent rose to US$26 billion (Alden 88-89). In 2019, Ogubay and Lin retraced a total sum of US$60 billion: "US$15 billion grants, interest-free loans and concessional loans; US$20 billion of credit lines; US$10 billion special fund for development financing; US$5 billion special fund for financing imports from Africa; US$10 billion investment by Chinese firms" (318).

Investments by private corporations usually go towards accessing the market in African states and developing infrastructure for their services. Compared with big data corporations in Silicon Valley, Chinese ICT companies are more assertive in their market-drivenness in public, focusing on economic growth as the cornerstone of development. The corporations' drive to access more user data in Africa overlaps with the CCP's aim to promote development over human rights (Weber 78). Reporters Without Borders observe this development with concern, viewing tech corporations that support oppressive Internet governance in China as a threat to other states and doubting their neutrality due to the involvement of CCP members (Cave et al. 9).

Chinese big data corporations like Huawei, ZTE and Tencent, all of which have Party committees in their decision-making bodies export surveillance and censorship technology to states like Ethiopia, Zambia or Zimbabwe (Weber 78). While the economic interests of Chinese companies do not differ from those at Google or Facebook, they are even less committed to investment restrictions concerning business and human rights or CSR (Gagliardone 32).

Since 2016, the ventures of Chinese corporations abroad are influenced by the trade war between China and the US, which took a similar path towards protectionism under the Trump administration. Some scholars see the competition as an economic cold war and a chance for China to pull ahead (Przychodniak 6). Several tech companies found themselves in the middle of a political crossfire such as Huawei which is excluded from several infrastructural projects for a lack of data protection or ByteDance's TikTok which is banned in India and prohibited from making transactions in the US (Swanson).

Overall, China and its corporations are careful in maintaining a certain extent of neutrality in their activities in Africa. In practice, however, that translates to increased cooperation with autocracies with suppressive Internet governance, because these governments do not have access to US or EU funding tied to stricter conditions. Nevertheless, China has also invested in liberal democracies and supported countries committed to developing an open Internet (Gagliardone 159). China's engagement with the Global South explicitly lacks a narrative that frames its own Internet regulation as a model or blueprint for other countries (Gagliardone 6, 15). Instead it aims at exporting the principle of Internet sovereignty which then provides the basis for governments to reject compliance with human rights.

Developments around the Belt and Road Initiative (BRI) show that China's strategy does not end there. In the long run, loans can turn into economic pressure which then turns

into political pressure. Former US Secretary of State Rex Tillerson articulated the fear of potential debt traps for dependent states, claiming that "the financing models are structured in a way that the country, when it gets into trouble financially, loses control of its own infrastructure or its own resources through default" (qtd. in Ogubay & Lin 311). While Tillerson's perception is both biased and hypocritical, there is some grounds to his argument that China uses loans as a calculated form of diplomacy to evoke first gratitude and later loyalty from African governments for decisions in international fora (Zhang 32). A typical example is political pressure to subscribe to the One-China policy which delegitimizes any claims to independence by Taiwan (Zhang 29). Observers note that similar strategies are in debated with regards to shaping norms and standards in Internet regulation (Kania 10). Thus, Chinese loans are only unconditional with regard to human rights and good governance, however, a different kind of conditionality is based on recognizing China's sovereignty in all national decisions, whether they concern geopolitical borders or Internet governance.

Critics have noted that there is possibly a counter effect to China's approach to development cooperation. Employing modernisation theory, Fodei Batty argues that, with increased access to the Internet, African economies will grow and produce an educated middle class that strives for democracy and liberalisation (151-153). However, dependency theory allows for predictions of a different kind: Following the developments outlined above, it is likely that dependent states increase their levels of debt while selling out their valuable resources, data, to dominant actors. Meanwhile, technological development will not wait until African states 'catch up', nor will it be 'achieved' when the Internet eventually spreads across the continent. Rather economic inequalities will continue to grow and open up new spaces for exploitation. For a dependency theorist, China's form of aid through loans reinforces the status quo rather than shifting relative power relations in such a way that African states can develop from norm-takers to norm-shapers in the field of Internet governance. The political sovereignty promised by China is merely a fig leaf, unable to veil the economic dependence waiting to be leveraged at any time to enforce political loyalty.

A typical element of relations between dominant and dependent states pointed out by dependency theorists are ties between the countries' respective elites. "These elites are typically trained in the dominant states and share similar values and culture with the elites in dominant states. Thus, in a very real sense, a dependency relationship is a voluntary relationship" (Ferraro). This reflects China's soft-power approach to influencing Internet governance in Africa. Particularly African media professionals and political leaders are targeted by China for exchange programmes or scholarships, with some critics alleging a

training in “Chinese information control techniques” (Weber 77) and others seeing a “cordial relationship” (Oginni & Joash 164). The Kenya-based subsidiary of China’s state-controlled TV station CGTN (formerly CCTV) is not a mere propaganda station, however, it covers events where China’s Internet vision is promoted, such as the 2015 Wuzhen WIC, and highlights the achievements of Chinese companies in the area of development (Gagliardone 112). Furthermore, China’s focus on supporting the state rather than other actors in its development policy promotes a societal structure that also sees media, including Internet platforms, as linked to public institutions and their values (Gagliardone 84). The recent popularity of TikTok can be seen as a success for China’s soft-power approach as it marks the first time a Chinese platform under state influence achieved such an international range (Brühl).

As regards soft-power approaches, China’s influence in Africa still pales in comparison to US and European culture, media and free-market capitalism. China aims at deconstructing these ties, by pitching itself as an alternative partner emerging from the Global South and pointing out commonalities with African states in a shared colonial experience (Ogubay & Lin 313). The “five-no” approach to development cooperation can be seen as a rejection of the conditionality of aid that shapes power structures between Western and African states. Instead, China attempts to replace it by a show of solidarity through South-South cooperation. The FOCAC summits regularly reinforce these ideas. At the same time, they provide a platform for exchanging “new modalities of delivery of transferable policy lessons to Africa” (Alden 93). Within this framework, China is able to portray itself not as a compulsory model, but as a leader for states of the Global South to follow. As Jili puts it, “Beijing’s claims do not deny the possibilities of other nations copying and adapting Chinese modes of governance, particularly after receiving support to build ICT infrastructure” (25).

## 5 Internet Regulation in Africa

After analysing the dominant powers’ different visions of Internet regulation as an independent variable, evaluating Internet governance in Africa gives an impression of how effective their strategies are. As emphasised above, it is vital to see African policies not as a mere reflection of the American, European and Chinese endeavours, but as a result of interactions. Nevertheless, the structural differences between economically dominant and dependent states constitute that the majority of these interactions are set on a non-level playing field.

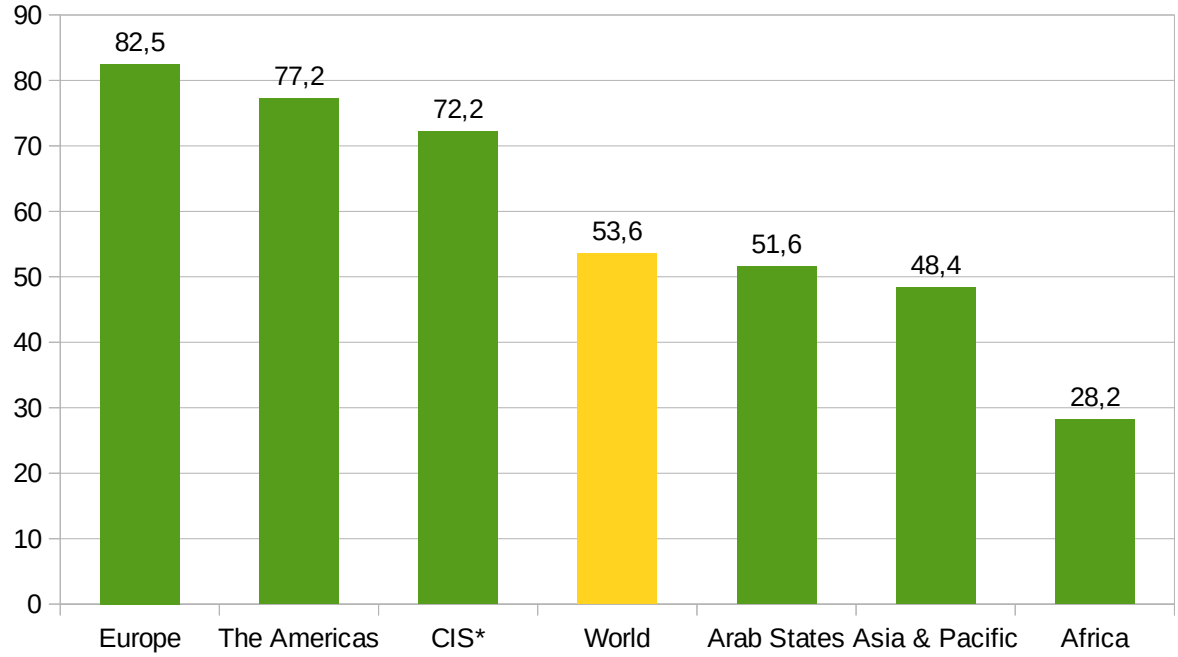
For many incumbent governments in Africa, Beijing's presence as an alternative partner for trade and development projects is welcome, while opposition leaders express concern about the unconditionality of support for autocratic rulers (Batty 159). In civil society, which is still entrenched in the legacy of European colonialism, fears of a new form of imperialism culminated in protests against China and its perceived overreach (Batty 160, 162). At the same time, calls for economic growth, justice and political inclusion rose to demonstrations fuelled by the mobilizing effect of social media platforms (Arnould et al. 4). While the increasing dependence on online services through all parts of private and professional life is becoming an inhibiting factor for complete Internet shutdowns to suppress demonstrations, selective blocking of platforms and censorship are still widespread.

This chapter briefly outlines the development of Internet infrastructure in Africa before addressing the common framework for governance provided by the African Union (AU) and the African Commission on People's and Human Rights (ACPHR). The case studies of Ethiopia, Ghana, Kenya, Nigeria, and Zimbabwe show that relations to the US, the EU and China play a crucial role in shaping Internet regulation.

## 5.1 An Overiew of Internet Infrastructure and Regulation in Africa

As in most areas of the world, the digital divide within African states separates Internet users from a large part of the population that remains offline. 2019's data by the ITU in fig. 3 shows that the estimated percentage of individuals using the Internet in Africa, exluding the Arab speaking countries of the North, is lower than in other regions of the world.

Fig. 3: ITU estimates of worldwide percentages of Internet users in 2019.




*Commonwealth of Independent States

Source: ITU, *Measuring Digital Development* 2.

Internet World Stats compiled additional statistics based on ITU rates and additional data from Internet browser and market research institutes (fig. 4).

Fig. 4: Internet World Stats estimates of percentages of Internet users in 2019.

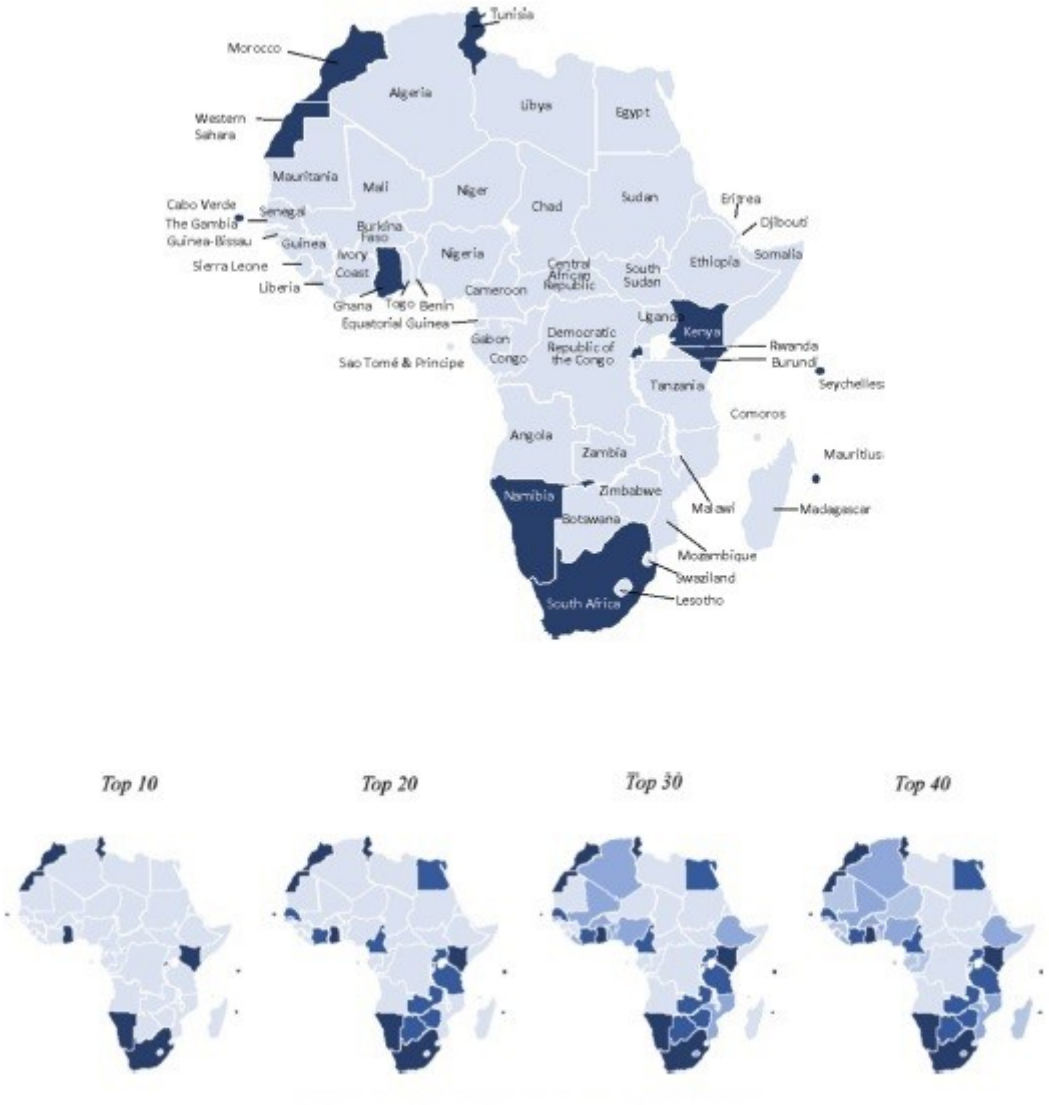
| State/Region | Population (2020 estimate) | Internet users 31 December 2019 | Penetration (Percentage of Population) |
|---|---|---|---|
| **Ethiopa** | 114,963,588 | 20,507,255 | 17.8 % |
| **Ghana** | 31,072,940 | 11,737,818 | 37.8 % |
| **Kenya** | 53,771,296 | 46,870,422 | 87.2 % |
| **Nigeria** | 206,139,589 | 126,078,999 | 61.2 % |
| **Zimbabwe** | 14,862,924 | 8,400,000 | 56.5 % |
| **Africa** | 1,340,598,447 | 526,710,313 | 39.3 % |
| **World** | 7,796,949,710 | 4,585,578,718 | 58.8 % |

Source: Internet World Stats.

Within each state, there are large divides along the lines of gender, race, income or between rural and urban households (Mutsvairo & Ragnedda 14). It should be noted that despite decreasing prices, Internet access in Africa remains expensive, taking up around 15% of income per capita for mobile access and 30% of income per capita for desktop access (Musa 75).

The ways in which people use the Internet depends on more than just whether or not access is provided. In 2019 Joubert et al. created an index of big data readiness in African states by evaluating 170 different variables categorized into 15 “drivers”: size, engagement, usage; innovation, capital, technology adoption; infrastructure, affordability, digital openness; trust and security, digital well-being, future readiness; regulations and institutions, human resources and impact (104-06). According to the authors, Kenya and Ghana are the most big data ready among the case study countries in this paper, followed by Zimbabwe and later Nigeria and Ethiopia, with all five states ranking among the continent’s top 30 (106).

Fig. 5: Top 10, top 20, top 30 and top 40 African Countries according to the Big Data Readiness Index by Joubert et al.




Source: Joubert et al. (106).

Assessments like these are particularly valuable for public and corporate investors who can include them into their market analysis when expanding services to African states.

Concerning Internet regulation, Africans often have limited possibilities to make their voices heard in the law-making process (CIPESA 8). However, Oginni and Joash identify a potential of change emerging from platforms themselves, claiming "[s]ocial media has emerged as a fundamental game changer to complement the shortfalls of traditional public policy process by connecting governments or policymakers directly to citizens" (163). Autocratic governments across Africa are often unwilling to accept that. Between 2015 and

2019, 20 African countries used selective disruptions of social media sites as a means of censorship arguing that these platforms "spread disinformation, propagate hate speech, and fan public disorder and undermine national security" (CIPESA 5). Reporters Without Borders quote an unnamed African leader asking researchers at a Namibian university "If China could become a world power without a free Internet, why do African countries need a free internet?" (11).

The US-based NGO Freedom House compiled several strands of data for their assessment of Internet freedom in 65 states, including all case study states except for Ghana, as well as five EU member states and an evaluation of China and the US (Fig. 6). The resulting "Internet Freedom Score" takes into account obstacles to Internet access, limits on content and violations of user rights and includes information from numerous NGOs, academia and journalists (Freedom House, "Internet Scores"). This comparison is a first indicator for the upcoming detailed analysis and shows the African case study states ranking between relatively high-scoring Western actors and China which is at the bottom of the scale.

Fig. 6: Levels of Internet Freedom according to Freedom House.

| **Country** | **Total Score and Status (max. 100)** | **Obstacles to Access (max. 25)** | **Limits on Content (max. 35)** | **Violation of User Rights (max. 40)** |
|---|---|---|---|---|
| **Ethiopia** | 28 – Not free | 3 | 12 | 13 |
| **Ghana** | no data | no data | no data | no data |
| **Kenya** | 68 – Partly free | 17 | 28 | 23 |
| **Nigeria** | 64 – Partly free | 17 | 26 | 21 |
| **Zimbabwe** | 42 – Partly free | 7 | 19 | 16 |
| | | | | |
| **China** | 10 – Not free | 8 | 2 | 0 |
| **EU*** | 79,4 – ** | 22,2 | 29,2 | 28,0 |
| **USA** | 77 – Free | 21 | 31 | 25 |

Source: Freedom House "Internet Freedom Scores".

*The EU score is the average score of the five member states assessed by Freedom House, namely Estonia, France, Germany, Hungary and Italy. The average was aggregated by the author and should be seen only as an indicator without decisive value.

** Since the EU score expresses an average, there is no overall assessment concerning Internet freedom.

While the five case study states are not representative of the entire continent, they can provide an indication of how relations between African states and the dominant powers presented in chapter 4 effect compliance with human rights in regulating the Internet. As of August 2020, all five of them have unique diplomatic relations with the dominant powers, with Zimbabwe being the most recent state to resume its contacts to the EU after a long embargo. Before carving out the differences between the states, it is crucial to analyse the common ground for the rights to freedom of expression and privacy that is provided by the AU, the African Commission on Human and People's Rights (ACPHR) and the African Court on Human and People's Rights (the Court).

### 5.2 The African Union

The regional human rights system in Africa is based on the African Charter on Peoples and Human Rights (the Charter) and continuously evolving to face challenges in the area of Internet regulation. The AU, the ACPHR and the Court work together to set a framework for states' legislations, a challenging task considering the fast-developing online world. While all African states except for Morocco ratified the Charter, the Protocol establishing the jurisdiction of the Court was only ratified by 30 states, among which are the case study states Ghana, Kenya and Nigeria – Ethiopia and Zimbabwe both signed in 1998 without ratifying it (African Union, "Establishment of an African Court").

The right to freedom of expression is constituted in article 9 of the Charter, which states "1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law" (Organization of African Unity). The Commission's 2019 Declaration of Principles on Freedom of Expression in Africa and Access to Information in Africa provides details as to how this should be applied regarding the Internet. Principle 37 focuses on the level of access, stating that "States shall, in cooperation with all relevant stakeholders, adopt laws, policies and other measures to provide universal, equitable, affordable and meaningful access to the internet without discrimination" (ACHPR). Nyokabi et al. add that the Charter's right to economic, social and cultural development as established in article 22 also encompasses access to ICTs which should be ensured by states (150). The Declaration's principle 38 prohibits interferences "through measures such as the removal, blocking or filtering of content, unless such interference is justifiable and compatible with international human rights law and standards" (ACHPR).

Principle 39 concerns the regulation of intermediaries, which includes online platforms like social media, declaring

> 3. States shall require internet intermediaries to ensure that in moderating or filtering online content, they mainstream human rights safeguards into their processes, adopt mitigation strategies to address all restrictions on freedom of expression and access to information online, ensure transparency on all requests for removal of content, incorporate appeal mechanisms, and offer effective remedies where rights violations occur.
> 4. States shall not require the removal of online content by internet intermediaries unless such requests are:
>
> a. clear and unambiguous;
>
> b. imposed by an independent and impartial judicial authority, subject to sub-principle 5;
>
> c. subject to due process safeguards;
>
> d. justifiable and compatible with international human rights law and standards; and
>
> e. implemented through a transparent process that allows a right of appeal (ACHPR)

The Declaration also weighs in on the process of regulation itself, calling for a "multi-stakeholder model of regulation" and the establishment of politically and commercially independent regulatory bodies in principle 17 (ACHPR).

While the right to privacy does not exist in the African Charter, the AU's 2014 Convention on Cyber Security and Personal Data Protection (the Malabo Convention) aims at filling this gap. Regarding personal data, it establishes inter alia the "[p]rinciple of consent and legitimacy", the "[p]rinciple of transparency" and the "[p]rinciple of confidentiality and security" (article 13, principles 1, 5 and 6). As of August 2020, however, only 14 out of 55 member states signed the Malabo Convention and only eight ratified it (African Union, "List of Countries"). Furthermore, critics point out the lack of considerations applying specifically to the big data corporations, which provides uncertainty for both private and state actors (Onuoha 60). Additional guidance is provided by the ACHPR's 2019 Declaration, which explicitly forbids states from resorting to "indiscriminate and untargeted collection, storage,

analysis ... of a person's communications" in principle 41 and obligates them to adopt data protection legislation and independent oversight bodies in principle 42 (ACHPR).

Onuoha argues that most African states that create data protection legislation do so without regard to the Malabo Convention and often make more specified laws (60). According to Greenleaf, national laws before the Convention resembled legislation in the EU but faced problems of enforcement (13). Overall, the AU's framework appears to be ineffective at uniting national legislators on the issue of data protection. Some experts argue for a new Bill of Data Rights based on the principles put forth by the AU to prevent corporations and states from endangering human rights online (Okolloh & Wekwete).

More progress has been made on the subregional level among the member states of Economic Community of West African State (ECOWAS), the East African Community (EAC) and the Southern African Development Community (SADC). Observers highlight the Supplementary Act on Personal Data Protection within ECOWAS, which was added to the ECOWAS treaty in 2010 and is influenced by the EU Data Protection Directive, a predecessor to the GDPR (Greenleaf 16). Agreements in other regions have taken only non-binding forms (Onuoha 59). Onuoha remarks that "disharmony at the regional level with respect to policy formulation generally undermines levels of compliance" (60). The issue is even broader, since there are additional laws on a national, continental and global level, with a potential to create uncertainty through over-regulation. Additional subdivisions are informed by the blocs of former colonial affiliation (Onuoha 60).

Overall, dominant foreign actors rarely take up relations directly with the AU to influence Internet regulation, preferring either bilateral agreements or international fora. Because of its (theoretical) potential to bundle member states' collective interests, the AU can been seen as both a facilitator and an obstacle to arrangements with foreign actors, depending on their commitment to human rights. There are some examples worth pointing out.

The Policy and Regulation Initiative for Digital Africa (PRIDA) is a joint project by the EU-AU partnership with a budget of €8 million, €7.5 million of which is paid by the EU and the rest by the ITU (The Africa-EU-Partnership, "Action Document..." 1). Besides addressing issues of access, its objective is to

> create a more harmonised and enabling legal and regulatory framework for the use of ICT for social and economic development, with an emphasis on boosting the spectrum market across Africa ... based on three pillars:
>
> a) efficient and harmonised spectrum utilisation,

> b) harmonisation of measurable ICT/Telecommunications policy, legal and regulatory frameworks
> c) African decision makers' active participation in the global internet governance debate (The Africa-EU-Partnership, "Action Document..." 9)

While the EU's regulatory approach is not specifically set forth as the model to follow, the Charter of Fundamental Rights constitutes that EU projects adhere to it. The AU-EU cooperation also includes a Human Rights Dialogue, but direct impacts on Internet regulation are not discernible (The Africa-EU Partnership, "AU-EU Human Rights Dialogue").

The US engages with the AU primarily through the African Union Commission – U.S. High-Level Dialogue. This has been used to promote a US approach to Internet regulation and includes a focus on "Digital Economy and Cyber Cooperation" aimed at capacity building projects for ICT officials and providing workshops for cybercrime and cyber strategies (US Department of State, "US Partnership with the African Union"). The 2019 summit ended in a US "commitment of additional programmatic support ... to increase technical training opportunities for African ICT regulators and policy makers" (African Union, "Joint Communique..."). The US approach is directed at stakeholders in governments, businesses and civil society.

The main platform for cooperation between China and the AU is the Forum on China–Africa Cooperation (FOCAC). The 2018 FOCAC Beijing Action Plan expresses a Chinese emphasis on securitizing online spaces in Africa stating that "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" (Forum on China–Africa Cooperation). Earlier in 2018, a story published in *Le Monde* caused concern by claiming that the AU's Addis-Ababa headquarters, which run on digital infrastructure provided by Huawei, had been used by Chinese spies to gain access to the Union's data (Tiloune and Kadiri). China repeatedly rejected these allegations, most recently when they were raised again by US delegates at the 2019 Web Summit, where a spokesperson for China's Foreign Ministry said: "It is nothing but fake news cooked by Western media and has long been thrown into the dustbin by our African friends. ... It is apparently a despicable ploy driven by ulterior motives" (qtd. in Olander). The African Union itself has never released an official statement concerning the allegations.

The attempts to create a framework for Internet regulation at a continental level had limited effects on human rights of users in AU member states. The African human rights

framework is not particularly effective in its enforcement mechanism, especially in comparison with the ECHR. As a political and economic body, the African Union gives impulses, but struggles with ensuring compliance. One reason is the lack of cooperation between the Commission and the Court (Viljoen 94). Critics also point out that the AU's and regional groups' top-down approach to setting Internet governance standards is one of the reasons that adoption and implementation by member states are hesitant (Onuoha 60). Another potential reason could be that member states face much more pressure than the AU to provide legislation that allows foreign actors to pursue their goals within the country.

### 5.3 Ethiopia

For an analysis of Ethiopia's Internet governance, it is important to consider a political shift since the administration of the current prime Abiy Ahmed, who introduced several reforms since taking office in April 2018. Before Abiy, the country saw over two decades of authoritarian rule by the Ethiopian People's Revolutionary Democratic Front (EPRDF), a coalition of four parties. Although Abiy himself was elected as a candidate of the EPRDF, he was central to dissolving the coalition in 2019 after 24 years of consecutively providing the head of government (Gardner). After taking office, parts of the agenda to liberalise Internet regulation were implemented, but 2020 saw new blocking and oppression (Netblocks).

Internet regulation in Ethiopia follows a core principle: the Internet is a matter of the state. After completely denying access to the Internet during its early technological rollout before 2000, the government created a unique system in which Internet service provision is a state monopoly (Gagliardone 73). Private actors were completely banned and are not present in the market as of August 2020. A market without competition is one of the reasons why Ethiopia still has one of the lowest rates of Internet penetration in Africa with 17.8 percent (Gagliardone 119; Internet World Stats). The government announced in July 2020 that, for the first time, it plans to award licences to two multinational mobile companies (Fick).

Several of Ethiopia's oppressive means to control the Internet stand in conflict with the 1994 constitution which establishes "freedom of expression without interference" and "[p]rohibition of any form of censorship" in article 29 (Constitution of the Federal Democratic Republic of Ethiopia). Interference is justified mainly by the 2009 Anti-Terrorism Proclamation, which not only penalizes terrorist acts, but also their encouragement in article 6.

> Whosoever publishes or causes the publication of a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission or preparation or instigation of an act of terrorism stipulated under Article 3 of this Proclamation is punishable with rigorous imprisonment from10 to 20 years. (Federal Republic of Ethiopia).

The former Prime Minister Meles Zenazi pointed out, that this Proclamation is modelled after Western legislation, claiming the government "took from America, England and the European model of anti-terrorism laws" (qtd. in Gagliardone 137). Indeed, article 6 is almost a verbatim copy of the United Kingdom's Terrorism Act of 2006, however, prosecutors in Ethiopia abuse the Proclamation to label groups promoting freedom of expression or gender diversity as terrorists (Gagliardone 130, 137).

The right to privacy is established by article 26 of the Constitution with several exceptions for "compelling circumstances" and laws aimed at "national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others" (Constitution of the Federal Democratic Republic of Ethiopia). However, this right is barely recognized by courts (Jili 40-41), leaving civil society with little legal possibilities to protect itself efficiently against the government overstepping its boundaries. This led to the imprisonment of bloggers accused of collaboration with "foreign human right activist organizations" (Gagliardone 85). Between 2009 and 2014, 13 our of 33 people convicted under the Anti-Terrorism Proclamation were journalists (Gagliardone 135).

Under EPRDF rule, the government resorted to complete Internet shutdowns when facing political unrest and long-term blocking of individual websites of media outlets, human rights activists, sites relating to the LGBTI* movement or from the political opposition (Evdokimov). A particularly controversial case of censorship concerns the *Oromia Media Network* which is viewed as a crucial source of independent journalism in the country and run by the diaspora (Jili 38). 15 more large media websites were blocked during a wave of protests in 2016 (Evdokimov). Additionally, the EPRDF government employed paid online trolls to manipulate online discourse in its favour (Freedom House, "Ethiopia").

The new prime minister introduced some reforms, but the Internet in Ethiopia remains restricted. Shortly after his election, Abiy released bloggers and journalists and stated his intention to liberalise Internet governance (Gagliardone 159). 264 websites were unblocked, including those of the *Oromia Media Network*, human rights NGOs and LGBTI* activists

(Netblocks). However, Internet shutdowns continued. After civil unrest in the Amhara Region in 2019, the messenger services WhatsApp and Telegram were blocked and later unblocked (Netblocks). In June and July 2020, the Internet was shut down for almost two weeks to disperse protests after the killing of musician and social activist Haacaaluu Hundeessaa (Access Now). As Freedom house notes, interferences are not officially declared, there are no lists of blocked sites nor transparent criteria for blocking decisions ("Ethiopia"). This leads to widespread self-censorship online, particularly among the LGBTI* community which suffers from the criminalisation of same-sex relations (Freedom House, "Ethiopia").

The Ethiopian government made heavy use of the US security agenda after 9/11. Gagliardone writes that the establishment of the Anti-Terrorism Proclamation was "[f]ramed as an attempt to comply with requests from the United Nations and the United States tot take the fight against international terrorism to a global level" (133). A further step was taken in 2011 with the re-establishment of the Information Network Security Agency (INSA), an intelligence service "shaped in the guise of the US National Security Agency (NSA)", with a similar approach built on heavy Internet surveillance (Gagliardone 135). In 2017, Human Rights Watch accused the NSA itself of providing Ethiopia with surveillance technology and training (Horne).

European actors equally participated in supporting the Ethiopian surveillance sector. Private corporations from the UK, Germany and Italy provided authorities with monitoring technologies enabling access to computer's hard-drives, cameras and microphones (Jili 32f; Gagliardone 138). Ethiopia maintains diplomatic relations with both the US and the EU, but its most important foreign partner is China.

In 2006, Ethiopia took a large step to advancing access to Internet by signing the largest deal in the African history of telecommunication with the China Development Bank and ZTE, a loan over US$1.5 billion (Gagliardone 78; Jili 26). 14 years later, ZTE is still a major partner for infrastructural projects launched by state-owned Ethio Telecom, but the company faces allegations of facilitating human rights violations. ZTE's technology allows authorities to access not only text and audio messages, but also enables real-time tracking of smartphone users' locations, information which is used against bloggers and journalists (Freedom House, "Ethiopia").

At the regulatory level, China supported reforms in the justice sector (Hackenesch 215). Hackenesch argues that the EPRDF was the African party with the closest ties to the CCP and "China has supported government measures to strengthen the effectiveness of state institutions and the usage of low-intensity coercion" (213).

Most importantly, China allowed Ethiopia to maintain its monopoly in terms of providing the Internet through the state. With a total of US$3 billion in loans, state providers were kept afloat without having to open the market to private actors (Gagliardone 70). As Jili argues, without China "the EPRDF would have been forced to liberalize or continue to lack connectivity" (27-28). This could have forced the government to loosen its tight grip on the Internet by cooperating with private actors with at least a basic level of data protection.

The role of China in shaping Ethiopian Internet policy is controversially discussed in Ethiopian politics. On the one hand, Sebhat Nega claims that "China has the most informed people in the World. [Ethiopia] needs the China model to inform the Ethiopian people" (qtd in Gagliardone 92). On the other hand, former Prime Minister Hailemariam Desalegn emphasized that "[i]f you see democracy you cannot take the Chinese way" (qtd. in Gagliardone 96).

Ethiopia's suppressive Internet governance picks up several elements put forward by foreign actors, particularly the US and China. Gagliardone claims that China has been "quietly taking care of the material implementation of a highly centralized and securitized information space" while the US is "offering the discursive terrain for Ethiopian authorities to justify the creation of such space" (10). By making use of opportunities provided economically dominant actors, the Ethiopian government continuously increased its capacities to control online communication. Even after a change in leadership, this results in human rights violations and one of the most restrictive webs on the continent.

### 5.4 Ghana

In 1994, Ghana was among the first Sub-Saharan states connected to the Internet (Africafex 5). While it continues to struggle with issues concerning access, its legal framework and executive regulation have received praise. An analysis of Internet governance in the country shows that influence from foreign actors is not as strong as in other states, mainly because the country boasts a strong civil society.

Ghana's economy has an open market for telecommunications. This was pushed for by the World Bank, which encouraged liberalisation and privatization, sparking competition among regional, national and international ICT corporations and reduced prices for customers (Gagliardone 60). Ghanaian Internet users are increasingly drawn to social media platforms, which were used by 20 percent of the population in January 2020 (Kemp).

The legal framework for laws affecting freedom of expression and the right to privacy is set by the Constitution's articles 18, protecting the privacy of "correspondence or communication", and 21, guaranteeing "freedom of speech and expression, which shall include freedom of the press and other media" (Constitution of the Republic of Ghana). Africafex, an advocacy group for freedom of expression, compliments the country's adherence to this right and it's media landscape as "one of the freest on the continent" (5).

Below the constitutional level, several laws regulate online communication. The 2008 Electronic Communications Act and the 2012 Data Protection Act sparked controversial debate among NGOs, who claimed that they lack sufficient requirements for law enforcement agencies to surveil Internet users (Africafex 8). Nevertheless, Africafex views Internet freedom in Ghana positively, noting "no reported incidents of government interference in the rights of citizens to freely use social media" (11). The same is true for Internet shutdowns. The police threatened to shut down social media during the 2016 elections, but this triggered heavy backlash from civil society until the plans were abandoned (Africafex 13).

Ghana's active civil society is perhaps the main reason why the country can be seen as a model for Internet governance in Africa. Ghanaians' strongly advocate for multi-stakeholder approaches to national and international Internet regulation (Gagliardone 59). The country was at the forefront of creating the West Africa IGF, providing a space for several IOs, NGOs, private corporations, academics and politicians to come together (Gagliardone 63).

Ghana maintains relations with all the economically dominant powers analysed in chapter 4. In terms of investments in the country's ICT sector, China's Exim Bank provided the largest loans in 2008 and 2010 amounting to US$180 million for the development of an e-government system (Jili 29-30). European and US investors passed on the opportunity because contracts were not awarded to private companies, while China has been willing to invest regardless of internal political decisions, as the former Ghanaian Deputy Minister of Information states:

> They have fewer conditions. And our engagement has been motivated mostly by economic conditions. This has been the case with all parties in Ghana. If you look at the different governments, they all made deals with China. The ideological factor has been diluted. (qtd. in Gagliardone 96).

Financial investments from China did not prevent Ghana from maintaining relations with other countries to discuss in Internet governance, particularly the US. During a 2018 trip to

Silicon Valley, Ghanaian Vice president Mahamudu Bawumia attempted to attract US investors by suggesting a loosening of regulations in favour of big data corporations: “We as a government want to set the framework, the environment, then move out of the way so that you guys can do what you do best” (Office of the President). A similar message was published by the US President’s Advisory Council on Doing Business in Africa, who visited Ghana in 2018 and concluded “more reform is needed to enable sustained growth of the digital economy, specifically regulatory conditions that allow U.S. companies to compete with domestic players” (9).

The EU is Ghana’s largest trading partner and continuously invests large sums to promote good governance in the country, allotting €75 million between 2014 and 2020 (European Commission, “Republic of Ghana...”). Aside from general projects aiming at strengthening the rule of law, there has recently not been much public exchange on Internet governance. This is possibly due to the fact that freedom of expression is rather well protected and the Ghanaian Data Protection Act already covers privacy concerns similar to the GDPR.

Foreign investments influenced the development of infrastructure in Ghana, but had little effects on the field of Internet regulation, where the country champions multi-stakeholderism at home and abroad. Ghana largely succeeded in basing its governance on demands expressed by its own civil society, which advocates for finding more consensus at regional and AU levels (Osiakwan).

### 5.5 Kenya

Over the last decade, Kenya developed one of the most innovative ICT sectors in Africa. Particularly digital payment is much more widespread than in the United States or most European states, with the mobile payment service M-PESA functioning as a monetary foundation for the country’s information society (Gagliardone 47). The digital landscape is mainly powered by private actors that push the boundaries set by the state and received support by an engaged civil society, particularly during the early stages of spreading Internet infrastructure (Gagliardone 83). Kenyan civil society played a crucial role in forming the East Africa IGF and stood up against attempts of securitizing online communication, stopping a suppressive Anti-Terrorism Bill in 2003 (Gagliardone 62, 139).

Since then, however, the government has used legislation to tighten its grip on the Internet. Although the 2010 constitution sets forth the right to freedom of expression in article

33, there are frequent violations (Constitution of Kenya). These are mainly enabled by the Security Laws Amendment Act of 2014 which states in article 12:

> A person who publishes, broadcasts or causes to be published or distributed, through print, digital or electronic means, insulting, threatening, or inciting material or images of dead or injured persons which are likely to cause fear and alarm to the general public or disturb public peace commits an offence and is liable, upon conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years or both. (Parliament of Kenya).

A similar development can be observed in terms of the right to privacy. It too is codified in the constitution in article 31 which protects individuals from having "information relating to their family or private affairs unnecessarily required or revealed" or "the privacy of their communications infringed" (Constitution of Kenya). However, NGOs report that corporations and public authorities collect data without oversight mechanisms and government agents enquire data from Internet providers without warrants (Freedom House, "Kenya").

The relationship between public and private actors is mutually beneficial, as it enables corporations to gather data on its users and provides law enforcement with enhanced possibilities. Particularly the National Intelligence Service profits from the securitization of online communication that has continuously gathered momentum since violence broke out during the 2007 and 2008 elections. Gagliardone sees these years as a turning point, claiming that the government began "developing relatively opaque relationships with private operators, which were asked to provide technical means to increase the ability to surveil and censor communications" (141). This set the scene for the Security Laws Amendment Act which was passed after the 2013 attacks on a mall by the Al Shabaab militia – later, the High Court struck down eight clauses for violating the constitution (Gagliardone 142). Another attempt at establishing more control over online communication was the 2018 Computer Misuse and Cybercrimes Act which includes penalties against anyone who "knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person" (Parliament of Kenya, article 23).

These laws led to several human rights violations, including an arrests of journalists, bloggers and social media users (Freedom House, "Kenya"). Besides filing charges against individuals, the state also pushes for the removal of content on the grounds of immorality,

which led to censorship of content displaying non-heterosexual relations (Freedom House "Kenya"). NGOs advocating for human rights which have a long history as part of public discourse are increasingly excluded as alleged representatives of foreign interests (Gagliardone 130).

Nevertheless, international relations remain a vital part of the Kenyan economy and legislators find themselves forced to bow to international pressure. 2019 saw a new Data Protection Bill which is in compliance with EU's GDPR and seen by Article19 as "part of Kenya's efforts to attract investment in its information technology sector" (56). Europe has history of influencing the Kenyan ICT landscape, since the country's digital payment service M-PESA originally emerged from a project funded by the UK's Department for International Development (Gagliardone 61).

The impact of the United States on Internet regulation in Kenya has been even greater, although not necessarily beneficial from a human rights perspective. In fact, the Data Protection Bill was partly a result of concerns over uncontrolled data collection particularly by US corporations Facebook and Google (Kazeem). While the bill limits ICT companies' rights, it also provides legal security from abuse by the government, which has led Amazon Web Services to open an operation basis for cloud computing in Kenya (Kazeem). Even more impactful than US investments are its security politics. The US sees Kenya as a strategic ally for fighting extremism in the region, particularly in Somalia (Gagliardone 139). As established above, a thorough surveillance of online communication is presented by the US as a crucial element of its 'War on Terror'.

While China's relations with Kenya have not led to much direct influence of Internet governance in its favour, the CCP determined the country as a hub for its state-controlled media. Major outlets including *CGTN Africa*, *Xinhua* and *China Daily* are all stationed in Nairobi where they are part of shaping public discourse on media regulation (Gagliardone 58). Gagliardone also points out that Chinese companies were often able to win government contracts to expand telecommunications infrastructure (70).

Overall, Kenya maintained relations to all three economically dominant powers, while increasing its control over the Internet. Of the external influences, the securitization agenda was arguably most impactful and gained momentum after the country experienced violent attacks. However, the new Data Protection Bill based on the GDPR could have long term consequences, potentially strengthening users' rights online.

### 5.6. Nigeria

Africa's most populous country Nigeria is home to a dynamic information society. Nigerians make political use of social media for debates and crowd-sourcing, particularly during political elections (Musa 84). However, society also shows signs of problematic digital divides, particularly among gender and language lines (Freedom House, "Nigeria"). While this lack of access to Internet is concerning from a human rights perspective, it remains attractive to international investors who note the growth potential of a market of approximately 200 million Nigerians.

Like China, the Nigerian government recognized market access to its large population as potential leverage for negotiations with international stakeholders (Foster & Azmeh 16). Since 2013 the Guidelines for Nigerian Content Development in Information and Communications Technology require corporations to "host all subscriber and consumer data locally within the country" (NITDA 15). However, observers have not witnessed a strong enforcement of the guideline and it remains unclear whether multinational corporations are in compliance (Africafex 29).

An enforced localization of data in Nigeria would have consequences, since the regulatory landscape is highly influenced by a continuous securitization of online communication. This is mainly the result of ongoing conflicts with armed groups, particularly the Islamist extremists of Boko Haram, and led to a muddying of the rights established by the 1999 Constitution which set forth the right to freedom of expression in article 39 and the right to privacy in article 37 (Constitution of the Federal Republic of Nigeria).

The Internet rights advocacy group Africafex points out, that particularly the right to privacy is not protected (26-27). The most concerning legislation in this regard is the Cybercrime Act of 2015. In section 24 it constitutes a prison sentence of up to three years for sending a message that is "false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety to another" (National Assembly of the Federal Republic of Nigeria). It further requires that platform operators "preserve, hold or retain any traffic data, subscriber information, non-content information, and content data" for two years and comply with law enforcement agencies when they request information" (National Assembly of the Federal Republic of Nigeria). The implied judicial oversight is not clearly defined (Freedom House, "Nigeria").

This law resulted in the arrests of numerous journalists, bloggers and social media users and several convictions for aiding and abetting prohibited actions (Freedom House, "Nigeria"). Africafex observes a "lack of balance of human rights and cyber-security in the

government's efforts to legislate and regulate the internet" (27). While the government usually refrains from blocking websites, it made exceptions for *Naij.com* and other media platforms promoting the independence of the contested Biafra region in the East of the country (Freedom House, "Nigeria"). Security advisor Sunday Ogunlana, who comments on the situation in Nigeria from a cybersecurity perspective, claims that the Nigerian Secret Police employs content-monitoring tools and firewalls to "filter terrorist messages before they reach the public" and ensure non-repudiation of online activities (93, 98-99).

To date, there are no reported incidents of complete Internet shutdowns in Nigeria. A partial shutdown in 2013 to three states in the context of fighting Boko Haram is criticised by Africafex which points out that "not only did terrorist attacks continue throughout the period when telecommunication services were cut off, in many instances such attacks intensified" (32). Presumably the governments technological potential to surveil online activity will increase, since several budget raises to the Office of the National Security Adviser and the Department of State Security were approved, always with the justification of fighting Boko Haram (Freedom House, "Nigeria").

Another recent development could potentially impact Internet regulation in the country heavily, namely the Digital Rights and Freedoms Bill. The bill is intended to protect human rights of Nigerians online, laying out details as to how Courts should interpret the rights to privacy, freedom of expression. However, President Muhammadu Buhari refused to sign bill in 2019 after it had passed both chambers or the National Assembly, claiming it "covers too many technical subjects and fails to address any of them extensively" (Freedom House, "Nigeria"). As of July 2020, an updated form has not been passed.

Nigerian civil society pushes for data protection legislation both domestically and internationally (Mihr 63), but the interests of the security sector weigh heavier. The government's conflict with Boko Haram is a lucrative business for contracted foreign cybersecurity corporations, since Nigeria's surveillance apparatus is rarely entrusted to domestic companies (Ogunlana 98). This exposes a conflict of interest with the country's data localization principle and reveals that support for the national economy is trumped by the government's desire for high-end security infrastructure.

The security sector is dependent on cooperation with foreign corporations and investors. Once again, China stands out as a source of funding, with the Exim Bank offering Nigeria a US$100 million loan in 2012 to "boost the sophistication and effectiveness of the government's efforts to tackle security challenges", as the Ministry of Finance claimed (qtd.

in Gagliardone 45). Security advisor Ogunlana is generally in favour of using China as a model for accessing user data, arguing that

> China enacted a National Security Law that gives police the authority to partner with private technology companies to help them bypass encryption or other security tools to access sensitive personal data. ... Although this approach is raising significant privacy concerns among users and human right activists, the benefits outweigh the risks if the government is determined to combat terrorism in cyberspace. (94)

Despite its restrictive Internet regulation, China is not seen as a danger to personal liberties among most Nigerians (Gagliardone 95). The two states' agendas line up in their prioritisation of security concerns over human rights.

A similar dynamic can be observed in Nigeria's relations with the US. These too revolve around security cooperation targeted at Boko Haram, which includes technology transfers and training for Nigerian law enforcement (Ogunlana 89). In 2016, the US requested an increase in bilateral and multilateral action (Ogunlana 99). Furthermore, US platform operators are responding to pressure to regulate their users, which resulted in Facebook deleting numerous Nigerian accounts that had been used to spread disinformation during elections (Freedom House, "Nigeria"). This move can be viewed as a concession to the Nigerian government which the social media giant is dependent on to maintain access to the market. Facebook is highly invested into the country's digital development. In 2019 it began work on MainOne, a 750km fiber line intended to connect about one million Nigerians to the Internet, a project in cooperation with local authorities (Facebook, "Enabling...").

The EU's influence on Nigeria's Internet regulation is marginal compared to China and the US. However, the GDPR's international impact could lead to an adoption of its principles into the Digital Rights and Freedoms Bill in case it passes into law. It should be noted, that European companies also profited from Nigerian securitization of online communications, e.g. the Italian company HackingTeam provided surveillance technology (Freedom House, "Nigeria").

Overall, Nigeria's security concerns shaped interactions with foreign stakeholders. All three dominant powers supported the country in increasing online surveillance, with China standing out as the largest source of funding. Legislation ensuring more data protection is in the making, but has not been able to overcome political obstacles.

### 5.7 Zimbabwe

Similar to Ethiopia, Zimbabwe recently experienced a change in leadership highly impacting the country's digital policies. After 37 years in power, first as prime minister and later as president, Robert Mugabe was removed from office in a 2017 coup and Emmerson Mnangagwa succeeded him in office (Melber). However, Mnangagwa can also be described as an advocate of *Mugabeism*, a political ideology that runs Zimbabwe as the "private property of a combined civil-political and military-security apparatus under the hegemony of ZANU–PF [Zimbabwe African National Union – Patriotic Front]", the party of both Mugabe and Mnangagwa (Melber). Any public data on Zimbabwe must be viewed critically, as it can be subject to government manipulation. This includes the theoretically high quotes of Internet penetration. NGOs pointed out that particularly rural areas have rates of around 10 percent (Freedom House, "Zimbabwe"). Africafex argues that this is likely due to data costs being the "third most expensive on the continent", with the cheapest costs for 1GB per month being at around US$30 (66).

In terms of legislation, the Constitution guarantees "freedom of expression and freedom of the media" in section 61, which includes "freedom to seek, receive and communicate ideas and other information" (Constitution of Zimbabwe). This right is frequently violated, particularly through the 2007 Interception of Communications Act (ICA), which makes service providers liable for content on their networks and compels them to ensure that "its services are capable of rendering real time and full time monitoring facilities for the interception of communications" in section 9c (The President and the Parliament of Zimbabwe). Africafex argues that service providers are thereby assigned the role of "watchdogs on behalf of the state and have the capability to enforce controls on the behaviour of their users" (67). Clearly, this is also in violation of the right to privacy, which is equally included in the Constitution in section 57 (Constitution of Zimbabwe).

Freedom House provides a long list of individuals arrested with charges of violating the ICA, from opposition politicians to students arrested for communications via Twitter, Facebook or WhatsApp ("Zimbabwe"), a practice that has been observed over several years (Africafex 70). Early 2019 also saw complete shutdowns of social media, with US platforms Facebook, WhatsApp, Twitter, LinkedIn, Reddit, and Tinder blocked nationwide for approximately a week (Freedom House, "Zimbabwe"). Information Minister Energy Mutodi justified the action claiming

> The social media was used by criminals to organize themselves, to go out there to loot shops, to cause mayhem, to terrorize residents. This tells that there is abuse of social media, this is why the government had to really block social media, to block internet and to stop organized crime, organized gatherings that end up in violent demonstrations, violent destruction of property and also disregard for other people's rights. Not only in Zimbabwe but Africa as a whole, there has been an abuse of social media; people still do not understand what social media really is. (qtd. in Mavhunga)

Africafex points out a similar incident in 2016 which was targeted at WhatsApp, but retracted after some hours (70). While the 2016 blocking saw no official explanations, the 2019 shutdown was publicly discussed and even brought before the High Court which ruled it illegal mainly on procedural grounds (Media Institute of Southern Africa). Freedom House criticised that the verdict "left room for future network disruptions ordered by an official with the correct legal authority" ("Zimbabwe").

The government's harsh control over Internet communications has also resulted in self-censorship after particularly human rights activists and politicians of oppositional parties experienced threats (Freedom House, "Zimbabwe"). Public discourse is additionally warped by government youth groups resorting to multiple social media accounts to attack political opponents and NGOs (Freedom House, "Zimbabwe").

Despite all this, the Mnangagwa administration publicly promotes an agenda of liberalisation. Minister of Foreign Affairs and International Trade, Sibusiso Moyo, wrote an opinion piece for the *EU Observer* claiming that "[o]ur new Zimbabwe is committed to opening up our nation, economy and society to the world" (n.p.). There is arguably some truth to that, since particularly Western states are resuming relationships with Zimbabwe after long-lasting embargoes during the Mugabe era. Moyo points out that sanctions imposed by the EU had successfully discouraged investment and engagement in the country, while claiming new laws now allow majority ownership for European investors, explicitly emphasising opportunities in a "transformed" media market (n.p.). It is unclear, however, if the entrance of EU corporations into the Zimbabwean market will result in an adoption of GDPR standards of data protection or merely in economic opportunities for private actors.

Political ties between Zimbabwe and China are much stronger, mainly because China was a welcome alternative to Western funding during Mugabe's rule (Batty 158). Reporters Without Borders points out that Beijing is by far the largest source of foreign investment in the country – at the same time Chinese ICT corporations like ZTE and Huawei received

numerous multimillion-dollar contracts from government agencies (Cave et al.11). This resulted in an exchange of political views as well. Indeed, Robert Mugabe was one of the few African leaders that publicly presented the Chinese strategy of Internet regulation as a model to be followed (Gagliardone 126). Zimbabwe signed several agreements with Chinese cyber-security corporations, including the highly controversial facial recognition company CloudWalk, which created a high-end system of surveillance (Cave et al. 12). Within the Belt and Road Initiative, China invested a total of US$71 million in the development of ICT in Zimbabwe (Freedom House, "Zimbabwe"). This has not changed after power transferred from Mugabe to Mnangagwa, who has since secured Beijing's support for his "Vision 2030", an attempt at developmental leapfrogging with a focus on ICT infrastructure, education and innovation (Ministry of Foreign Affairs of the People's Republic of China). In return, Mnangagwa expressed his political loyalty to China which earned approval by Xi Jinping who welcomed that "Zimbabwe is steadfast to the One China policy and actively participates in the Belt and Road Initiative" (qtd. in Ministry of Foreign Affairs of the People's Republic of China).

Due to sanctions during the Mugabe era, US relations with Zimbabwe are more distant compared to the other case study countries. However, private corporations have played their part in effectively dismantling net neutrality in the country. Counteracting the high costs for data, Facebook and other US platform operators made deals with the largest mobile operators, creating cheaper data plans that offer unlimited access, but only to their platforms (Africafex 67).

After the end of Robert Mugabe's rule, Zimbabwe's government essentially remained authoritarian, which extends to its Internet regulation. Although the High Court ruled the most recent shutdowns illegal, future compliance with human right is unlikely, since the Mnangagwa administration is scaling up its surveillance sector, primarily supported by Chinese technology.

### 5.8 Reappearing Issues

The situation in the case study countries makes clear that Internet regulation in African states is extremely diverse. However, some common human rights issues emerge in multiple countries, which can be grouped along seven clusters: 1) legislation conflicting with the rights to freedom of expression and privacy, 2) non-transparent decision-making processes in executing Internet regulation, 3) full or partial Internet blocking, 4) arrests of journalists,

bloggers and social media users for unwanted communications, 5) censorship of platforms and websites, 6) enforced access to user data on platforms and 7) increasing investments in surveillance technology.

These reappearing issues are subject to different degrees of external influence. Concerning legislation, the case studies prove that many laws passed in African states are based on existing laws in Western democracies. Particularly with regards to problematic cybersecurity and anti-terror legislation, African governments build on existing templates, that allow for abuse in states with weak rule of law. The non-transparency of decision-making processes in applying this legislation can be seen as a problem independent of external influence and rather caused by pre-existing governmental issues in many African states. However, some influence could be traced back to the unbalanced Chinese policy of excluding stakeholders from civil society which counteracts the establishment of non-governmental oversight mechanisms. Internet blocking is not practised by any of the economically dominant actors, but appears in several African states. Together with censorship of platforms and websites as well as arrests of users, blocking can be seen as central means to restrict critical voices online. Many of these measures reflect China's highly effective system of censorship and arrest of dissenters, which provides a blueprint for authoritarian governments on how to execute oppressive regulation, even if China declines to be seen as a model. Enforced access to user data on platforms is used by US and Chinese law enforcement and intelligence services to different degrees. Unlike the US and China, however, African states are rarely home to the large ICT corporations used by their populations and thus rely on crasser means to access data, e.g. through laws requiring full cooperation with authorities or data localization laws. Finally, the US, the EU and China all supported African governments increasing their surveillance capacities, by participating in the abstract 'War on Terror' with African states as geostrategically selected allies, through private corporations exporting surveillance technology and by financing the governments' security sectors.

Another common development visible in the case studies is the liberalisation of African ICT markets. While an increased presence of private foreign actors does not necessarily have a direct positive or negative impact on the rights to freedom of expression and privacy online, it offers more options for Internet users to choose forms of communication that least endanger their human rights. Leaning in to the agenda of private actors could lead to increased datafication, but could also result in stronger data protection laws to prevent state interference. This is mostly dependent on the extent to which the interests of civil society are taken into consideration.

# 6 Recommendations to Improve Human Rights

The case studies in chapter 5 demonstrated a number of individual and reappearing issues with regards to Internet regulation. In order to improve compliance with the rights to freedom of expression and privacy online, stakeholders need to take active measures. This chapter first analyses international organisations' possibilities to secure human rights of Internet users. It then turns towards suggestions to the US, EU and China before engaging in the debate on possible means for African states to fulfil their tasks as duty bearers. Finally, it draws the connection between regulatory issues prevalent to the Global South and the overall dilemma of regulating digital capitalism.

## 6.1 Challenges and Opportunities for International Organisations

As of August 2020, IOs have not been able to establish an effective regulatory framework specifically binding states and private actors to an Internet regulation in compliance with human rights. The main challenge is that there is little consensus to build upon, since the relevant human rights treaties have not been ratified by all stakeholders. Particularly authoritarian states view individuals' rights to freedom of expression and privacy as obstacles to security interests or a collective right to development. If human rights were in fact universally accepted as indivisible, interdependent and interrelated, this would not be an issue, but a lack of agreement on these fundamentals is at the root of the problem.

Academia has a long history of debating IOs' possibilities to establish a global data regime, with norms and principles that guide Internet regulation in a common direction. Foster and Azmeh discuss some basic principles including the free flow of data across borders or the prohibition of conditionalities for foreign corporations to enter markets (15). This free trade approach clearly favours actors from economically dominant states at the expense of the Global South, but even so, it is unlikely to find much support in the era of the US-China trade war.

Mihr suggests two options that deserve consideration. Firstly, a social contract with a "legally binding 'cyber constitution'" as well as "monitoring bodies, such as a global cyber-court, multistakeholder committees, or otherwise rotating, participatory, and transparent government regimes" (67). This institutional approach could be developed under the United Nations, either as a tenth human rights treaty with a monitoring committee or in the form of a

new body, possible emerging from the ITU. The advantage of a new treaty could be that states willing to cooperate on a human rights-based approach to Internet governance could set standards for cooperation and thereby apply pressure to other states. However, the experience with human rights treaties shows that even treaty ratification does not necessarily result in compliance and mechanisms of enforcement are unrealistic as long as Internet sovereignty remains popular. This can be seen by the limited impact of treaties in regional human rights systems such as the ACHPR's Malabo Protocol, which require continued promotion.

An alternative would be a non-binding agreement without a treaty (Mihr 66). While this option does not provide security for individuals, corporations, nor states, it might be a preliminary step to outline policies that find agreement. In a later step non-binding agreements could lead towards treaties, monitoring bodies etc. A multi-stakeholder approach that takes the concerns of non-state actors seriously is vital at this stage, as it allows for bottom-up regulation, rather than strengthening top-down dynamics. An example is the African Declaration on Internet Rights and Freedoms which arguably had limited impact, but gave a voice to several strands of civil society groups (African Declaration Group).

Presumably, a conference like the 2012 WCIT would result in even less agreement today, but it could be an opportunity for civil society to express joint concerns and form strategic alliances. The WSIS Forum 2020 has a focus on digital transformation and global partnerships to achieve the UN Sustainable Development Goals (ITU). Its High-Level Track, which includes stakeholders from the "government, private sector, civil society, academia and international organizations", is projected to conclude in September 2020 with a joint agreement on policy (ITU). Mihr also sees potential in IGFs, claiming a "global public policy concept might be a way out of the dead-lock of the multistakeholder approach versus a governmental run international cyber governance regime" (66). For legitimate global regulation to emerge, it is crucial to include civil society groups based in the Global South into these debates, as a dominance of Western non-state actors will likely lead to an imbalanced political outcome and low acceptance among African governments.

The WTO and World Bank push for a transformation of the digital landscape in the Global South. However, the WTO is neutral on human rights issues and dedicated to its agenda of liberalising trade and "creating and improving efficiency for business activities rather than for social change" (Musa 85). Foster and Azmeh note that signing on to digital free trade agreements in exchange for access to aid could become problematic for African states, because complete market liberalisation is difficult to roll back when the focus shifts from infrastructural development to finding regulatory solutions for ICT problems (16-17). African

alliances recently stopped a “Trade Liberalization Agenda” tying e-commerce to development that was supported by China (Foster & Azmeh 17). Given its role in supporting the global expansion of the ICT sector, the WTO’s neutrality on human rights makes it a problematic actor that adds leverage to the interests of economically dominant states without regards to regulatory dilemmas in the Global South. Reforms are long overdue.

### 6.2 More Responsibilities for Dominant Actors

As of 2020, the influence of the US through the predominance of its platforms and its anti-terror agenda still outweighs other foreign actors’ impact on Internet regulation in Africa. While the US government’s engagement with African states and IOs decreased under the Trump administration, not much has changed in these regards. Instead, the withdrawal from international fora has led to a stagnation of the development of international Internet governance that acknowledges human rights, while the cybersecurity agenda saw increased attention. Unfortunately, the damage is done and anti-terror and cyber-security laws in African states will not be retracted, even if the US were to change its position as a trailblazer of securitizing online communication.

Going forward, domestic US laws directed at platform operators could be the most important source of external influence on freedom of expression in Africa. However, the unclear assignment of regulatory responsibilities culminating in an open conflict between social media platforms and the government is a sign that US ICTs developed much faster than legislation. It is crucial that the US finds solutions that are in compliance with the ICCPR. A potential resurgence of cooperation in IOs is largely dependent on the results of the November 2020 elections. Intensified dialogue with international stakeholders could result in advancing developments in the areas of business and human rights and the extraterritoriality of human rights.

The EU’s GDPR was a major step in setting standards far beyond its borders and, as part 5 showed, its impact can be seen in African legislation as well. The EU needs to build on this and update its data protection standards to a continuously evolving ICT landscape (Kontargyris 76). The upcoming Digital Services Act could be a next step in setting a human rights-based model for Internet governance if it includes suggestions from civil society. However, the DSA’s attempt to bolster EU values in Internet regulation could also lead to an even more fractured web, rather than a joint approach.

The EU's direct engagement with African governments is also in need of improvement. Foreign relations show that the alleged conditionality of aid on good governance and human rights is muddied by economic interests to access African markets and political interests to datafy African migrants. The EU needs to ensure that when it engages in development programmes, they are first and foremost in the interest of people on the ground. Furthermore, European corporations regularly export highly invasive surveillance technology to authoritarian regimes. In this regard, the EU could set standards similar to the 2008 Common Council Position that governs the export of weapons to prevent authoritarian rulers from using European technology against their own people. For such an approach to be effective, however, it would require stricter enforcement.

Among the dominant powers, China is arguably the most threatening to the future development of the rights to freedom of expression and privacy in Africa. Getting China to acknowledge these rights by signing on to the ICCPR seems unrealistic, since the CCP long since embarked on its own path to reforming the international order according to its ideology, rather than vice versa. Possibilities to influence the regime from the outside are limited, since the CCP is apt at deconstructing any alleged moral high ground by Western actors by pointing out their own human rights violations. More importantly, most states do not even dare to bring up human rights issues directly in their diplomatic relations with Beijing for fear of economic repercussions.

However, reform is also possible in China and some steps could be considered realistic. While Internet censorship is unlikely to be abandoned anytime soon, a more transparent filtering of content with comprehensible rules on publishing and privacy could help users of Chinese ICTs in Africa to make more informed decisions on what information they want to share. More transparency in the realm of diplomacy and trade could also help combat possible corruption that has allegedly secured lucrative contracts for Chinese corporations with African governments (Cave et al. 11).

Less realistic but nevertheless crucial is that China discontinue its efforts to exclude non-state actors from international fora. The CCP's top-down approach to Internet regulation inevitably endangers human rights of individual users who are not given a voice. Civil society's participation is also vital in relations between African states and China to ensure that loans do not lead to more human rights violations by enabling authoritarian oppression or increasing economic and political dependence. China will not be impressed by sanctions emerging from other states, but a civil society that chooses not to make use of ICTs that violate users' rights to freedom of expression and privacy is difficult to oppose.

With regards to the economically dominant actors analysed in this paper, the most important path to ensuring human rights of Africans online is more cooperation. Projects such as 2Africa, on which Facebook works jointly with investors from China and the EU to lay a subsea Internet cable, show that corporations' pursuit of resources can sometimes lead to infrastructural development. In terms of Internet regulation, foreign actors need to refrain from using Africa as a proxy battlefield for a cold war of normative compatition. To some extent, the current situation is still in balance since, as Gagliardone points out, governments are "not being asked to pledge allegiance to one or another model and there is a great deal of hybridization and recombination happening" (17).

However, tensions between the US and China are rising. In August 2020, the Trump administration announced it would expand its "Clean Network" program which aims at disconnecting Chinese apps, data clouds and subsea cables from their US counterparts and called on "allies and partners in government and industry around the world to join the growing tide to secure our data from the CCP's surveillance state and other malign entities" (Pompeo). If this aggressive technological polarisation is reciprocated by China, it could have a detrimental impact on digital development in the Global South where states would be forced to connect to one Internet and disconnect from another.

A change of geopolitical mindsets is necessary. Influencing global Internet regulation must not be understood as a realist zero-sum game with one player's rise inevitably resulting in another player's demise. There does not need to be a scramble for Africa when there could be a discourse among all actors involved, including those from civil society. This discourse could deconstruct the cold war rhetoric that is growing among dominant powers attempting to shape the Internet in their favour and instead lead to a strengthening of users' human rights.

### 6.3 Towards a United African Approach

The main responsibility to protect the rights to freedom of expression and privacy lies with African states that are bound by the ICCPR and ACHPR. Apart from struggling with problems arising from different forms of authoritarian rule, these states face a dilemma. Their citizens demand improvements to Internet infrastructure and access to modern communication forms like social media platforms. However, the regulation of these platforms is not entirely up to African states and the funding for infrastructural development largely depends on foreign investors looking to achieve economic aims by getting access to data. Authoritarian governments often see liberalisation as their only option to achieve digital development goals

while continuing to use complete or partial Internet and platform shutdowns, criminalisation of communications and increased surveillance as means of maintaining the upper hand in regulation that is otherwise set by external private actors.

Digital development programmes that are based on modernization theory fail to recognize that the path of independent infrastructural and regulatory development taken by states in the Global North is not made available to African states, regardless of governments' ambitions to catch up or leapfrog into a modern information society. The Internet as it is spread across the Global South by economically dominant actors is no longer the anarchic web of the 1990s. Online communication is dominated by a small group of companies with budgets much larger than those of dependent states.

There are many ways to approach this dilemma. Although some dependency theorists discuss it, autarky is not an option, as it opposes one of the central functions of the Internet, namely creating worldwide connections. Complete liberalisation on the other hand will foreseeably lead to a strengthening of dependence relationships without the possibility for African states to achieve economic gains or make their voices heard in terms of regulation policies.

Bilateral, multilateral and multi-stakeholder relations can provide fora to find a middle ground. For African states to impact global Internet regulation themselves, a promising path forward would be to bundle overlapping interests to gain leverage in negotiations, a method that proved successful during the WTO negotiation on liberalisation of e-commerce (Foster & Azmeh 17). The AU can be the uniting institution for such an approach, but governments need to give up a degree of sovereignty for it to work effectively. The AU could then guide infrastructural advancements while mainstreaming human rights into agreements with foreign stakeholders. It could also play a role in advancing reforms to anti-terror and cybersecurity legislation where those stand in contrast with the rights to freedom of expression and privacy (Ethiane 122).

AU partnerships with international stakeholders such as FOCAC could be transformed into more efficient platforms to discuss a human rights-based approach to Internet regulation with China (Ogubay & Lin 314-15). The same applies to the AUC–U.S. High-Level Dialogue. Particularly the AU-EU partnership has the potential to grow into a powerful alliance to shape global Internet governance. A cooperation that extends to potentially standard-setting legislation like the upcoming DSA would resonate even more across the globe and lead to increased compliance of big data corporations. South-South cooperations with Asian and Latin American states and federations could also result in larger influence on

global Internet governance (Ogubay & Lin 320), and counterbalance the power of economically dominant actors.

To protect human rights in Internet regulation, the AU needs also needs to increase functionality of the African Court of Human and People's Rights. This requires more states to recognise the courts jurisdiction and apply its rulings, but also referrals of cases from the ACHPR to the Court. Viljoen also argues for greater access of individuals and NGOs to the Court as amicus curiae (94). This could draw attention to structural violations of freedom of expression and the right to privacy.

### 6.4 Moving Data Protection Foward

A central element to empowering Internet users in Africa is the establishment of data protection legislation that ensures the right to privacy and is enforceable in African courts. Onuoha argues that companies handling personal data must agree to be held accountable by "data protection and privacy laws within their operational jurisdictions, whether or not they are registered as a business entity in those jurisdictions" (62). Applying this rule worldwide would also save companies from their own dilemma of deciding whether to comply with their home country's jurisdiction or their operating country's (PoKempner 229). YouTube is an example of developments going in this direction, at least in terms of content regulation. The streaming platform claims to have created 91 localized versions for individual countries (YouTube).

For the localisation principle to work with regards to privacy, more transparency is needed as to what data private companies collect and generate through algorithms. It would also mean abandoning a web that is indeed worldwide and advancing the process of Internet 'balkanisation'. Localisation of data protection is only worthwhile if African legislators and courts adjust to human rights standards, which seems less workable than pursuing a joint approach through a regional framework such as the EU with its GDPR.

Data protection legislation guaranteeing that information is safe from infringement through government agencies is not only crucial to individual users' rights, but also to corporations offering services. Kriebitz and Lütge point out the asymmetric relationship between authorities requesting data and platform operators forced to give it up, suggesting adherence to the principle of proportionality by "balancing the right to privacy with the public's general interest in investigating criminal or administrative offences" (13-14). This could require additional training for law enforcement officers and judges.

A major step towards securing human rights could be achieved if businesses adhered to the principle of data minimization, which implies "not collecting more personal information than needed for a particular purpose" (Kriebitz & Lütge 13). However, this is contrary to the economic interests of companies pushing for datafication of communications. To what extent private actors could still be held accountable to the principle of data minimization depends on which direction the developing framework of business and human rights takes.

### 6.5 Strengthening Civil Society

To ensure that human rights are at the core of Internet regulation, it is crucial to include civil society in all stages of law-making. Democratic structures in both economically dependent and dominant states have much room for improvement in this regard. An essential requirement is to keep up dialogue in multi-stakeholder fora by including NGOs, academia and other groups and individuals. African activists could increase their contribution by forming alliances at WSIS and in IGFs (Foster & Azmeh 18).

Gurstein puts forth an Internet vision in the name of African civil society, if it were given the opportunity to make decisions eye to eye with dominant stakeholders from the US, the EU and China:

> It would seem that the most appropriate position of CS [civil society] in the emerging 'Cold War' is one of 'non-alignment' where CS recognizes the validity of certain elements in the stance of both camps including support for free expression and open access on the one hand, and of digital inclusion and a fair distribution of the economic benefits of the Internet on the other; and on the other hand rejects other elements of these camps – attempts to restrict free expression on one side and an absolutist anti-statist anti-regulatory position regarding the governance of the Internet on the other. But particularly the CS position would be characterized by its commitment to the governance of the Internet in the global public good and to the operation of the Internet in the global public interest. In this way CS would reject support for an Internet dominated by private corporate interests as well as one supporting the interests of control oriented governments who would use the Internet for repression and as a way to enhance internal control. (qtd. in Gagliardone 147)

While similar positions are found in various documents and reports from NGOs, the space is shrinking for civil society to articulate them in decision-making processes of states and IOs where they are excluded. Civil society voices need to be heard in IOs, where they can establish common ground between opposing opinions and in domestic processes that governments consider 'internal', such as establishing norms in anti-terror or cybersecurity surveillance. An integration of civil society as the objects of surveillance could alleviate the impact of securitising online communications and reinstate human rights protection against invasive law enforcement and intelligence agencies.

Increasing ICT literacy should be a core part of investing into digital development (Oginni & Joash 168). It is important that this literacy be informed by an African perspective, rather than using training merely to spread skills useful to US, European or Chinese investors. Digital education could emerge as one of the few opportunities to break relations of economic dependence.

### 6.6 Mainstreaming Human Rights in ICTs

As chapter 3.1 established, the task of content filtering is gradually reassigned from human contractors to algorithms coded by ICT companies. This stage of intra-platform regulation needs to be regulated by international standards and requires a debate on when and how algorithms should make decisions over the legality of content. So far, frameworks established by the OECD and G20 have not succeeded at effectively regulating the use of algorithms by private actors and a binding framework at the UN level is still in progress. Many academic and civil society institutions released ethical guidelines, but they are neither binding nor particularly impactful. Nevertheless, they can be seen as a first step.

The main principle necessary to securing human rights in regulation of algorithms is transparency. This includes disclosing all data points going into an algorithmic calculation and their assessment. Increased transparency would allow for more trust and accountability, by both users and regulators (Reins 26). Corporations should establish internal mechanisms of remedy and comply with external oversight to protect individuals from unjust automated decisions (Kriebitz & Lütge 18).

External oversight mechanisms can take various forms. The NGO Article19 calls for the establishment of social media councils, "a transparent, inclusive, independent, and accountable mechanism to address content-moderation problems on the basis of international human rights law" (41). Article19 argues that governments and civil society "understand their

work is being impacted by social media to a very dramatic degree, but they complain that they have absolutely no way to even talk to Facebook" (42). Social media councils could be fora to discuss regulatory norms and thereby provide African governments with alternatives to blocking platforms when they perceive them as threatening. An important step for these independent councils would be the inclusion of Chinese platform operators like Tencent or ByteDance. While this would require the CCP to take a step away from Internet sovereignty and its rejection of multi-stakeholderism, it could be a lifeline that saves platforms like TikTok and WeChat from further bans.

A final suggestion, which is also discussed in the developmental stage of the EU's DSA, is the possibility of introducing a mandatory interoperability of platforms (Berthélémy and Penfrat 19-22). Communication platforms like Facebook or Weibo would then function more like email providers, allowing users to find and interact with others across platforms, while being able to maintain their own technical and regulatory guidelines. This could be an interesting option to counteract frontal competition – particularly between US and Chinese platform operators – by providing a common ground that is not mutually exclusive. African ICT developers could also enter the online communications market with platforms, apps and clients reflecting their own regulatory background without having to break through the monopolies of Facebook or Twitter.

### 6.7 Digital Reforms or Digital Revolution?

While states are bound by international law, the application of human rights to private actors is still evolving. In day to day operations, ambitious mission statements by ICT corporations translate into a loose culture of CSR, which often amounts to little more than a marketing scheme. Kontargyris claims that self-regulation could still be an option if interoperability and data protection are promoted while user-profiling and censorship are banned or discouraged (69). IOs, governments and civil society stakeholders have long brought forward these demands – to little effect. Even disgruntled customers rarely lead to comprehensive changes in platform policies because companies effectively control communicative monopolies.

Enforceable laws, such as the GDPR, on the other hand already affected global Internet standards more than many critics expected. This provides hope for a future scenario in which international law could be applicable directly to private actors. Reporters Without Borders argue that holding ICT corporations accountable to human rights is particularly necessary "in developing countries, where the state may be less able or less willing to do so

because of challenges arising from governance, legislative and regulatory capacity, transparency and corruption" (Cave et al. 9). Shifting the scope of international law to apply to non-state actors could one day result in ICT corporations having to justify their algorithmic decision-making processes in front of treaty monitoring bodies. However, this is a long-term project with an uncertain outcome.

A more revolutionary approach to tackling the issue is by reassigning the services currently provided by private actors to public institutions that are bound by international law. Scholars discussing this solution can be divided into two groups: those in favour of establishing new platforms and those in favour of communisation of existing platforms.

Regarding the establishment of a new public platform, it is important to distinguish this from a government-controlled corporation. Rather, it would be subject to independent oversight i.e. by the AU, and inclusive to actors from across Africa or the world. Creating such a public platform has been discussed as a potential strategy for the EU to tackle the problem of efficiently regulating US corporations. In a fictional report for the European Union Institute for Security Studies titled "What if... Europe created an International Social News Platform", cybersecurity analyst Nathalie van Raemdonk outlines a platform she calls NovaWeb:

> Societies all over the world had been struggling with the unintended harmful side-effects of Silicon Valley platforms. Publishers and civil society in Latin America and Africa ventured into NovaWeb, and a vibrant ecosystem of subnovas with a South American and African focus found its place in the network. Their policymakers also took note, and welcomed the platform's positive influence on their countries. Other countries saw NovaWeb as a threat and blocked access. Rigorous content control was however a very costly affair for most states with limited resources. The lack of openness stunted their development and caused them to lag behind in digitisation and innovation. (26)

A challenge for such an approach would be to find a market because it is too late to simply create an EU-sponsored version Facebook or TikTok – they already exist. Furthermore, it is uncertain if a platform launched by the EU would indeed be interesting to users in the Global South or whether they would see a potential for further dependence.

Nonetheless, experimenting with public alternatives to private actors could be worthwhile, particularly in the EU where public media outlets already established networks of

cooperation. Current legal restraints prevent public service media from venturing too far into areas where Facebook, Google and other ICT corporations hold digital monopolies (Fuchs 220). However, Derakshan argues that public broadcasters like *ARD*, *BBC* and *France Télévisions* could share journalistic output on a collective platform (n.p.). This could be a first step to building a network governed by the Charter of Fundamental Rights and a public regulatory body to avoid violations of the rights to freedom of expression and privacy, as well as pitfalls common to private social media like algorithmic discrimination or echo chamber communication. In a second step, the platform could gradually open to communications by companies and individuals. The success of such a project could be a model for similar initiatives under the aegis of the AU.

The other path to establishing Internet platforms under public control is via communisation of existing platforms. Scholars have debated different levels of communisation. In its mildest form, PoKempner suggests treating large platforms as public utilities and enforcing an inclusion of human rights into terms of use with mandatory public reports, as well as appeals mechanisms to mitigate wrong decisions (238).

A more radical approach is put forward by Christian Fuchs who suggests the expropriation of big data corporations, to advance "the struggle for alternatives to digital capitalism, the de-commodification, de-capitalisation and de-commercialisation of the digital and the Internet" (220). Fuchs sees ICT corporations as expropriators of data who need to be transformed "from technologies of capital into technologies of commoning" (218). However, Fuchs' digital socialism is no guarantee for the protection of freedom of expression and the right to privacy.

Undoubtedly, though, the digital world requires a redistribution of power away from the "oligopoly of data billionaires" (Feng Xiang qtd. in Arora), because not only African users are currently excluded from the upper levels of decision-making. Couldry and Meíjas stress that this demands reimagining economic structures on a larger level:

> It is time for a more radical grounding of established regulatory discourse that enables it to challenge datafication's social order. This must involve more than regulatory adjustments to certain aspects of contemporary capitalism. What is required is a fundamental challenge to the direction and rationale of capitalism as a whole in the emerging era of data colonialism. (12)

History has proven that Africans have the potential to express and execute revolutionary ideas on equality and communitarianism, turning existing power structures up-side down (Gagliardone 163). It is crucial to include their voices into the global discourse on Internet regulation without constraining African positions to the existing capitalist structures that gave birth to the problematic inequalities in the first place.

## 7 Conclusion

Many African Internet users experience an online world that they have little possibility of shaping themselves. It is structured by the datafication agenda of foreign corporations and surveilled by government authorities prone to violating the rights to freedom of expression and privacy. Numerous regulatory decisions are not the result of civil society's engagement, but rather of interactions between international stakeholders.

The US, the EU and China all pursue their own political and economic interests in influencing Internet regulation in Africa. Arguably, the most impactful impulses originate in the US. The securitization of online communication in the aftermath of 9/11 led to the establishment of mass online surveillance that has since been adopted in large parts the world. At the same time, US big data corporations set standards through their internal regulatory systems that affect users in every country where they control the market. An EU push to strengthen human rights through data protection legislation has had some effects in African states. On the other hand, authoritarian governments looking to scale up their control over the Internet find a potential partner in China, which provides loans without good governance conditionality, promoting the principle of Internet sovereignty.

The dominant actors' strategies of influencing Internet regulation in Africa have seen varying results. Foreign investment, cooperation on development projects or bilateral agreements led to continuously improving Internet infrastructure. The case studies show that open markets with competing private actors can be effective for making the Internet more accessible and affordable. However, low Internet penetration rates in Ghana vis-à-vis high penetration rates in Zimbabwe indicate that market liberalisation is not a panacea for digital development. The case studies do not indicate a causal relationship between economically dominant actors' development agendas and Internet access in African states. Whether this could be due to misdirected funding and corruption, or overarching structural issues in the field of development requires further research. However, funding from the US, the EU and

particularly China caused an increase in Internet surveillance capabilities of African governments.

Concerning Internet regulation through legislation, foreign influence on African governments is both direct and indirect. African anti-terrorism and cybersecurity legislation is often based directly on Western laws and follows political agendas originating in the US. Data protection legislation, on the other hand, is mainly influenced by the EU's GDPR. China's impact on the legislative process is mainly indirect, but nonetheless crucial. By advocating for multilateral over multi-stakeholder approaches to international Internet governance, it excludes civil society from a vital part of the norm-shaping procedure.

The case studies show that the greatest dangers to the rights to freedom of expression and privacy online lie at the executive level where authorities make use of Internet blocking, censorship, surveillance and arrests. While individual decisions by African governments are largely independent of external actors, it makes a difference whether the international community publicly denounces them as human rights violations or whether they are accepted as an expression of Internet sovereignty. In this regard, stakeholders from the US and the EU have taken more action to protect human rights from naming and shaming to sanctions for authoritarian regimes. The CCP's principle of Internet sovereignty, on the other hand, effectively translates to a highly problematic neutrality on human rights violations by African states.

On an intra-platform level, executive regulation is performed by private platform operators. Following the principles of datafication and data colonialism, they continuously digitise communication and regulate it via content moderators and algorithms. In this regard, US corporations have the highest impact on freedom of expression and the right to privacy because of their quasi-monopolies in large areas of online communication. However, they are increasingly pressured to adapt to legislation in the US, in African states and to the EU's GDPR. Further research will be needed on how Chinese platforms like TikTok and WeChat respond to similar pressure and whether a US push for "Clean Networks" (Pompeo) will lead to a division of African Internet landscapes into US-aligned and China-aligned territory.

The decisive element to advancing human rights in Internet regulation is an inclusion of civil society at all regulatory stages. Despite dialogues in countless multi-stakeholder fora, the interests of private actors and states dominate decision-making. Initiatives emerging from IOs, particularly the AU, could reopen spaces for NGOs to debate Internet regulation without being outweighed by governments. These debates must include a critical assessment of digital

capitalism as a replicator of economic inequalities that make Africans dependent on the political agendas of dominant actors.

The Internet's increasing fragmentation along the lines of national jurisdictions marks the end of many connective elements that crossed political borders. Human rights could be the shared framework, on which global regulation can be built, but that requires the cooperation of states that oppose the principle of Internet sovereignty. The time to act is now, since the continuous development of algorithmic regulation, unchecked for compliance with human rights, can lead to individual and societal damage that will be difficult to reverse.

**Bibliography**

Access Now. "Back in the dark: Ethiopia Shuts Down Internet Once Again" *accessnow.org,* 16 July 2020, accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again. Accessed 29 July 2020.

African Commission for Human and Peoples' Rights (ACPHR). Declaration of Principles on Freedom of Expression in Africa and Access to Information in Africa. Adopted 21 Oct. – 10 Nov. 2018. *ACPHR.* achpr.org/legalinstruments/detail?id=69. Accessed 22 July 2020.

African Declaration Group. *African Declaration on Internet Rights and Freedoms.* 2014. africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf. Accessed 25 June 2020.

African Union. "Joint Communique on the 7th Annual AUC – U.S. High-Level Dialogue." *African Union*, 17 November 2019, au.int/en/pressreleases/20191117/joint-communique-7th-annual-auc-us-high-level-dialogue. Accessed 22 July 2020.

African Union. "List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" *African Union,* 18 June 2020, au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf. Accessed 22 July 2020.

African Union. "List of Countries which have signed, ratified/acceded to the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights." *African Union,* 16 January 2017. au.int/sites/default/files/treaties/36393-sl-protocol_to_the_african_charter_on_human_and_peoplesrights_on_the_estab.pdf. Accessed 22 July 2020.

African Union. African Union Convention of Cyber Security and Personal Data Protection. Adopted 27 June 2014. *African Union.* au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Accessed 22 July 2020.

Alden, Chris. "Evolving Debates and Outlooks on China-Africa Economic Ties." *China-Africa and Economic Transformation.* Oxford Scholarship Online, June 2019. doi:10.1093/oso/9780198830504.001.0001. Accessed 3 May 2020.

Alston, Philip. "End-of-mission statement on China, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights." *OHCHR.org,* 23 August 2016, ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=20402&LangID=E. Accessed 14 April 2020.

Arnould, Valerie et al. *Africa Uprising? The Protests, the Drivers, the Outcomes*. European Union Institute for Security Studies (EUISS), 2016, jstor.org/stable/resrep06751. Accessed 6 Apr. 2020.

Arora, Payal. “Benign Dataveillance? Examining Novel Data-Driven Governance Systems in India and China”. *First Monday*, vol. 24., no. 4, Apr. 2019, doi:10.5210/fm.v24i4.9840. Accessed 3 May 2020.

Article19. *International Annual Report 2019: Defending Freedom of Expression and Information around the World.* Article19, 2020. article19.org/wp-content/uploads/2020/04/A19_Annual_Report_2019.pdf. Accessed 1 July 2020.

Batty, Fodei. “No Questions Asked? Development and the Paradox of China’s Africa Policy.” *Insight Turkey*, vol. 21, no. 1, 2019, pp. 151–166. *JSTOR*, jstor.org/stable/26776052. Accessed 8 Apr. 2020.

Beach, Derek and Brun Pedersen, Rasmus. *Process-Tracing Methods. Foundations and Guidelines.* U of Michigan P, 2013.

Berthélémy, Chloé and Jan Penfrat. *Platform Regulation Done Right: EDRi Position Paper on the EU Digital Services Act.* European Digital Rights (EDRi), 9 April 2020. edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf. Accessed 15 June 2020.

Block, Hans and Moritz Rieseweck, directors. *The Cleaners.* Gebrueder Geetz Filmproduktion, 2018. *Bundeszentrale für politische Bildung*, fsk16.bpb.de/mediathek/273199/the-cleaners. Accessed 21 June 2020.

Bradsher, Keith. "How China Obtains American Trade Secrets." *The New York Times,* 15 January 2020, nytimes.com/2020/01/15/business/china-technology-transfer.html. Accessed 13 July 2020.

Brooks, Sarah M. “Will the Future of Human Rights Be ‘Made in China’?” *Dog Days: Made in China Yearbook 2018*, edited by Ivan Franceschini et al., ANU Press, 2019, pp. 170–175. *JSTOR*, jstor.org/stable/j.ctvfrxqcz.35. Accessed 13 May 2020.

Brühl, Jannis. "Zerreißprobe für das Internet." *Sueddeutsche.de,* 11 July 2020, sueddeutsche.de/digital/tiktok-usa-social-media-zensur-1.4963262. Accessed 11 July 2020.

Buzan, Barry et al. *Security: A New Framework for Analysis.* Lynne Rhienner Publishers, 1998.

Cave, Danielle, et al. *Enabling & Exporting Digital Authoritarianism*. Australian Strategic Policy Institute, 2019, pp. 8–15, *Mapping China’s Technology Giants*, jstor.org/stable/resrep23072.8. Accessed 18 Apr. 2020.

CIPESA (Collaboration on International ICT Policy for East and Southern Africa). *Digital Rights in Africa: Challenges and Policy Options,* March 2019, cipesa.org/?wpfb_dl=287. Accessed 21 July 2020.

Clement, Jessica. "Hours of video uploaded to YouTube every minute as of May 2019." *Statista,* 9 August 2019, statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute. Accessed 10 July 2020.

Clinton, Hilary. "Remarks by Secretary of State Hillary Rodham Clinton on Internet Freedom, January 21, 2010." *Financial Times*, 21 January 2010, ft.com/content/f0c3bf8c-06bd-11df-b426-00144feabdc0. Accessed 14 July 2020.

CNET. "Everything Facebook CEO Mark Zuckerberg just said to Congress in 16 minutes." *YouTube,* 30 July 2020, youtube.com/watch?v=EjU1chIhnug.

Collier, David. "Understanding Process Tracing." *PS: Political Science and Politics,* vol. 44, no. 4, 2011, pp. 823-30.

Constitution of Kenya, 2010. Adopted 27 August 2010. N*ational Council for Law Reporting*, kenyalaw.org:8181/exist/rest//db/kenyalex/Kenya/The Constitution of Kenya/docs/ConstitutionofKenya 2010.pdf. Accessed 5 July 2020.

Constitution of the Federal Democratic Republic of Ethiopia. Adopted 4 Dec. 1994. servat.unibe.ch/icl/et00000_.html. Accessed 3 July 2020.

Constitution of the Federal Republic of Nigeria. Act No. 24. Adopted 5 May 1999. *Federal Ministry of Justice.* refworld.org/docid/44e344fa4.html. Accessed 23 July 2020.

Constitution of the People's Republic of China. Adopted 4 December 1982. *The National People's Congress of the People's Republic of China.* npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm. Accessed 18 May 2020.

Constitution of the Republic of Ghana. No. 282. Adopted 28 April 1992*. GhanaWeb*. ghanaweb.com/GhanaHomePage/republic/constitution.php?id=Gconst5.html. Accessed 1 June 2020.

Constitution of Zimbabwe Amendment (No. 20) Act, 2013. Adopted 22 May 2013. *Refworld.* refworld.org/docid/51ed090f4.html. Accessed 30 July 2020.

Couldry, Nick and Ulises Meíias. "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?" *Internet Policy Review*, vol. 8, no. 2, 2019. doi:10.14763/2019.2.1411. Accessed 4 March 2020.

Court of Justice of the EU. *Judgement of the Court (C-311/18).* 16 July 2020. curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9710063. Accessed 18.07.2020.

Dean, Jodi. "Critique or Collectivity? Communicative Capitalism and the Subject of Politics." *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data,* edited by David Chandler and Christian Fuchs, U Westminster P, 2019, pp. 171–182.

Derakshan, Hossein. "Why Europe Should Build its own Social Platform for News." *The Guardian*, 2 July 2019, theguardian.com/commentisfree/2019/jul/02/europe-band-together-rival-facebook. Accessed 10 June 2020.

Dos Santos, Theotônio. “The Structure of Dependence.” *The American Economic Review*, vol. 60, no. 2, 1970, pp. 231–236. *JSTOR*, jstor.org/stable/1815811. Accessed 8 July 2020.

Drinhausen, Katja. "China's Digital Revolution". *The China dream goes digital: Technology in the Age of Xi,* published by European Council on Foreign Relations, 2018, pp. 2-4, *JSTOR,* jstor.org/stable/resrep21518. Accessed 10 May 2020.

Ehiane, Stanley O. “Strengthening the African Union (AU) Counter-Terrorism Strategy in Africa: A Re-Awakened Order.” *Journal of African Union Studies*, vol. 7, no. 2, 2018, pp. 109–126. *JSTOR*, jstor.org/stable/26889811. Accessed 8 Apr. 2020.

Ester, Peter. “Innovation and Startups in Silicon Valley: An Ecosystem Approach.” *Accelerators in Silicon Valley*, by Peter Ester, Amsterdam University Press, Amsterdam, 2017, pp. 37–62. JSTOR, jstor.org/stable/j.ctt1zrvhk7.7. Accessed 15 July 2020.

European Commission. "The Digital Services Act Package". *Europa.eu,* 22 June 2020, ec.europa.eu/digital-single-market/en/digital-services-act-package. Accessed 18.07.2020.

European Commission. *Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy*. 2 May 2017, /ec.europa.eu/europeaid/sites/devco/files/swd-digital4development_part1_v3.pdf. Accessed 4 April 2020.

European Commission. *Republic of Ghana – European Union, National Indicative Programme 2014–2020.* 19 June 2014. ec.europa.eu/international-partnerships/system/files/nip-ghana-20140619_en.pdf. Accessed 1 August 2020.

European Court of Human Rights. "Access to Internet and freedom to receive and impart information and ideas." *Council of Europe*, June 2020. echr.coe.int/Documents/FS_Access_Internet_ENG.pdf. Accessed 23 July 2020.

European Investment Bank. *EU-Africa Infrastructure Trust Fund. Annual Report 2018.* European Investment Bank, 2019, eib.org/attachments/country/eu_africa_infrastructure_trust_fund_annual_report_2018_en.pdf. Accessed 2 May 2020.

European Parliament. *Charter of Fundamental Rights of the European Union*. Office for Official Publications of the European Communities, 2000.

Evdokimov, Leonid et al. "Ethiopia: Verifying the Unblocking of Websites." *Open Observatory of Network Interference (OONI),* 29 June 2018, ooni.org/post/ethiopia-unblocking. Accessed 26 June 2020.

Facebook. "Building a transformative subsea cable to better connect Africa." *Facebook,* 13 May 2020, engineering.fb.com/connectivity/2africa. Accessed 7 June 2020.

Facebook. "Enabling better global connectivity through new partnerships and technologies." *Facebook,* 25 February 2019, connectivity.fb.com/news/mobile-world-congress-2019. Accessed 4 June 2020.

Federal Democratic Republic of Ethiopia. Anti-Terrorism Proclamation. No. 652/2009, adopted 28 Aug. 2009. *Federal Negarit Gazeta*, no. 57, pp. 4827-4842. ilo.org/dyn/natlex/docs/ELECTRONIC/85140/95140/F260526391/ETH85140.pdf. Accessed 8 July 2020.

Ferraro, Vicent. "Dependency Theory: An Introduction." *The Development Economics Reader*, edited by Giorgio Secondi. Routledge, 2008, pp. 58-64. *Mount Holyoke College,* mtholyoke.edu/acad/intrel/depend.htm. Accessed 6 July 2020.

Fick, Maggie. "Ethiopia to issue two telecom licenses, minority stake in monopoly: official." *Reuters*, 5 July 2019, reuters.com/article/us-ethiopia-telecoms/ethiopia-to-issue-two-telecom-licenses-minority-stake-in-monopoly-official-idUSKCN1U01M8. Accessed 15 July 2020.

Fine, Shoshana, et al. *False moves: Migration and development aid*. European Council on Foreign Relations, 2019, jstor.org/stable/resrep21606. Accessed 11 Apr. 2020.

Flanders, M. June. “Prebisch on Protectionism: An Evaluation.” *The Economic Journal*, vol. 74, no. 294, 1964, pp. 305–326. *JSTOR*, jstor.org/stable/2228481. Accessed 8 July 2020.

Forum on China-Africa Cooperation (FOCAC). "Forum on China-Africa Cooperation Beijing Action Plan (2019-2021)". *FOCAC,* 09 December 2018. focacsummit.mfa.gov.cn/eng/hyqk_1/t1594297.htm Accessed 22 July 2020.

Foster, Christopher and Shamel Azmeh. “The Digital Trade Agenda and Africa.” *Bridges Africa,* vol. 7, no. 2, 2018, pp. 15-18. ictsd.iisd.org/sites/default/files/bridges_africa_march2018.pdf. Accessed 8 April 2020.

Freedom House. "Ethiopia." *Freedom House,* 2019. freedomhouse.org/country/ethiopia/freedom-net/2019. Accessed 7 July 2020.

Freedom House. "Internet Freedom Scores." *Freedom House,* 2019. freedomhouse.org/countries/freedom-net/scores?sort=desc&order=Total%20Score%20and%20Status. Accessed 21 July 2020.

Freedom House. "Kenya." *Freedom House,* 2019. freedomhouse.org/country/kenya/freedom-net/2019. Accessed 9 July 2020.

Freedom House. "Nigeria." *Freedom House,* 2019. freedomhouse.org/country/nigeria/freedom-net/2019. Accessed 10 July 2020.

Freedom House. "Zimbabwe." *Freedom House,* 2019. freedomhouse.org/country/zimbabwe/freedom-net/2019. Accessed 13 July 2020.

Fuchs, Christian. "Appropriation of Digital Machines and Appropriation of Fixed Capital as the Real Appropriation of Social Being: Reflections on Toni Negri’s Chapter." *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data,* edited by David Chandler and Christian Fuchs, U Westminster P, 2019, pp. 215-222.

Gagliardone, Iginio. *China, Africa and the Future of the Internet*. Zed Books, 2019.

Gardner, Tom. "Will Abiy Ahmed's Bet on Ethiopia's Political Future Pay Off?" *Foreign Policy,* 21 January 2020. foreignpolicy.com/2020/01/21/will-abiy-ahmed-eprdf-bet-ethiopia-political-future-pay-off. Accessed 27 June 2020.

Gosh, Shona and Jake Kanter. "Google says data is more like sunlight than oil, one day after being fined $57 million over its privacy and consent practices." *Business Insider,* 22 January 2019. businessinsider.com/google-data-is-more-like-sunlight-than-oil-france-gdpr-fine-57-million-2019-1. Accessed 3 May 2020.

Greenleaf, Graham. "The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108." *University of New South Wales Faculty of Law Research Series,* vol. 42, 2011, pdfs.semanticscholar.org/7039/5f9bf6608a7310d3c248fecd55cc7e997b52.pdf. Accessed 9 July 2020.

Hackenesch, Christine. *The EU and China in African Authoritarian Regimes. Domestic Politics and Governance Reforms.* Palgrave Macmillan, 2018.

Harsin, Jayson. "Regimes of Posttruth, Postpolitics, and Attention Economies." *Communication, Culture & Critique*, vol. 8, no. 2. pp. 327-333. doi:10.1111/cccr.12097. Accessed 8 March 2020.

Horne, Felix. "How US Surveillance Helps Repressive Regimes—the Ethiopia Case." *Human Rights Watch,* 3 October 2017, hrw.org/news/2017/10/03/how-us-surveillance-helps-repressive-regimes-ethiopia-case. Accessed 23 July 2020

International Telecommunication Union (ITU). "WSIS 2020 High-Level Interactive Policy Sessions". *ITU,* n.d., itu.int/net4/wsis/forum/2020/HighLevel Accessed 28.07.2020

International Telecommunication Union (ITU). *Measuring digital development: Facts and figures 2019*. ITU Publications, 2019. itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf. Accessed 18 June 2020.

Internet World Stats. "Internet Users Statistics for Africa." *Internet World Stats,* March 2020. internetworldstats.com/stats1.htm. Accessed 21 July 2020

Jili, Bulelani. "Chinese Social Credit Initiatives and African Surveillance States." FUTUREID3: Identification in the Era of Automated Decision Making, 18–21 March 2019, Cambridge.

Joubert, Anke et al. "Big Data Readiness Index – Africa in the Age of Analytics." *Digital Transformation for a Sustainable Society in the 21st Century*. Edited by Ilias O. Pappas et al. Springer Nature, 2019.

Kania, Elsa B. "Enthusiasm and Challenges in China's Embrace of AI." *The China dream goes digital: Technology in the Age of Xi,* published by European Council on Foreign Relations, 2018, pp. 9-12, *JSTOR,* jstor.org/stable/resrep21518. Accessed 10 May 2020.

Kazeem, Yomi. "Kenya is stepping up its citizens' digital security with a new EU-inspired data protection law." *Quartz Africa*, 12 November 2019. qz.com/africa/1746202/kenya-has-passed-new-data-protection-laws-in-compliance-with-gdpr. Accessed 14 July 2020.

Kemp, Simon. "Digital 2020: Ghana" *Datareportal,* 18 February 2020, datareportal.com/reports/digital-2020-ghana. Accessed 24.07.2020

Kendi, Ibram X. "The Day *Shithole* Entered the Presidential Lexicon". *The Atlantic* 13 January 2019. theatlantic.com/politics/archive/2019/01/shithole-countries/580054. Accessed 15 July 2020.

Kessler, Jeremy K. and David E. Pozen. "The search for an egalitarian first amendment" *Columbia Law Review*, vol. 118, no. 7, 2018, pp. 1953–2010. *JSTOR*, jstor.org/stable/26524952. Accessed 14 July 2020.

Kontargyris, Xenofon. *IT Laws in the Era of Cloud Computing. A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy.* Nomos, 2018.

Kreye, Andrian. "Monopol des Hasses." *Süddeutsche Zeitung Online*, 6 July 2020, sueddeutsche.de/politik/facebook-hass-monopol-1.4954589. Accessed 6 July 2020.

Kriebitz, Alexander and Christoph Lütge. "Artificial Intelligence and Human Rights: A Business Ethical Assessment." *Business and Human Rights Journal,* vol. 5, no. 1, 2020, pp. 1–21, doi:10.1017/bhj.2019.28. Accessed 17 May 2020.

Lamer, Wiebke. *Press Freedom as an International Human Right.* Palgrave Pivot, 2018.

Leenes, Ronald. "Regulating New Technologies in Times of Change". *Regulating New Technologies in Uncertain Times,* edited by Leonie Reins, pp. 3–17. T.M.C. Asser Press, 2019.

Lessig, Lawrence. *Code. Version 2.0*. Basic Books, 2006.

Lewis, James A. "Racing the Paper Dragon." *China's Uneven High-Tech Drive: Implications for the United States*, edited by Scott Kennedy, published by Center for Strategic and International Studies (CSIS), 2020, pp. 16–20. csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200302_Kennedy_ChinaUnevenDrive_v3.pdf?33r3oE.zYL35PXvcofD5frIVeK1lzS9G. Accessed 20 Apr. 2020.

Mavhunga, Columbus. "Zimbabwe Activists Push Back on Social Media Restrictions." *Voice of America News*, 7 Feb. 2020. voanews.com/africa/zimbabwe-activists-push-back-social-media-restrictions. Accessed 7 April 2020.

Melber, Henning. "Stopping a dynasty does not mean democracy". *D+C* no.1, 2018, p. 13. dandc.eu/en/article/mugabe-era-over-mugabeism-likely-live. Accessed 27 July 2020

Mihr, Anja. *Cyber Justice: Human Rights and Good Governance for the Internet.* SpringerBriefs in Political Science, 2017.

Ministry of Foreign Affairs of the People's Republic of China. "Xi Jinping and Zimbabwean President Emmerson Mnangagwa Exchange Congratulatory Messages on the 40th Anniversary of the Establishment of China-Zimbabwe Diplomatic Relations." *Ministry of Foreign Affairs of the People's Republic of China,* 18 April 2020. fmprc.gov.cn/mfa_eng/zxxx_662805/t1771806.shtml. Accessed 22 June 2020.

Media Institute of Southern Africa (MISA). "High Court sets aside internet shutdown directives" *MISA,* 21 Jan. 2019, zimbabwe.misa.org/2019/01/21/high-court-sets-aside-internet-shut-down-directives. Accessed 27 July 2020.

Moyo, Sibusiso. "Towards a New Era in EU-Zimbabwe Relations". *EUObserver.com,* 22 Nov. 2019, euobserver.com/opinion/146676. Accessed 12 June 2020.

Musa, Muhammed. "Technology and the Democratic Space in Africa. A Re-Examination of the Notion of 'Digital Divide'." *Mapping the Digital Divide in Africa. A Mediated Analysis,* edited by Bruce Mutsvairo and Massimo Ragnedda, Amsterdam UP, 2019.

Mutsvairo, Bruce and Massimo Ragnedda. "Comprehending the Digital Disparities in Africa." *Mapping the Digital Divide in Africa. A Mediated Analysis,* edited by Bruce Mutsvairo and Massimo Ragnedda, Amsterdam UP, 2019.

National Assembly of the Federal Republic of Nigeria. Cybercrimes (Prohibition, Prevention, etc) Act, 2015, passed 5 May 2015. *Nigeria Computer Emergency Respose Team.* cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf. Accessed 27 July 2020.

Netblocks. "Ethiopia partially restores internet access days after blackout following reported Amhara coup attempt." *Netblocks*, 27 June 2019, netblocks.org/reports/ethiopia-partially-restores-internet-days-after-amhara-coup-attempt-blackout-V8xxlo8k. Accessed 29 June 2019.

NITDA (Nigerian National Information Technology Development Agency). *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT),* 2013. nitda.gov.ng/wp-content/uploads/2018/08/Guidelines-for-Nigerian-Content-Development.pdf. Accessed 27 July 2020.

Nyokabi et al. "The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa." *Global Campus Human Rights Journal* vol. 3, no 2, 2019, pp. 147-172. doi:20.500.11825/1582. Accessed 4 July 2020.

Odell, Rachel Esplin. "Chinese Regime Insecurity, Domestic Authoritarianism, and Foreign Policy." *Artificial Intelligence, China, Russia, and the Global Order, e*dited by Nicholas D. Wright, Air University Press, 2019, pp. 123–128. *JSTOR*, jstor.org/stable/resrep19585.22. Accessed 10 May 2020.

Office of the President, Republic of Ghana. "Vice President Bawumia Woos Silicon Valley Investors." *Office of the President, Republic of Ghana,* 15 April 2018, presidency.gov.gh/index.php/briefing-room/news-style-2/611-vice-president-bawumia-woos-silicon-valley-investors. Accessed 24 July 2020

Oginni, Simon Oyewole and Joash Ntenga Moitui. “Social Media and Public Policy Process in Africa: Enhanced Policy Process in Digital Age.” *Consilience*, no. 14, 2015, pp. 158–172. *JSTOR*, jstor.org/stable/26188747. Accessed 9 May 2020.

Ogunlana, Sunday O. “Halting Boko Haram / Islamic State’s West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies.” *Journal of Strategic Security*, vol. 12, no. 1, 2019, pp. 72–106. *JSTOR*, jstor.org/stable/26623078. Accessed 6 April 2020.

Okolloh, Ory and Sharon Wekwete. "As the continent digitizes rapidly, Africans need a bill of data rights to protect them online." *Quartz Africa*, 12 June 2019, qz.com/africa/1641394/africans-need-a-bill-of-data-rights-for-protection-in-digital-age. Accessed 8 Apr. 2020.

Olander, Eric. "African Union Caught in Middle of Bitter U.S.-China Feud Over Huawei". *The China Africa Project,* 12 Nov. 2019, chinaafricaproject.com/analysis/african-union-caught-in-middle-of-bitter-u-s-china-feud-over-huawei. Accessed 20 July 2020.

Onuoha, Raymond. "AI in Africa. Regional Data Protection and Privacy Policy Harmonisation." In *Artificial Intelligence. Human Rights, Social Justice and Development, e*dited by Global Information Society Watch, 2019, giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf. Accessed 18 Apr. 2020.

Oqubay, Arkebe & Justin Yifu Lin. "The Future of China-Africa Economic Ties." *China-Africa and Economic Transformation.* Oxford Scholarship Online: June 2019. doi:10.1093/oso/9780198830504.003.0015. Accessed 5 May 2020.

Organization of African Unity (OAU). African Charter on Human and Peoples' Rights ("Banjul Charter"). CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), adopted 27 June 1981. *African Union*, au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf. Accessed 11 April 2020.

Osiakwan, Eric (speaker). "The ITU: Building Connectivity and Cooperation in Internet Governance." *CRF.org* 20 Nov. 2014, cfr.org/event/itu-building-connectivity-and-cooperation-internet-governance-0. Accessed 24 July 2020

Parliament of Kenya. The Computer Misuse and Cybercrimes Act, 2018. Assented 16 May 2018, *Kenya Gazette Supplement*, no. 60. kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf. Accessed 26 July 2020.

Parliament of Kenya. The Security Laws (Amendment) Act, 2014. No. 19. Assented 22 Dec. 2014, *Kenya Gazette Supplement*, no. 167. kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf. Accessed 26.07.2020.

Paul, Kari. "Naked protesters condemn nipple censorship at Facebook headquarters." *The Guardian,* 3 June 2019, theguardian.com/technology/2019/jun/03/facebook-nude-nipple-protest-wethenipple. Accessed 5 July 2020.

PoKempner, Dinah. "Regulating Online Speech: Keeping Humans, and Human Rights, at the Core." *Free Speech in the Digital Age,* edited by Susan J. Brison and Katharine Gelber. Oxford UP, 2019.

Pompeo, Michael R. "Announcing the Expansion of the Clean Network to Safeguard America's Assets." *US Department of State,* 5 August 2020. state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets. Accessed 8 August 2020.

Przychodniak, Marcin. "China: Competitor in the Global Technological Race." *The China dream goes digital: Technology in the Age of Xi,* published by European Council on Foreign Relations, 2018, pp. 5-6, *JSTOR,* jstor.org/stable/resrep21518. Accessed 10 May 2020.

Ramluckan, Trishana et al. "The Relevance of South African Legislation on Social Media as a Strategic Disaster and Crisis Communications Tool." *Journal of Information Warfare*, vol. 15, no. 1, 2016, pp. 60–74. *JSTOR*, jstor.org/stable/26487481. Accessed 6 Apr. 2020.

Raymond, Mark and Laura DeNardis. "Multi-Stakeholderism: Anatomy of an inchoate global institution." *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance,* published by Centre for International Governance Innovation, 2017, pp. 19–44. *JSTOR,* jstor.org/stable/resrep05243.7. Accessed 13 July 2020.

Reins, Leonie. "Regulating New Technologies in Uncertain Times – Challenges and Opportunities." *Regulating New Technologies in Uncertain Times,* edited by Leonie Reins, pp. 19–28. T.M.C. Asser Press, 2019.

Ruggie, John Gerard. "Multilateralism: The Anatomy of an Institution." *International Organization,* vol. 46. no. 3, pp. 561–98, 1992.

Ryan, Fergus. "China's Online Warriors Want More Gates in the Firewall". *ForeignPolicy.com,* 29 June 2020. foreignpolicy.com/2020/06/29/china-great-firewall-wolf-warrior-nationalism. Accessed 19 July 2020.

Snowden, Edward. *Permanent Record.* Macmillan, 2019.

Srinivasan, Sharath et al. "Rethinking publics in Africa in a digital age". *Journal of Eastern African Studies*, vol. 13, no. 1, 2019, pp. 2-17. doi:10.1080/17531055.2018.1547259. Accessed 15 April 2020.

State Council of the People's Republic of China. *The Internet in China. White Paper*. 8 June 2010. china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm. Accessed 19.07.2020

State Council of the People's Republic of China. *Planning Outline for the Construction of a Social Credit System (2014–2020)*. Translated by China Copyright and Media, chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-1the-construction-of-a-social-credit-system-2014-2020. Accessed 28 April 2020.

Stokke, Kristian. "Process Tracing with Kristian Stokke". *YouTube.* Published by Institutt for Sosiologi og Samfunnsgeografi. youtube.com/watch?v=XCCXjgsA8MI.

Swanson, Ana et al. "Trump Targets WeChat and TikTok, in Sharp Escalation With China." *New York Times,* 6 August 2020. nytimes.com/2020/08/06/technology/trump-wechat-tiktok-china.html. Accessed 7 August 2020.

The Africa-EU Partnership. "AU-EU Human Rights Dialogue." *The Africa-EU Partnership*, n.d. africa-eu-partnership.org/en/projects/au-eu-human-rights-dialogue. Accessed 29 July 2020.

The Africa-EU-Partnership. "Action Document for Policy and Regulation Initiative for Digital Africa (PRIDA)". *Africa-EU-Partnership,* 2017, africa-eu-partnership.org/sites/default/files/pan-africa-programme-annexe-4_en.pdf. Accessed 22 July 2020.

The European Parliament and the Council of the European Union. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). *OJ L 119,* 4 May 2016, pp. 1–88. eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679. Accessed 23 June 2020.

The President and the Parliament of Zimbabwe. Interception of Communications Act. No. 6/2007 [Ch 11:20]. Adopted 3 August 2007. *Vertic.org.* vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf. Accessed 4 July 2020.

The [US] President's Advisory Council on Doing Business in Africa. "Fact-Finding Trip Report and Recommendations" *Trade.gov,* 26 September 2018, legacy.trade.gov/pac-dbia/docs/PAC-DBIA%20Final%20Report%20Sep%202018.pdf. Accessed 21 July 2020.

Tiloune, Joan and Ghalia Kadiri. "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin" *LeMonde.fr,* 26 Jan. 2020, lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html. Accessed 22.07.2020.

Trump, Donald, @realDonald Trump. "Republicans feel that Social Media Platforms totally silence conservatives voices. We will strongly regulate, or close them down, before we can ever allow this to happen. We saw what they attempted to do, and failed, in 2016. We can't let a more sophisticated version of that.... ." *Twitter,* 27 May 2020, 13:11, twitter.com/realDonaldTrump/status/1265601611310739456.

Twitter. "Trump makes unsubstantiated claim that mail-in ballots will lead to voter fraud." *Twitter,* 26 May 2020. twitter.com/i/events/1265330601034256384?s=13. Accessed 29 May 2020.

UN Committee on Economic, Social and Cultural Rights (CESCR). *Concluding observations on the second periodic report of China, including Hong Kong, China, and Macao, China.* E/C.12/CHN/CO/R.2, 13 May 2014. *Refworld.* refworld.org/docid/53c77e524.html. Accessed 8 July 2020.

UN Conference on Trade and Development (UNCTAD). *World Investment Report 2019.* 12 June 2019. unctad.org/en/PublicationsLibrary/wir2019_en.pdf. Accessed 19 June 2020.

UN General Assembly. *International Covenant on Civil and Political Rights (ICCPR)*, 16 December 1966, United Nations, Treaty Series, vol. 999. ohchr.org/en/professionalinterest/pages/ccpr.aspx. Accessed 15 July 2020.

UN Human Rights Committee (HRC). *General comment no. 34, Article 19, Freedoms of opinion and expression.* CCPR/C/GC/34,12 September 2011. ohchr.org/english/bodies/hrc/docs/gc34.pdf. Accessed 8 July 2020.

UN Secretariat of the Internet Governance Forum. "National IGF Initiatives." *Internet Governance Forum,* n.d. intgovforum.org/multilingual/content/national-igf-initiatives. Accessed 7 August 2020.

UN Security Council. *Security Council resolution 1373 (2001).* S/RES/1373 (2001), 28 September 2001. undocs.org/S/RES/1373(2001). Accessed 6 April 2020.

UN Treaty Collection. "International Covenant on Civil and Political Rights." *United Nations*, 3 July 2020. treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND. Accessed 3 July 2020.

UN Treaty Collection.“Optional Protocol to the International Covenant on Civil and Political Rights.” *United Nations,* 3 July 2020. treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-5&chapter=4&lang=en. Accessed 3 July 2020.

United States, Executive Office of the President [Donald Trump]. Executive Order 13925: Preventing Online Censorship. 28 May 2020. *Federal Register*, 2 June 2020, pp. 34079-83. whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship. Accessed 4 June 2020.

US Constitution. Amendment I. Adopted 15 December 1791. National Archives. archives.gov/founding-docs/bill-of-rights-transcript. Accessed 8 June 2020.

US Department of State. *Internet Freedom,* 2017. state.gov/wp-content/uploads/2019/03/Internet-Freedom.pdf. Accessed 9 April 2020.

US Department of State. *US Partnership With the African Union.* 15 November 2019, state.gov/wp-content/uploads/2019/03/Internet-Freedom.pdf Accessed 24.06.2020.

Van Dijk, Pieter et al. "Freedom of Expression." *Theory and Practice of the European Convention on Human Rights,* edited by Pieter van Dijk et al., Intersentia, 2018.

Van Raemdonck, Nathalie. "What if … Europe created an international social/news platform?" *WHAT IF …? 14 Futures for 2024*, edited by Florence Gaub and European Union Institute for Security Studies (EUISS), 2020, pp. 24–29, *JSTOR*, jstor.org/stable/resrep21146.7. Accessed 16 Apr. 2020.

Viljoen, Frans. “Understanding and Overcoming Challenges in Accessing the African Court on Human and People's Rights.” *International and Comparative Law Quarterly*, vol. 67, no. 1, 2018, pp. 63–98. doi:10.1017/S0020589317000513. Accessed 20 April 2020.

VPN Mentor. "The Complete List of Blocked Websites in China & How to Access Them". *VPN Mentor* 16 June 2020, vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them. Accessed 19 July 2020

Wæver, Ole. “Politics, Security, Theory.” *Security Dialogue*, vol. 42, no. 4/5, 2011, pp. 465–480. *JSTOR*, jstor.org/stable/26301802. Accessed 8 July 2020.

Weber, Valentin. "Understanding the Global Ramifications of China’s Information-Control Model." *Artificial Intelligence, China, Russia, and the Global Order* Air, edited by Nicholas D. Wright, University Press, 2019, pp. 76–80. *JSTOR,* jstor.org/stable/resrep19585.15. Accessed 8 April 2020.

World Justice Project. *Rule of Law Index. 2020.* World Justice Project, 2020. worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2020-Online_0.pdf. Accessed 19 July 2020.

Xi, Jinping. "Full text of Chinese President Xi Jinping's speech at opening ceremony of 2018 FOCAC Beijing Summit." *Xinhua,* 3 Sept. 2018. xinhuanet.com/english/2018-09/03/c_137441987.htm. Accessed 11 June 2020.

Xi, Jinping. "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference." *Ministry of Foreign Affairs of the People's Republic of China,* 16 December 2015. fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml. Accessed 20.07.2020

Yan, Li. "Reforming Internet Governance and the Role of China". *Focus Asia* no. 12, 2015. isdp.eu/content/uploads/publications/2015-LiYan-Reforming-Internet-Governance-and-the-role-of-China.pdf. Accessed 15.07.2020

YouTube. "Global Reach." *YouTube,* n.d. youtube.com/intl/en-GB/about/press/. Accessed 5 July 2020.

Zhang, Denghua. *A Cautious New Approach: China's Growing Trilateral Aid Cooperation*. ANU Press, 2020. *JSTOR*, jstor.org/stable/j.ctv103xdqk. Accessed 20 April 2020.