MEGATRENDS Afrika

Benedikt Erforth

Data Extraction, Data Governance and Africa–Europe Cooperation: A Research Agenda

Working Paper 14
July 2024, Bonn

Dr. Benedikt Erforth
Project Lead at Megatrends Afrika and Senior Researcher at IDOS
Benedikt.Erforth@idos-research.de

Executive summary

At the heart of the ongoing digital transformation lies the force of data. Its processing and utilization stand as the cornerstone of unprecedented advancements and innovations, rendering data one of the most prized assets in today's information age. Embedded in a global competition for markets, influence, and ideas, the extraction and governance of data also affects the relationship between Africa and Europe. Historically, Africa has trailed behind in terms of regulation of the digital space. Nevertheless, as the youngest continent, it hosts a growing population of digital natives, also fostering better and more comprehensive approaches to data governance. Under the auspices of the African Union (AU) and pioneering countries, Africa has adopted a more strategic and assertive approach towards its digital transformation trajectory. No fewer than 36 African states have enacted some sort of data protection guidelines at the time of writing. After ten years of waiting, the AU data protection convention entered into force in 2023. Conversely, the European Union (EU) stands as a global leader in data governance, advocating for a regulated digital sphere to promote what it terms a human-centric approach to data. Moreover, the EU leverages the export of its regulatory model as a strategic tool to assert its position in a digital realm dominated by both state and non-state actors from the United States and China.

Drawing on an extensive review of the literature, alongside first-hand interview material and survey data collected in six African countries, the paper delves into the dynamics and patterns of cooperation between Africa and Europe within the domain of digital data governance, shedding light on both promising avenues and inherent constraints. Based on this analysis, the text draws three main conclusions.

First, it observes a highly dynamic African data space with increasing uptake of regulatory frameworks and data protection norms. At the same time, it points to persisting differences between countries, and to the challenges in implementing newly established legislation.

Second, the EU's pioneering role in this domain not only strengthens existing partnerships but also offers new avenues of intensified cooperation. A more regulated and standardized African data space can be beneficial for individual African citizens as well as for economic growth. However, and despite global leadership in the area of data protection, the EU is only one among many partners when it comes to the African digital market, and its investment remains modest by comparison with that of others. This is important to note, as investment, knowledge exchange and regulatory harmonization need to go hand in hand in order to realize full potential and create a strong partnership between the two regions.

Third, it remains uncertain whether the solutions on offer align with existing demands. African tech entrepreneurs, innovators, and policymakers may not necessarily turn to the EU when charting their technological trajectories and innovation paths. In particular, the EU's emphasis on regulatory rigour is not always embraced by everyone but is sometimes even viewed as a hindrance to economic development. Debates in Africa focus on the appropriate and balanced level of regulation, with various stakeholders advancing different viewpoints. And while the benefits of a digital single market are emphasized by both African

and European policymakers, it is crucial not to overlook the disparities between the two regions (as well as within them).

In light of these observations, the paper advocates for the EU to follow a strategic and differentiated approach to cooperation, and to avoid adopting an overly paternalistic stance that heavily relies on conditionality. Instead, it recommends fostering a discourse centred on the global significance of data sovereignty and leveraging the EU's expertise in establishing a digital single market as a constructive contribution to the partnership. Further research can offer more dependable data regarding local demands in various different African contexts as well as unpacking Africans' perceptions of the different digital governance models vying for the continent's consideration. Additionally, exploring the nexus between regime types and the adoption of digital governance is prone to produce valuable insights.

Content

Introduction

The processing and appropriation of data is at the core of unprecedented advances and innovations, making data one of the most valuable resources of the modern information age. Major technology companies have perfected the extraction, systematization and monetization of data trails of billions of humans and in so doing made extraordinary profits.[1] In 2023, the market valuation of Alphabet surpassed that of the entire German DAX Index, while Amazon's annual revenue exceeded the GDP of any African economy.[2] These companies provide innovative services and uncover previously unknown information to the extent that they generate novel forms of knowledge and capabilities that in specific areas already surpass human skills. This holds true even before considering all the possible implications of the ongoing AI revolution.

The potential of digital solutions extends to industrialized, emerging, and developing markets alike, presenting substantial opportunities for progress and growth. In Africa, in particular, where young populations and a comparatively untapped market spur growth fantasies, the digital is poised to spark major transformations in the upcoming decades. Much of the digital promise is rooted in the sector's economic might. A collaborative report by the International Finance Corporation (IFC) and Google – relying on forecast data by Accenture – projects the internet economy to contribute nearly USD 180 billion (5.2% of projected GDP) to Africa's economy by 2025 and USD 712 billion (8.5% of projected GDP) by 2050.[3] While these projections underscore the vast potential of the digital economy, they also highlight the persistent technology gap between Africa and other world regions. A telling example of this duality is evident in the successful acquisition of USD 1.2 billion in start-up funding by Africa in 2020 – a substantial six-fold surge since 2015. Yet, in the broader context, this figure remains a mere fraction, representing less than 1% of the staggering USD 156 billion raised by US start-ups in the same year.[4] By 2025, venture capital investment in Africa is forecast to reach USD 10 billion, with a strong concentration of capital in Nigeria, Kenya, Egypt, South Africa, and Ghana.[5] Most importantly, these projections are contingent upon the implementation of appropriate policies and increased technology adoption by businesses.[6] Data extraction and its monetization not only revolutionize the human existence and offer significant business opportunities, they also pose a threat to the right to privacy, fostering surveillance, and exacerbating social inequalities. *Datafication* refers to the continuous and pervasive recording of everyday data. Some of this data rendering is willingly accepted by citizens, while most is collected without our awareness.[7] The large-scale purchase of surveillance technologies by African governments is just one example of how new technologies, intended to address issues like crime prevention and

[1] Soshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette, 2019).
[2] Data retrieved from: Companies Market Cap, https://companiesmarketcap.com/; Deutsche Börse https://www.boerse.de; and International Monetary Fund, https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD.
[3] Google and International Finance Cooperation (IFC), e-Conomy Africa 2020: Africa's $180 Billion Internet Economy Future, (Google, IFC, 2020), 15-17. N.B. The forecast relies on extrapolation and as such is subject to high levels of uncertainty.
[4] Harsha Desai et al., Regional Action Group for Africa: Attracting Investment and Accelerating Foruth Industrial Revolution Adoption in Africa, *White Paper: January 2022* (World Economic Forum & Deloitte, 2022).
[5] Niall McCarthy, Funding for Africa's Startups Is at a Record High–This Is Where It's Going (*World Economic Forum,* 2021).
[6] Google and IFC, e-Conomy Africa 2020, 15-17. N.B. The forecast relies on extrapolation and as such is subject to high levels of uncertainty.
[7] Wendy H. Wong, *We, the Data* (Cambridge, MA: MIT Press 2023), 3.

conviction rates, often simultaneously and purposefully undermine privacy rights and freedoms, as seen in Uganda and Zambia.[8] Uganda's USD 126 million purchase of Huawei CCTV equipment in 2019 illustrates this and also points to the interlinkage of the economic and the geopolitical dimensions of the digital revolution.[9]

The harvested information endows technology firms with unprecedented levels of control over people. Echoing Foucault's surveillance paradigm (panopticism), control – be it for the purpose of economic gain or political power – in the digital era hinges predominantly on constant, pervasive, and automated observation.[10] Consequently, a handful of corporations wield power surpassing that of nation-states by a considerable margin. Economists refer to this phenomenon as "a positive network effect", whereby a select few platforms amass user bases rivalling or even surpassing entire populations of states or even continents.[11]

In contexts where the establishment of robust data protection measures is either still underway, or enforcement is lacking, citizens are particularly vulnerable to abuse and exploitation. This reality is prevalent across many African countries, where the potential benefits of the digital revolution intersect with the risks of extractive practices.

The Geopolitics of Technology

Whilst the digital revolution's key players – corporations – are actors in their own right and in pursuit of economic gains, they emerge and act in a given political and socio-cultural context. The competition over who controls whose data brings to the fore hard-nosed interests. In their quest for power, influence or returns, corporations and states seek to extract and shape the digital world according to their own preferences, often without any regard to those from whom the information emanates in the first place. States also proactively engage in the collection and treatment of data for a wide variety of reasons, ranging from economic competition, strategic autonomy, security-related concerns to absolute control of their citizenry. As such, states find themselves in a dual role: they can either protect their citizens against abusive data extraction or leverage data pools for their own interests.

Amidst the ongoing geo-political competition, various great powers present diverse propositions concerning the treatment of data, each emanating from different political and societal traditions and resonating with distinct stakeholder groups. Among the leading economies, the US, China, and the EU adopt contrasting approaches to digital governance.

The US embraces a liberal, business-driven stance, which critics associate with the concerning practices of *surveillance capitalism*.[12] Capitalizing on a largely hands-off approach by the US government, Silicon Valley has seized the opportunity to assert its dominance in the global digital landscape. China puts forth a model centred on state-led techno-policy and innovation, and strong surveillance, coupled with extensive investment in infrastructure. With the introduction of the Digital Silk Road (DSR), China "combines the domestic push to export Chinese technologies developed with assertive industrial policies, with a broader agenda to augment interoperability and compatibility between Chinese and overseas technological networks, on Chinese terms".[13] While Europe has been instrumental in

[8] Samuel Woodhams, "Huawei Says its Surveillance Tech Will Keep African Cities Safe but Activists Worry it'll Be Misused," *Quartz,* 2020.
[9] Elias Biryabarema, "Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei," *Reuters,* 2019.
[10] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (London: Penguin, 1975 (1991)).
[11] Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI and Our Human Future* (London: John Murray, 2021), 95-96.
[12] Zuboff, *The Age of Surveillance Capitalism.*
[13] Brigitte Dekker, Maaike Okano-Heijmans, and Eric Siyi Zhang, Unpacking China's Digital Silk Road, (*Clingendael Report,* July 2020), 2.

laying much of the groundwork for the digital revolution, the EU faces challenges in building a digital ecosystem that rivals others. In response, it focuses on leveraging its current strengths and advocating for robust regulation, positioning itself as a champion of a human-centric approach to data usage. This approach is an attempt to win partners' hearts and minds. It entails a robust and effective regulatory framework, with a primary focus on safeguarding individual privacy rights. Simply put, the United States leads in exporting its private sector, which includes some of the world's most valuable companies, China wields power and influence through extensive infrastructure programmes by means of which it also seeks to export its alternative regulatory model, whereas Europe focuses on influence qua regulation.[14]

That said, these different models also share commonalities. For instance, arguments for a rules-based international digital order (although with a different outlook) can be heard in Europe, China, and the US. Most importantly, each of the three models can be conceptualized and comprehended as imperial enterprises with their own unique characteristics.[15] Their divergent strategies underscore the significance of data in shaping global dynamics, as these great powers vie for influence and control over the digital realm. Each approach carries its own allure and implications, adding complexity to the evolving landscape of digital governance and its far-reaching impact on societies and economies worldwide. In their difference, the digital empires share the fact that they are "both admired and reviled across the territories that fall under their influence".[16]

The reason why such initiatives, whether we define them as imperialistic or simply as efforts at norm externalization, take root in Africa is partly due to the constituent nations of Africa having been reluctant to develop their own data protection frameworks and promote their underlying principles. This inertia stems from a variety of factors, including resource constraints, lack of political impetus, and a low level of awareness of the risks of unregulated data extraction.[17] Other explanations advance the contested view of the collectivist nature of African societies.[18] And yet others point to divergent priorities, and, as Abdulrauf argues, a belated recognition by the African Union (AU) of its pivotal role in championing data privacy and regulatory compliance. The specific composition of factors varies between countries. The thinking has changed, but has also put the continent at a disadvantage and has relegated it primarily to the role of a norm taker rather than a norm maker.[19]

By intertwining discussions on digital empires with the swift technological evolution occurring on the African continent, this study calls for the filling of a void in the existing literature, which has yet to delve into detailed and more systematic analyses of how African governments interact with various digital partnership proposals. The focus of this study centres on the crucial role of data governance in the Europe–Africa relationship. This consideration takes into account the vast potential and associated risks linked to data as the foundation of the digital transformation.[20] The significance of this focus emerges from Africa's rapid

[14] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 290.
[15] It is important to note that the global competition for digital leadership extends beyond these three entities. However, at the time of writing, these three pools possess the most far-reaching influence over global data regulation. Consequently, they are at the heart of the following considerations.
[16] Bradford, *Digital Empires,* 21.
[17] Lukman Adebisi Abdulrauf, "Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms" *Information & Communications Technology Law* 30, no. 2 (2021): 98.
[18] Alex B. Makulilo, "A Person Is a Person through Other Persons - a Critical Analysis of Privacy and Culture in Africa," *Beijing Law Review* 7 (2016). Makulilo refutes the notion of Africans living in a collectivist culture as overly static. Instead, privacy in Africa, too, is an evolving concept allowing for the emerging of privacy regulation over time.
[19] Abdulrauf, "Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms".
[20] For a more detailed comparison between the different models, see: Benedikt Erforth and Kerstin Fritzsche, *Towards a Digital Development Partnership that Meets African Interests* (Washington, DC: Heinrich Böll Stiftung,

adoption of digital tools, existing interdependencies, and the EU's substantial commitment to contributing to African data regulation. It is further corroborated by the fact that China and the US also engage in regulatory outreach, rendering the field increasingly contested.

As a yardstick of the state of the current debate, and as a conversation starter, the paper begins with a brief overview of key definitions and trends pertaining to data governance in the African data space(s). The section highlights both risks and opportunities associated with data processing in the region. It also points to the latest advancements in the realm of data regulation, which oscillate between African self-assertion and adoption of international, mainly European, standards. The subsequent section introduces the core tenets of the geopolitical competition on data, and explores the European approach to global data governance, which also goes by the Brussels-bred moniker "human-centric approach" and makes use of the "Brussels effect", which denotes the "unilateral power to regulate global markets", examining its reach and limitations.[21] Lastly, the paper evaluates the potential, limitations, and areas of cooperation between Africa and Europe in the realm of data. The section argues that the EU's regulatory influence carries weight in Africa and could bolster the continent's regulatory landscape. However, while it presents opportunities, it is not a cure-all for the challenges faced by African nations and, in its rigid application, may even impede the continent's economic progress. EU involvement in African data regulation must prioritize mutual ownership and acknowledge regional disparities to be effective. In essence, drawing on extensive desk and literature research, ten expert interviews conducted between 2020 and 2024, and first-hand survey data in six African countries, this paper explores data governance in the African context and the prospects for fruitful cooperation between Europe and Africa, all while acknowledging the broader ramifications of such efforts in our rapidly changing world.

2022); Chloe Teevan and Lidet Shiferaw Tadesse, *Digital Geopolitics in Africa: Moving from Strategy to Action*, B*riefing Note* 150 (ECDPM, 10 October 2022); Bradford, *Digital Empires.*

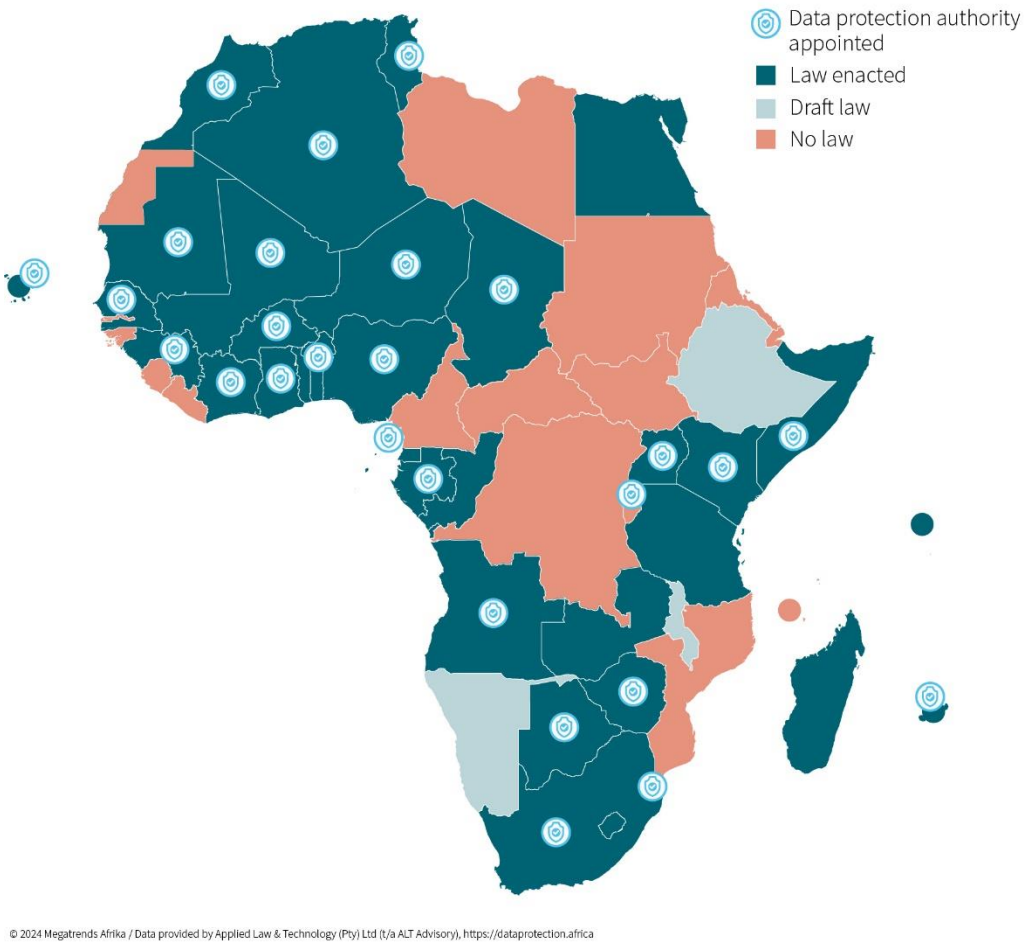
[21] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press 2020).

The Regulatory State of the African Data Space

Africa is currently witnessing one of the most rapid data protection adoption rates on a global scale. At the current rate of adoption, one can anticipate that by the end of the 2020s data protection frameworks will encompass the entire continent. The political goals of African data protection frameworks at the continental, regional, and local levels centre on economic development qua harmonization and giving Africa a voice at the global stage. Human rights and the privacy of citizens are also part of the canon but are less emphasized than in Europe.[22] The primary challenge for African data protection, however, does not lie in the absence of or insufficient regulation; instead, it resides in the effective implementation and enforcement of these laws.

The African digital landscape has historically operated in a state of relative regulatory ambiguity. More recently, both on a national and continental scale, Africa has undergone a significant regulatory transformation, resulting in the adoption of more robust data protection and privacy frameworks. Whilst substantial differences between countries persist, to date,[23] the proliferation of digital solutions and the rapid expansion of internet and smartphone usage have underscored the necessity for comprehensive data privacy laws. Before 2016, only 16 African countries had established specific data protection legislation,[24] but as of the time of writing, this number has risen to 36 across the continent. Notably, the majority of these data protection laws empower designated independent data protection authorities, a crucial component of a well-functioning data protection scheme. Despite provision for such authorities, it is worth noting that approximately half of the African countries with data protection regulations in place have yet to establish these oversight bodies.[25] In some cases, these authorities have limited or no independence from the funding ministry. Only 11 countries have implemented safeguards to prevent the unjust removal of data protection commissioners, while 14 countries remain ambiguous on the matter, and another 11 lack such protection altogether.[26] While the potential for constitutional protection of privacy in Africa is considerable, practical application remains limited, with minimal case law to date.[27] Consequently, a significant gap persists between the theoretical commitment to data privacy and its real-world implementation. Without adequate regulation, individuals are left vulnerable to potential exploitation and misuse of their personal data by both public and private entities. This lack of oversight increases the likelihood of data breaches, identity theft, and infringement of individuals' privacy rights, undermining trust in digital systems but also hindering economic and social development due to the limited access that African companies have to more regulated markets.

[22] Graham Greenleaf and Bertil Cottier, "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis," *Computer Law & Security Review* 44, no. April (2022): 33.
[23] *Data Protection Africa*, https://dataprotection.africa/.
[24] Brian Daigle, "Data Protection Laws in Africa: A Pan-African Survey and Noted Trends," *Journal of International Commerce and Economics* February (2021): 6.
[25] Greenleaf and Cottier, "International and Regional Commitments in African Data Privacy Laws," 6-7.
[26] Data Protection Africa, "How Independent Are African Data Protection Authorities? ," https://dataprotection.africa/standing-alone-the-independence-of-african-data-protection-authorities/.
[27] Greenleaf and Cottier, "International and Regional Commitments in African Data Privacy Laws," 10.



At the continental level, the AU's Digital Transformation Strategy for Africa (2020–2030), which builds on several regional and international initiatives, seeks to harmonize digital policies to allow the creation of an African Digital Single Market. The AU strategy emphasizes the importance of "continental ownership with Africa as a producer and not only a consumer in the global economy"[28] as well as the need to "[e]nsure digital identity data belongs to, and remains in the control of Africans".[29]

The 2014 Malabo Convention on Cybersecurity and Personal Data Protection constitutes an important step towards a more data-secure Africa. It reflects the AU's commitment to African ownership and calls for a continent-wide common data protection framework.[30] Nine years after its adoption, the Malabo Convention came eventually into force on 8 June 2023, following Mauritania's ratification of the document by which the threshold of 15 ratifying nations was passed. The Convention is a milestone in African data protection law. It is also the "only binding regional treaty on data protection outside Europe".[31] The Convention derives the right to privacy from international human rights law, and calls upon each state party that it shall "commit itself to establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal

[28] African Union, *The Digital Transformation Strategy for Africa 2020-2030*, (Addis Ababa: African Union, 2020), 2.
[29] Ibid., 42.
[30] Daigle, "Data Protection Laws in Africa," 2.
[31] Yohannes Eneyew Ayalew, The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force nearly after a Decade. What Does it Mean for Data Privacy in Africa or Beyond?, EJIL: Talk!, 17 June 2023.

data."[32] Concretely, for Guinea Bissau and Sierra Leone, two countries without data protection laws, who have signed yet not ratified the Convention, this means that they are now obliged under international law to enact a national privacy law. For monist countries among the signatories (Rwanda, Mozambique, Namibia), the entering into force of the AU convention implies that the convention should become part of their national laws. In practice, however, it is expected that Rwanda and Mozambique will apply a more narrow interpretation of the provisions.[33]

As these examples show, there is a momentum in the African data space. Several factors instigated this rise in data protection legislation. First, the increased penetration of digital technologies and growing digital markets across the continent make more sophisticated regulatory frameworks necessary. Second, African nations, both individually and at the AU-level, are committed to make the continent's digital transformation work, which in turn requires legal certainty. Third, the advancement of the African Continental Free Trade Area – economic and trade integration – and the broader globalization of African societies, reinforced the need for pan-African regulatory standards. The waning collectivism and the return to individualism in post-colonial and globalized African societies can be regarded as a further impetus for stricter privacy legislation, where the individual takes precedence.[34] Almost all African constitutions recognize the right to privacy as a human right.[35] Currently, the main obstacle to comprehensive data protection is not the absence of a legal framework, but rather the lack of coherence across jurisdictions and the challenges encountered in its implementation.[36] Some of these challenges are related to resource constraints by governments, which also impede the continent's data sovereignty; others emerge from a lack of independence of data protection agencies, and the absence of their separation from government.

Lastly, the regime type of the country under consideration needs to be factored in in the reflections. To start with, there is little structured data available and few studies investigating a correlation between regime types and data protection levels. This is clearly an area where more research will be needed in the years to come. In common parlance, the bottom-line assumption persists that the right to privacy is a liberal concept, and as such a correlation is drawn between robust privacy laws and (liberal) democratic governance, contrasting with a lack of stringent privacy regulations in autocratic regimes. Yet, this correlation, when juxtaposed with case-study findings, is weak and continues to dwindle as data protection legislation is further disseminated. China is a prime example of an authoritarian regime with a proclivity for strong data protection regulation.[37] Of course, such protection standards advance a different understanding of the relationship between the individual and the state, and the rights and duties of both, when compared to liberal democracies.

Surfshark, a cybersecurity company, publishes an annual Digital Quality of Life Index that measures data protection levels on a scale from 0 (no data protection) to 5 (GDPR-level data

[32] African Union Convention on Cyber Security and Personal Data Protection (also called Malabo Convention), adopted on June 27, 2014, entered into force on 8 June 2023, Article 8.
[33] Greenleaf and Cottier, "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis," 9.
[34] Yohannes Eneyew Ayalew, "Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law" *International Data Privacy Law* 12, no. 1 (2022); Makulilo, "A Person Is a Person through Other."
[35] Ayalew, "Untrodden Paths" 16-17.
[36] Bitange Ndemo and Aaron Thegeya, "A Prototype Data Governance Framework for Africa," in *Data Governance and Policy in Africa*, ed. Bitange Ndemo, et al. (Cham: Palgrave Macmillan 2023), 10.
[37] Mark Jia, "Authoritarian Privacy," *The University of Chicago Law Review* (Forthcoming). In his study, Jia contends that China, driven not only by the desire to build trust in its digital economy and attract data flows to enhance its global influence and national security but also by a bottom-up movement that emerged amidst an unregulated environment and major scandals, eventually resulted in the Party characterizing privacy invasions as a source of social instability (p.5).

protection). Comparing these data with regime types, researchers find that democracies average a data protection level of 3, while autocracies average 1.[38] In Africa, this correlation is weaker. Among the 24 African countries in the dataset, the average democracy scores 1.6, and the average autocracy scores 1.3 on the data protection index. Next to the overall lower level of data protection, the findings suggest that the regime type in Africa carries less weight when compared to other world regions. Some African nations with robust democratic systems have enacted comprehensive privacy laws to protect individuals' personal data. In these countries, privacy regulations may reflect the principles of democratic governance, including transparency, accountability, and respect for human rights. However, the situation is not uniform across the continent. Other African countries with democratic systems may have weak or inadequate privacy laws due to various factors such as limited resources, competing priorities, and above all challenges in implementation and enforcement. Conversely, certain autocratic regimes in Africa have strict privacy regulations, although these are primarily aimed at controlling information and suppressing dissent rather than safeguarding individual privacy rights.

The study is of exploratory nature, which implies that the results should be read with caution. The hybrid nature of political regimes across the continent is likely to have impacted the conclusion. Still, one possible explanation of smaller than expected margins between regime types is related to the fact that data protection and privacy regulation are motivated by a series of factors ranging from economic reasoning to geopolitical considerations. In the competition for global data flows, data protection creates the necessary trust for data exchange. It is from this perspective that both democratic and authoritarian states show interest in data protection and data governance, or, as de la Bruyère and colleagues put it, "in a digital environment, power is therefore a function of both capturing data and controlling the architecture of digital exchange".[39] Moreover, a turn to privacy law can allow governments in authoritarian regimes to offer an alternative avenue to legitimacy when electoral legitimacy is lacking.[40]

On Data Colonialism, Extraction and Sovereignty

Another pivotal aspect in the African context is the enduring power disparities, which constrain the region's capacity to play a more significant role in shaping global data governance standards. Consequently, African citizens often find themselves in a position of reinforced vulnerability, subject to the dominance of large data processors predominantly located beyond the continent's borders, relegating them to the status of passive data subjects.

In line with this structural deficit, critical and Marxist scholars coined the term "data colonialism" or "digital colonialism", which – according to their reading – combines "the predatory extractive practices of historical colonialism with the abstract quantification methods of computing" to eventually induce a new stage of capitalism for which the appropriation of human life through data will be central.[41] One does not need to embrace Marxist rhetoric to

[38] Agneska Sablovskaja and Kasparas Kajus Jucaitis, "Data Protection Levels in Democracies and Autocracies", *Surfshark,* 24 October 2023.
[39] Emily de La Bruyère, Doug Strub, and Jonathon Marek, eds., *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order* (Seattle: The National Bureau of Asian Research, 2022), 5.
[40] Jia, "Authoritarian Privacy," 42.
[41] Nick Couldry and Ulises A. Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject ," *Television & New Media* 20, no. 4 (2019): 317.

acknowledge that data has become a commodity. The appropriation of human life through data is facilitated by the economic needs of data subjects, which, the more vulnerable they are, the more likely they agree into forfeiting their data in exchange for immediate rewards. While privacy preferences are also attributed to cultural factors, the individual's economic circumstances and awareness of risks related to the sharing of personal data play a more significant role. According to Thatcher and Dalton, "there are real material advantages to the acts of participation that play out differently across different populations […] the very *choice* is only offered to those who have access to the advantages through other means".[42]

Data extraction, as a global phenomenon, assumes a distinct character and encounters comparatively less resistance when it infiltrates contexts lacking robust constitutional protections for personal data or where such protections have only recently been enacted. Activist-researchers from Pollicy have identified nine methods of digital extraction, which they contend perpetuate colonial legacies. These methods include (1) digital labour, (2) illicit financial flows, (3) data extraction, (4) natural resource mining, (5) infrastructure monopolies, (6) digital lending, (7) funding structures, (8) beta testing, and (9) platform governance.[43] In each of these domains the researchers detect forms of extractivism, which sees the "African market as an untapped source of data", leading to profit maximization outside the continent.[44] Although the argument is somewhat limited due to its linear and monocausal nature, it remains undeniable that all nine areas mentioned contain methods of extraction and are tangible realities within the African digital landscape.

The risks, widely present in various African countries, are compounded by the prevailing bias in global development and investment narratives. These narratives often present digital solutions in a predominantly positive light, particularly when addressing what is commonly known as the Global South. While cautious discourse on technology is often encountered in advanced economies, particularly in the EU, it is, if not replaced, at least overshadowed by a narrative of opportunity when applied to developing contexts.[45] Interestingly enough, this careless techno-optimist narrative is not yet accompanied by the investments one would expect, and which the continent would need. These two dynamics, when combined, pose a risk of marginalizing the most vulnerable participants in the market. To mitigate these consequences, it is essential to adopt a more nuanced perspective that acknowledges both the risks and opportunities of digital technologies. It is crucial to emphasize that this approach does not seek to negate the benefits of technology, nor does it stem from a desire to stifle innovation or promote a pessimistic view of technology. Instead, it represents a genuine effort to engage honestly with the empirical reality of digital Africa, which combines the need for economical and swift solutions with the imperative to provide protection within an environment where regulatory oversight and enforcement remain constrained.

To avoid abuses, the collection and processing of data needs to occur within the boundaries of regulatory standards in order to protect the individual and assure fair competition. In conjunction, with various forms of data use and extraction, the notion of data sovereignty is key. The term data sovereignty carries a multitude of different meanings. For some, data

[42] Jim E. Thatcher and Craig M. Dalton, *Data Power: Radical Geographies of Control and Resistance* (London: Pluto Press, 2022), 64. Emphasis in the original.
[43] For a more detailed discussion of each of the nine methods of digital extractivism see: Neema Iyer, Garnett Achieng Neema Iyer, Favour Borokini, Uri Ludger, *Automated Imperialism, Expanionist Dreams: Exploring Digital Extractivism in Africa* (Pollicy, 2021).
[44] Ibid., 6-7.
[45] Payal Arora, "The Bottom of the Data Pyramid: Big Data and the Global South," *International Journal of Communication* 10 (2016): 1682-83. Even in the US, and notably in California, the prototype of a techno-optimist society, caution towards new advances, especially in the realm of AI, has become an omnipresent factor in public discourse.

sovereignty is "reducible to more specific conditions and values", for others it describes an ability to obtain a specific result, and yet again for others it is a right.[46] At a very elementary level, data sovereignty "relates in some way to meaningful control, ownership, and other claims to data or data infrastructure".[47] The AU acknowledges the safeguarding of data sovereignty as one of its key priorities concerning Africa's digital agenda. Beneath the pursuit of sovereign recognition for the African data space lies a deeper aspiration: to evolve Africa into a vibrant ecosystem of digital innovators, rather than merely a hub for digital consumption.[48] One of the biggest challenges on the path to a data sovereign Africa are the related costs that occur when building the necessary infrastructure, such as data centres.

In sum, sustainable governance of the African data space needs to reduce the risks pertaining to data extraction while developing a foundation for a data sovereign continent. This requires the right balance between self-assertion and economic and technological integration. The regulatory dynamics evident across the continent indicate that governments and regulators recognize this reality and are actively working to address it.

Innovation Before Regulation?

Attitudes and practices of stakeholders towards data protection are also shaped by their respective desire to employ technological innovation for the purpose of economic development and job creation. Within the current discourse on African digital capacities and needs, various voices, particularly those emerging from the African tech community, raise concerns regarding excessively stringent regulation, particularly if it originates from a different context and may consequently overlook the intricacies of the African digital ecosystem. "Ideas", according to an African industry representative, that "may seem good in Europe may hinder the economic development in Africa".[49] "Regulators", as a former African government official put it, "need to allow innovators a certain degree of freedom to innovate".[50] This discourse has taken hold of both tech and government circles, especially concerning recent advancements and future developments of Artificial Intelligence (AI). As articulated by Kenya's ambassador to the EU, "regulation around AI needs to be slow" until we attain a comprehensive understanding of the technology under consideration.[51] On the opposite end of the spectrum, advocates for data protection and digital rights denounce the inadequate adoption and execution of data protection laws, particularly highlighting the inclusion of problematic exemptions evident across various jurisdictions. This phenomenon transcends regime types and is observable, for instance, in both Kenya and Uganda. In Kenya, the Data Protection Act of 2019 features several exemptions, while in Uganda, the Data Protection and Privacy Act of 2019 similarly grants exemptions, citing national security concerns.[52]

A similar debate is currently unfolding within the EU in the context of the EU Artificial Intelligence (AI) Act and its global implications. Critics of a rights-driven approach are not

[46] Patrik Hummel et al., "Data Sovereignty: A Review " *Big Data & Society* 8, no. 1 (2021): 6.
[47] Ibid., 12.
[48] Onica N. Makwakwa, Intervention at the State of the Union Conference, 2021, Fringe Event, "EU-African Digital Partnership in a Changing World", European University Institute, https://cadmus.eui.eu/handle/1814/71523, accessed 6 May 2021.
[49] Country director (East Africa), US Tech Company, stakeholder meeting, 11 June 2020.
[50] Liberian policymaker, stakeholder meeting, 28 May 2020.
[51] Ambassador Bitange Ndemo (panel discussion), "How will AI Shape International Development?". Event organized by Enabel, Estdev, Tony Blair Global Institute, 22 February 2024.
[52] Bridget Andere and Megan Kathure, *Strengthening Data Protection in Africa: Key Issues for Implementation* (*Access Now*, 2024).

singular to the African region, but also a constant in the European discourse, assuming "that stringent regulation hinders innovation and therefore explains why the EU has fallen behind the US and China in nurturing a thriving tech industry".[53] Another widely voiced concern with European data regulation and its export is "that it might be too blunt, with the risk of constraining value creation of all sorts of platforms that might fall under the gatekeeper status, doing little to promote competition, and in some cases producing unintended consequences that actively harm competition".[54] A core argument that these critics bring forward states that regulation generally "performs poorly in dynamic markets with rapid technological change".[55] The digital economy is such a market, especially in Africa.

Arguably, the key lies in striking a right balance between creating a regulatory environment that allows for cross-border flows of data, creates trust, predictability and legal certainty without overburdening market participants. Despite the internet's global reach, there is no one-size-fits-all regulation that can easily be applied around the world. Many stakeholders in the African tech discourse perceive significant benefits in digital regulatory sandboxes, which convene a wide array of relevant participants, including policymakers, regulators, entrepreneurs, academics, civil society members, and regional and international partners. These sandboxes facilitate dialogue aimed at formulating reliable regulations that address local needs effectively.[56]

From the outside, the stringently regulated European digital market can also be seen as highly protective. Due to high compliance costs, it is especially difficult or even impossible for small and micro-enterprises in Africa to penetrate the European market.[57] This is an important factor to consider, given that the promises of the digital sector are also based on its ability to dismantle such barriers owing to its intangible nature. Practices like the offshoring of digital labour or the processing of user data in third countries could then present economic opportunities for the African continent.

[53] Bradford, *Digital Empires,* 108, 36-39.
[54] Carmelo Cennamo and Daniel D. Sokol, "Can the EU Regulate Platforms without Stifling Innovation?," *Harvard Business Review* 1 March 2021 (2021).
[55] Ibid.
[56] Stakeholder meeting, 28 May 2020.
[57] Private sector specialist, World Bank, stakeholder meeting, 11 June 2020.

European Ambitions: The Power and Intent to Regulate

The EU – to paraphrase former Belgian Foreign Minister Mark Eyskens – often appears as a dwarf in the areas of digital innovation and AI investments.[58] Contrary to its initial aspiration, set out in the Lisbon strategy in 2000, to become "the most competitive and dynamic *knowledge-based* economy in the world by 2010", the EU continues to lag behind the US and China.[59] At the same time, it is arguably the one regime in the world that offers individuals the farthest reaching levels of data protection.[60] In response, the EU seeks, among other policy measures, to "put forward a new approach to digital transformation that projects European values onto the international stage".[61]

This new approach, according to the European Commission, will help establish a European model as a citizen-centred alternative to both the US-bred *surveillance capitalism* and Chinese *state-led digital surveillance*. By definition, this focus puts regulation first. In line with past experience, the EU hopes to achieve, qua regulation and emulation, what Bradford labelled the "Brussels effect", that is, the voluntary alignment with European standards and norms.[62] As part of this strategy, and given the intensified competition with global leaders, namely the US and China, other regions – especially the neighbourhood and growth-heavy Africa – move increasingly into the focus of the EU's efforts to shape the global digital order.[63] From an economic policy perspective, this focus on global competition is meaningful. At the same time, and in the context of developing discourses in and with Africa, the EU has been criticized for viewing the continent through the lens of global competition, reducing the region to a battleground rather than a source of innovation and a partner in the digital transformation.

The European Commission leaves no doubt that it seeks to shape the global digital order. In its Communication "Shaping Europe's Digital Future", the European Commission affirms that the "European model has proved to be an inspiration for many other partners around the world" and that "the EU should leverage its regulatory power, reinforced industrial and technological capabilities, diplomatic strengths and external financial instruments to advance the European approach and shape global interactions".[64] Accordingly, partnerships with other regions are deemed crucial and are partly viewed in instrumental terms:

[58] Mark Eyskens quoted in: Craig R. Whitney, "Gulf Fighting Shatters Europeans' Fragile Unity", *New York Times*, 25 January 1991.
[59] José-Luis Gómez-Barroso, Claudio Feijoo, and Edvin Karnitis, "The European Policy for the Development of an Information Society: The Right Path," *Journal of Common Market Studies* 46, no. 4 (2008): 791.
[60] Ibid.; Data-Pop Alliance and ADE, *Study for the Assessment of DEVCO Work in Digitalisation in Sub-Saharan Africa (Final Report June 2020)*, (Data-Pop Alliance, ADE, 2020), 3.
[61] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future, 2020, 14.
[62] Bradford, *The Brussels Effect*.
[63] European Commission, Roadmap Initiative: Communication on a [Sic] Europe's Digital Decade: 2030 Digital Targets, Ref. Ares(2021)1152850, 2021, 2.
[64] European Commission, Shaping Europe's Digital Future, 13.

> The EU needs to strengthen its capacity to **project its digital goals into its international cooperation** promoting its human-centric, rules-based approach. This requires the development of partnerships and alliances that can underpin European investment in infrastructure, capacity building and the enabling environment, as well as fostering regulatory cooperation notably with like-minded partners.[65]

Commission President Ursula von der Leyen put it even more bluntly at the beginning of her mandate, when saying, "We will jointly define standards for this new generation of technologies that will become the global norm".[66] This manifestation of political will is also attested in the more recent Commission proposal for an AI Regulation. The regulation, which was adopted in April 2024, stands to "support[] the objective of the Union being a global leader in the development of secure, trustworthy and ethical artificial intelligence".[67] The EU's involvement in Africa's digital transformation is propelled by the conviction that a human-centric approach represents a superior method. Simultaneously, it is also motivated by the notion that the EU can propagate its values through standardization, aiming to establish a level playing field and predictable regulations for the conduct of business with African partners.[68] At the operational level, the dialogue sometimes takes on a distinct tone. EU officials assert that their foremost objective is not the imposition of their regulatory framework but rather the exchange of expertise and the acknowledgment of shared adequacy standards. Their aim is to facilitate a seamless data exchange by recognizing similar, if not identical, standards, thereby fostering a climate conducive to free data flow.[69]

The notion of European leadership and technological sovereignty emerges as the most prominent trope in the EU's digitalization discourse. With the advances of AI, both the need for new regulation and the rivalries that accompany this regulatory moment have further increased. Currently, the regulatory rivalries surrounding AI mainly unfold between the EU, China and the US, yet their implications are to be felt globally.[70]

The combination of regulatory appetite, skills and capacities and the world's largest common market transform the EU in a global regulator. The EU's influence on third party legislation occurs on two different levels. On the one hand, there is the extraterritorial reach of the GDPR. On the other hand, there is active promotion of its standards through technical assistance and other support measures that the Union willingly offers to third party countries. Both facets of externalization are united in the fact that they stem directly from EU domestic policymaking and are harmonized with decisions formulated for the common market. As one Commission official insisted, "there is total alignment of internal and external policies and priorities".[71]

Extraterritorial Application of European Regulation

As stipulated in the General Data Protection Regulation (GDPR), the regulation covers all "processing of personal data of data subjects who are in the Union by a controller or

[65] European Commission, Roadmap Initiative, 2.
[66] Mark Scott, "What's Driving Europe's New Aggressive Stance on Tech," *Politico,* 2019.
[67] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artifical Intelligence Act) and Amending Certain Union Legislative Acts, Com(2021) 206 Final, 2021, 1.
[68] Interview, DG Connect, 8 February 2021.
[69] Interview, European Commission DG JUST, 24 March 2021. See also: European Parliament, Corrigendum of the Regulation (EU) 2024/… of the European Parliament and of the Council of … laying down harmonized rules on artificial intelligence, P9_TA(2024)0138, CO_TA, europa.eu.
[70] European Parliamentary Research Service, Briefing: Artifical Intelligence Act, PE 698.792, June, 2023.
[71] Interview, European Commission, 17 December 2020.

processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services […]. to such data subjects in the Union; or (b) the monitoring of their behaviour […] within the Union."[72] With this, the EU enacted a radical shift in how to view general data protection. With the adoption of the GDPR, the application of EU law shifted "the primary focus from the geographical location of the processing to the place where the effects of the processing are felt".[73] It is worth noting that the extraterritorial extension of the EU's regulatory reach is based on territoriality. It requires a "terri-national" affiliation of those being monitored for EU law to be applicable.[74] Due to the territorial limits of enforcement jurisdiction, the GDPR's reach depends on cooperation with third party regulators as much as it depends on third parties' desire to engage in trustworthy relationships with the EU.[75] In other words, the desire to partner with the EU, mainly incentivized by the large European consumer base, makes EU law such a powerful tool at the global level.[76] Beyond voluntary cooperation, the EU approaches the limited enforceability of EU law abroad by adding additional safeguarding measures, which take effect ex-ante, such as requirements to store data within the EU, to designate a data representative in the EU, or the above-mentioned adequacy clause. From this perspective, alignment by third parties can be described as quasi-voluntary behaviour in response to legal conditionalities, with economic consequences imposed by the world's largest common market. Through the Brussels effect, that is the unilateral exercise of its jurisdiction abroad, the EU has affected global corporations and international legislation.

Helping Others to Adapt

The Commission sees a "strong digital presence in the EU's enlargement, neighbourhood and development policy"[77] as a prerequisite to and enabler of the achievement of the SDGs. Through its digital development agenda, the EU seeks to capacitate developing states to develop both the digital infrastructure and regulatory environment that allow for economic growth and help strengthen human rights and democratic values. Digital development cooperation, according to Okano-Heijmanns and Vosse, by far exceeds grants and loans in the ICT sector and "includes assistance with the design and implementation of infrastructural broadband projects, as well as capacity building with the aim of governance of the digital domain that reflect norms and values of a free and open internet".[78]

To achieve what is often termed "Africa's digital transformation", the Commission emphasizes the role of the EU-African Union Digital Economy Task Force and pushes for the creation of a single African Digital Market.[79] On the one hand, exporting the idea of a digital single market is guided by the expected economic benefits of a harmonized market, which is both competitive and innovative. On the other hand, in so doing, the EU also exports parts of its own DNA. When stating that the EU "stands ready to share its experience in

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), art. 3, 2.
[73] Benjamin Greze, "The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives," *International Data Privacy Law* 9, no. 2 (2019): 110.
[74] Cedric Ryngaert and Mistale Taylor, "The GDPR as Global Data Protection Regulation?," *AJIL Unbound* 114 (2020): 6.
[75] Greze, "The Extra-Territorial Enforcement of the GDPR".
[76] Chad Damro, "Market Power Europe," *Journal of European Public Policy* 19, no. 5 (2012).
[77] European Commission, Shaping Europe's Digital Future, 13.
[78] Maaike Okano-Heijmans and Wilhelm Vosse, "Promoting Open and Inclusive Connectivity: The Case for Digital Development Cooperationv," *Research in Globalization* 3 (2021): 2.
[79] European Commission, Shaping Europe's Digital Future, 13.

integrating previously fragmented markets", it externalizes the centre piece of its domestic integration project – the common market – and as such contributes to a further promotion of the European model at the global stage.[80] It is in this context that the DETF also recommends strong links between a future African digital single market and the European digital single market – a relationship that shall be governed by the principles of the GDPR.[81]

Technical assistance and support in skills developments constitute two of the central tools the EU offers to partner countries willing to reform their domestic systems in line with the EU's global aspirations. With the introduction of the Digital for Development Framework in 2017, the EU began to "mainstream digitalisation in EU interventions for sustainable development and economic growth" globally and especially in Africa.[82]

This support can occur either as part of a multilateral effort, as was the case when the European Union lent support to ITU and African governments in establishing the Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA) Framework, or bilaterally, when advising African governments in setting up their national data regulation frameworks. A lot of this work also happens on the basis of experience sharing.[83] According to the Commission,

> cooperation between developing countries and the EU in the area of digitalisation can lead to a "win-win" situation. "Made-in-Europe" solutions can help address the needs of developing countries and in parallel **promote EU policies and standards**, as well as 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, based on co-development and co-innovation.[84]

The Commission aims to foster a proactive industrial policy by assisting others in adopting standards akin to those in the EU. This approach is anticipated to yield mutual benefits for the economies of partner countries as well as for the EU itself. In this regard, the EU incorporates aspects of both the Chinese and the US approaches to global digital governance. By leveraging strong state intervention, the aim is to unleash competitive market forces that drive growth.

While the desire to influence the global digital order according to its own standards, that is, centring on individual privacy, regulatory oversight, and firm checks and balances, is a prevalent theme in Brussels, the strategic planning does not currently encompass Africa to its fullest extent. Projects and investments are primarily evaluated on a case-by-case basis rather than through a coordinated regional and long-term approach.[85] Consequently, the EU is not yet prepared or inclined to pursue a more confrontational stance in regions where competitors, namely China and the US, hold sway. For example, in Uganda, the EU exercises caution when engaging with the public sector, which has shown a propensity to adopt Chinese surveillance technology. Instead of presenting a counter-offer, the EU opts to engage with the private sector.[86]

These dynamics unfold against the ongoing trend that causes EU development cooperation to increasingly distance itself from its original mandate – poverty alleviation – towards a more interest-driven and strategic approach. As the SDGs gradually recede from the forefront of EU public discourse and action, doubts arise regarding the frequently touted notion

[80] Digital Economy Task Force (DETF), *New Africa-Europe Digital Economy Partnership: Accelerating the Achievement of the Sutsainable Development Goals* (DETF, 2019), 12.
[81] Ibid., 17.
[82] European Commission, Commission Staff Working Document: Digital4development - Mainstreaming Digital Technologies and Services into EU Development Policy Swd(2017) 157 Final, (2017).
[83] Interview, European External Action Service, 22 January 2021.
[84] European Commission, Mainstreaming Digital Technologies and Services into EUDevelopment Policy, 15.
[85] Interview, European Commission, 21 January 2021.
[86] Ibid.

of a mutually beneficial partnership. The efficacy of the European model still needs to withstand the test of practice, necessitating a tangible demonstration of whether the model is actual superior or the most apt solution from the perspective of partner countries. It must substantiate its value proposition through practical implementation, proving why it stands as the preferred choice among many alternatives.

The African Data Space and the EU

Against the backdrop of an increasingly data-conscious Africa, global competition, and an EU that seeks to further disseminate its own model of global data governance, the EU–Africa digital partnership unfolds. Soon after its adoption in 2016, the wide-ranging GDPR emerged as a global data privacy standard as it was gradually adopted by all leading American and European tech companies.[87] The rest of the world followed suit, with more and more countries aligning with European standards in line with respective policy goals and capacities, with Africa being no exception.[88] The collaborative and adaptable nature of EU regulation, coupled with its availability in over 20 languages, facilitates adoption and implementation in various contexts through simple copy-paste operations.[89] The cost of this exercise lies in the risk of generating misplaced regulation that could ultimately harm the end-user.

The implementation of the EU's GDPR has not only spurred the harmonization of current laws but has also catalyzed the introduction of new data protection regulations in Africa. Many of these regulations either bear strong resemblance to the GDPR or share close alignment with its principles. The EU's influence on African data protection is evident across multiple fronts. For instance, there is a notable qualitative transformation in African data protection laws when comparing the periods before and after the adoption of the GDPR, as highlighted by Daigle.[90] He observes a trend toward more stringent data protection regulations across the African continent after the adoption of the EU GDPR in 2016. It is important to highlight that the observed norm externalization both pre-dates and surpasses the GDPR's scope. Notably, the 1981 Council of Europe Convention (Convention 108, later updated to 108+ in alignment with the GDPR) on data protection had a significant influence on several African states. When the Convention's Consultative Committee and the Council of Europe decided to globalize the Convention, African countries were among the earliest adopters of the framework. Cabo Verde, Mauritius, Morocco, Senegal, and Tunisia even joined the said regional framework.[91] Greenleaf and Cottier note that the AU Convention, in particular, does not display any Africa-specific approach to data protection but, rather, mirrors European instruments to a point that similarities even pertain to areas that go beyond OECD privacy guidelines, which could be considered as the global minimum standard.[92] One explanation that is put forward to explain why the AU and the majority of its member states tend to replicate European norms rather than develop a distinctly African data privacy framework, relates to the underlying economic rationale driving African actors' engagement with data protection. Given the overarching goal of bolstering commerce and attracting European business ventures, adopting the regulatory framework of the European region appears logical, as it aligns with efforts to cultivate economic relationships.[93]

[87] Bradford, *Digital Empires,* 324.
[88] Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal* 106, no. 1 (2017).
[89] Bradford, *Digital Empires,* 332.
[90] Daigle, "Data Protection Laws in Africa."
[91] Greenleaf and Cottier, "International and Regional Commitments in African Data Privacy Laws," 11.
[92] Ibid., 33.
[93] Abdulrauf, "Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms " 99-100.

However, alignment with European standards is not necessarily an indicator for the success or effectiveness of norm externalization. Survey data from six African countries (Ethiopia, Ghana, Kenya, Nigeria, Senegal, and Tanzania) reveal that public perception generally views the EU as lagging behind China in terms of its role and impact on ICT development. When asked about areas of cooperation where the EU or China play a very important role, respondents in all six countries rated China's involvement in the ICT sector higher than that of the EU. Even in Ghana, where 20% of respondents consider the EU a particularly influential partner, 27% believe the same about China. In Kenya, 16% believe in the EU's influence whereas 22% see China as a particularly influential partner. The difference is most pronounced in Nigeria, where only 16% view the EU as influential, compared to 34% who attribute this influence to China. As we will see below, these results are largely unrelated to the EU's formal role and impact on the development of data protection frameworks in these countries. In the case of China, there is a strong positive correlation between its overall perception as an important and influential partner and its role as a key partner in ICT development. This correlation is much weaker for the EU, suggesting that the EU's footprint in the digital sector is generally less pronounced than that of China.[94] While the European data protection regime is considered as a global standard, African actors do not necessarily equate it with influence of the EU over their domestic regime.

Finally, adopting EU standards also stems from the aspiration to meet the *adequacy* requirements of the EU, and in so doing avoid the exclusion from a dominant market.[95] This runs the opposite risk of igniting the accusation of Europe exerting some form of data imperialism. Whilst the coercive nature of the EU's market power is manageable across industrialized nations, "for emerging countries, the cost and administrative burden of applying the EU privacy standards can be daunting" and risk being viewed as a practice derived from and reinforcing colonial asymmetries.[96]

When Nigeria and Kenya, Africa's second and seventh largest economies respectively, adopted their national data privacy legislation in 2019, they emulated the GDPR. The scope of the Nigerian regulation, for instance, was nearly the same as that for the GDPR. At the same time, it had limitations such as the absence of extraterritorial processing or processing data of foreign non-residents of Nigeria. Moreover, the Nigerian Information Technology Development Agency was not an independent data protection authority but a government agency. Taken together, this made an adequacy decision on the part of the EU rather unlikely.[97] Following pressure, among others from ECOWAS, Nigeria adopted the Nigeria Data Protection Act in 2023 and instituted an independent data protection authority.[98] In that sense, the developments observed in Nigeria are a prime example of institutional learning and conversion. Nonetheless, public perception consistently ranks the EU's influence in the ICT sector below that of China.[99]

[94] German Institute of Development and Sustainability (IDOS), Original survey data collected in Ethiopia, Ghana, Kenya, Nigeria, Senegal, and Tanzania (2024).
[95] Ayalew, "Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law " 18. For more on the adequacy requirement, see: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 25; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance), art. 45.
[96] Mark Scott and Laurens Cerulus, "Europe's New Data Protection Rules Export Privacy Standards Worldwide" *Politico*, 31 January 2018.
[97] Graham Greenleaf, "Nigeria Regulates Data Privacy: African and Global Signficance" *Privacy Laws & Business International Report* 158, no. 23 (2019).
[98] Nigeria Data Protection Act (2023), https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf.
[99] German Institute of Development and Sustainability (IDOS), Original survey data.

The Kenyan Data Protection Act acts as a general data protection law, which takes inspiration from the EU's GDPR and serves as stand-alone comprehensive law governing data protection and privacy. The law regulates the handling of data by the government and both national and international corporations. Since the adoption of the law in November 2019, the EU and its member states, notably Germany, have continued to support Kenyan efforts in the realm of data protection by providing financial and technical expertise to the newly established Office of the Data Protection Commissioner. The Commissioner, which started from scratch, setting up both staff and offices, offers a unique opportunity for the EU to co-constitute Kenyan privacy narratives and contribute to the promotion of European norms. This exercise, however, has brought challenges, ranging from technical difficulties to active resistance on the part of government or other stakeholders. In the concrete case of the Kenyan Data Protection Commissioner, an overly strong EU involvement would put into question the very legitimacy of the office, which is rooted in absolute independence.

Alongside countries that have developed data protection regulations in accordance with the GDPR, there are others that had pre-existing data protection regimes that pre-dated the GDPR and do not, therefore, conform to it. When comparing the evolution of data privacy and data protection regulation in the EU and South Africa, Michael Gastrow and Rachel Adams identify "both areas of alignment and misalignment".[100] The drafting of South Africa's Protection for Personal Information Act (POPIA) debuted in 2003 and was based on the 1994 EU data protection regulation. It took another 17 years before the act finally came into effect in 2020. In the meantime, the EU had moved on and adopted the GDPR. Despite numerous similarities, the fact that POPIA is based on a predecessor of GDPR and does not match the "stronger focus on data flows of personal information", makes it unlikely that South Africa will be granted adequacy by the European Commission. Unless data protection regulation is "rapid and responsive", it risks falling behind the standards set by the dominant regulator. This reading is also based on the observation of persisting colonial asymmetries between the two data spaces.[101]

Two observations can be made here, which, in combination, amount to a dilemma. First, formal influence over rule-making does not equate to perceived influence. The EU may actively promote a human-centric, privacy-based regulatory framework and still not be seen as one of the most influential external actors in a country's ICT development. Second, if the EU is perceived as an influential power, its rigid regulatory system risks evoking negative connotations, such as the impression that it stifles the development of emerging countries.

[100] Michael Gastrow and Rachel Adams, "Digitalisation in Science and Technology Policy: Engagement, Alignment, and Misalignment between the European Union and South African Data Protection and Privacy Frameworks," in *Africa-Europe Cooperation and Digital Transformation* ed. Chux Daniels, Benedikt Erforth, and Chloé Teevan (London: Routledge 2022), 161.
[101] Ibid., 163-64.

Emergence of an African–European Partnership in Data Governance? Conclusions and Future Research Agenda

The paper has described a highly dynamic African data space, with increasing and continent-wide uptake of more stringent regulatory frameworks. In this context, the prospect of establishing an African–European data partnership holds considerable promise, presenting opportunities for collaboration and mutual benefit. The mutual recognition that Africa and Europe, each to varying extents and across diverse domains, are trailing in the global race for digital supremacy could serve as a unifying factor between these regions. Proximity in other policy fields may reinforce this trend,[102] which benefits from the proactive pursuit of engagement between the two regions by African partners in recent years. For some countries, such as Ghana, Kenya, and Nigeria, the EU has become the reference point in their efforts to reform, modernize and adapt their domestic data protection regulation.[103] This is particularly noteworthy, given that cooperation in other areas pertaining to fundamental rights, such as the rule of law and democracy, is witnessing regressive tendencies. The reason for this, of course, lies in the economic promise that looms behind a frictionless flow of data.

EU engagement for a more regulated and standardized African data space can be beneficial for data subjects. The intent of embedding African data extraction and processing in firmer and more restrictive frameworks can serve individuals' privacy rights and shelter them from additional layers of exclusion. In the medium- to long-term it can also provide for more attractive environments for investors. If the EU supports African states in their endeavour to establish a more protective and competitive data environment, this can be considered a positive outcome in the partnership. However, this potential faces numerous obstacles that may impede its realization.

Firstly, the EU's involvement in digital cooperation still appears modest, particularly in contrast to China's extensive infrastructure initiatives over the past decade. This emerging domain of collaboration is intricately linked to the broader vitality of the Africa–Europe partnership. While it presents an opportunity for non-politicized engagement, its success hinges on the foundational health of the overall relationship. The EU's regulatory power holds significant potential for reshaping global regulatory frameworks and markets. Yet, this power is contingent upon partners possessing robust industrial foundations and substantial trade and investment ties with the EU common market. Moreover, the conditionality underpinning the EU's regulatory influence and a rather static and strict interpretation of data protection and privacy may not align well with emerging markets and developing economies still seeking a competitive edge. It may even be perceived as a paternalistic or

[102] Interview, African Union, 27 January 2021.
[103] Interview, European Commission DG JUST, 24 March 2021.

neo-colonial approach to data extraction.[104] Consequently, in the absence of expansive digital infrastructure initiatives, the primary focus of engagement should revolve around knowledge exchange, skill enhancement, and technical expertise development.

Secondly, it remains uncertain whether the offered solutions align with existing demands. African tech entrepreneurs, innovators, and even policymakers may not necessarily turn to the EU when charting their technological trajectories and innovation paths. Despite the GDPR's significant dissemination effect, the EU's emphasis on regulatory rigour, in particular, is not always embraced, and is sometimes viewed as a hindrance to economic development.

Aspirations for national data sovereignty cannot be ignored. Whilst EU support qua a human-centric approach may improve the sovereignty of individuals it may equally be perceived as an act of interference in the national data space. As interlocutors both from the private and public sector have voiced regularly, African stakeholders seek solutions that are adapted to their local contexts.[105] A European blue-print might then not only be ill-fitting, but also be perceived as an additional barrier that the EU imposes in order to hinder the more dynamic and less institutionalized digital development on the African continent.

Thirdly, while the benefits of a unified digital single market are emphasized by both African and European policymakers, it is crucial not to overlook the disparities between the two regions (as well as within them). Despite the often-claimed notion of equal partnership, the reality remains largely one-sided. This also evokes a conundrum. The mantra of equal partnership makes international partners, and as such the EU, focus on advanced tech environments around a handful of African capitals. This is where a partnership between equals can be realized, where economic opportunities are looming and geopolitical interests are located. At the same time, the EU is committed to, and is called upon to assure that, marginalized groups in particular are not further disenfranchised. Catering to both dimensions, when it comes to digital cooperation, still remains somewhat elusive.

Alignment between the two regions should not be considered as an automatism. It is also unlikely to unfold across the entire continent to the same extent. A more likely scenario involves consortia of like-minded states that work together on an ad-hoc basis or within selected issue areas.

The African data space is experiencing a noticeable surge, emphasizing the critical need for implementing recently adopted regulations. The EU possesses valuable technical expertise that can support this process during both legislative development and implementation phases. However, it is imperative for the EU to steer clear of adopting an overly paternalistic stance, which could potentially entail imposing conditionalities tied to its market size. Instead, a discourse emphasizing the global significance of data sovereignty is to be preferred. This said, the notion of sovereignty in digital governance is also at the heart of the Chinese state-driven model and exported as part of the country's digital offer. To maintain a balance between the right to sovereignty and preventing the undermining of multistakeholder institutions, the EU should provide additional support to regional organization, notably the AU, and its efforts to establish an African digital single market. In this regard, the EU can play a particularly constructive role by sharing the expertise it has gathered while establishing its own digital single market.

Regulation and expertise alone will not suffice to create more equitable data environments and associated economic opportunities. The need for reliable and accessible infrastructure and private investments remains. For the EU, this implies not only being

[104] Cara Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets," *Vanderbilt Journal of Transnational Law* 53, no. 2 (2020).
[105] Megatrends Afrika and ACET Policy Workshop, Digitalization in Ghana, 19 April 2023.

associated with the regulatory side of the African data space but also becoming a reliable and visible partner on those other dimensions, providing hands-on solutions to some of the continent's most pressing problems.

Lastly, research can accompany this policy momentum across several fronts. Firstly, there is a pressing need for deeper exploration of local demands, and their alignment with the diverse offerings in the global digital market. Complementing this demand-side analysis is a heightened emphasis on partner perceptions. Understanding both the perceived and actual impact of EU policy actions is crucial. Additionally, there is a call for studies to enhance understanding of African agency in the data space, for example, examining it from institutional perspectives and investigating the relationship between regime types and data protection regulations. Furthermore, existing research on the needs of innovators, particularly SMEs, should be expanded and supported to foster growth within their respective ecosystems.[106] Finally, it is essential to broaden focus beyond economic growth to consider the social implications of the data revolution, including issues such as equitable access and ethical data extraction practices.

[106] Freda Yawson and Tahis Mahmoud, „Innovation Meets Growth? Navigating the Digital Landscape in Ghana", *Megatrends Working Paper* 11, (2024).

Megatrends Afrika is a joint project of SWP, IDOS and IfW.
The views expressed in this publication are those of the author(s).
All project publications are subject to an internal peer review process.

SWP Stiftung Wissenschaft und Politik | German Institute for International and Security Affairs
IDOS German Institute for Development and Sustainability
IfW Kiel Institute for the World Economy

www.megatrends-afrika.de
megatrends-afrika@swp-berlin.org

ISSN 2747-4275
DOI 10.18449/2024MTA-WP14

Stiftung Wissenschaft und Politik
German Institute for
International and Security Affairs

German Institute
of Development
and Sustainability

KIEL INSTITUTE FOR
THE WORLD ECONOMY

Funded by:

Federal Foreign Office

Federal Ministry
of Defence

Federal Ministry
for Economic Cooperation
and Development