Chapter 3 – Integrating digital sovereignty in EU external action by Chloe Teevan and Ennatu Domingo

1. Introduction

The EU increasingly refers to digital sovereignty both domestically and internationally, and yet there is still quite a lot of ambiguity about precisely what this term means to European stakeholders, and indeed whether they share the same vision. The European approach is multifaceted and encompasses a wide range of regulatory measures, coupled with a growing focus on industrial policy. There is a strong focus on individual rights, while at the same time, there is a growing focus on supporting European businesses. The concept is also increasingly evoked in EU foreign and security policy, as well as in the EU's wider international partnerships, but it is not entirely clear how this approach carries over to EU external action. The EU remains somewhat vague about defining this term when using it at multilateral fora or in its relations with other countries.

This chapter looks at how the EU might develop a new approach to digital sovereignty at the international level, working more closely with others in a collaborative and open-minded way. The EU would need to better demonstrate how its policies back up its promise of supporting digital sovereignty in partner countries, and ensure that its domestic policies are consistent with its international rhetoric around developing more respectful and mutually beneficial international partnerships. At present, there is a great deal of geopolitical competition around investments and international partnerships with developing countries in the Global South. If the EU is seen to be preaching and trying to externalise its vision and regulations, this may ultimately be counterproductive and may give rise to accusations of neocolonial practices. This means that the EU should work with others to come up with a shared basic understanding of this term. This chapter aims to lay out some of the ways that the EU might approach this exercise.

This chapter draws on interviews and ongoing conversations with policymakers, academics and analysts, mainly in Europe, Africa and India. It also draws on a range of EU and partner country policy documents, academic literature and the work of other policy researchers. In the first section, it looks at different approaches to defining digital sovereignty within the EU. It then moves on to look at how the EU might better integrate the concept of digital sovereignty into its external actions, identifying some key dimensions of a new approach. In the third section, it looks at how the EU can work more closely with partner countries, particularly in the Global South to come up with common approaches to digital sovereignty, and in the final section, it summarises some of the arguments contained in the paper and some of the recommendations that these arguments lead to.

2. Defining Digital Sovereignty

As previously mentioned, although the term is widely used, the term digital sovereignty is rarely defined in most EU policy documents. However, in the European Council Conclusions of October 2020, the following quite broad goals were laid out to make the EU digitally sovereign: "To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure." This development should follow a human-centric approach that would "safeguard our values, fundamental rights and security, and be socially balanced" (EUCO 2020). To pave the way for its digital sovereignty, the EU outlined its strategy in the Digital Compass, a ten-year roadmap for Europe's digital transformation. It aims to both build on Europe's strengths, including its single market, its values and its educated workforce, while also addressing “any strategic weaknesses, vulnerabilities and high-risk dependencies.” (EC 2021a).

Yet as a number of analysts have previously pointed out, there appear to be a number of divisions between EU policymakers with regard to the essential element of digital sovereignty, and there are a number of tensions in the ways that different policymakers define the term. Pons points to a tension between the French and German approaches: ‘France defines digital sovereignty in terms of infrastructure, while the Germans prefer to talk about data sovereignty (Datenhoheit). For Germany, sovereignty is a barrier to the export of its goods, whereas France thinks it is a protective barrier for its values.’ (Pons 2023) Others have also pointed to the tension between a definition that focuses on individual sovereignty versus collective sovereignty in the EU approach (Bauer 2020). Indeed, for certain theorists, the EU should not attempt to construct European giants through a reinforced state role, but should rather invest in creating a democratic policy on digital sovereignty by ending the monopoly power of big tech through reinforcement of competition policy (Rimbaud 2021).

Yet, as discussed elsewhere in this report, the EU is taking a two-prong approach to digital sovereignty, which has accelerated since the beginning of the von der Leyen Commission in 2019. On the one hand, it is looking to increase the robustness of its regulatory toolkit through the adoption of a host of new policies and laws with the aim of creating a more democratic and competitive digital environment. On the other hand, it has begun to gradually embrace an active digital industrial policy, hoping to stimulate the development of European digital champions through more investments in the digital sector (See chapters by Musoni and Karkare in this report). At the heart of the EU’s regulatory approach is what it refers to as its human-centric vision of digital governance. Commission Executive Vice President Vestager, when launching the European Declaration on Digital Rights and Principles for the Digital Decade, highlighted that the Declaration would be the cornerstone of the EU’s human-centred digital policy: ‘We believe in a human-centred digital transformation. A transformation where no one is left behind. We want safe technologies that work for people, and of course that our rights and values are as well respected online as they are offline. And we want everyone to be empowered that we as citizens feel that it is our society, that we feel empowered to actively to take part.’ (Vestager 2022).

3. Key dimensions of a new approach

The EU Commission started using the term ‘digital sovereignty’ in its external action as early as 2016, in the EU’s ‘Global Strategy for Foreign and Security Policy,’ linking it to its concept of ‘strategic autonomy.’ (EEAS 2016). The July 2022 Council Conclusions on Digital Diplomacy highlight the importance of a more robust digital diplomacy to support the EU’s “ambitious quest to strengthen its technological and digital sovereignty.” (CoEU 2022) These efforts have been most apparent in the EU’s recent efforts to proactively influence global standards through stepped up diplomacy at multilateral fora, and by leveraging its position as one of the world's largest markets with the ‘Brussels Effect’ - its capacity to shape or align regulatory environments outside of the EU to its domestic policies and regulations, initially via market mechanisms (see Musoni in this report). Meanwhile, the Global Gateway Strategy, with its focus on sustainable and trusted connections with the rest of the world, does not explicitly mention digital sovereignty, but makes clear that it hopes to provide partner countries with “secure and trustworthy digital infrastructures and technologies underpinned by proper regulation,” thereby echoing some of the elements at the heart of the European approach to digital sovereignty (EC 2021b).

Yet beyond these specific external-facing measures, the EU also needs to begin to demonstrate that there is consistency between the concept of digital sovereignty in its internal and external policies in line with the aims of the so-called “Geopolitical Commission” (Teevan and Sheriff 2019, Teevan 2019). It will also need to show an openness to compromising with partners across the world, working with them to come up with common approaches to key concepts that are central to the European approach, including developing an inclusive approach to "human-centric" digital transformation. Further, the EU will need to demonstrate how its approach to data governance and to digital governance more broadly can be meaningful to others, and again show an openness to new approaches and to compromise.

3.1. Consistency between internal and external policies

An essential element will involve developing greater consistency between internal and external policies. Thus, the approach to digital sovereignty in external action would need to both; 1) integrate an understanding of the external dimension into laws and regulations that aim to strengthen Europe's domestic digital sovereignty; and 2) take into account the indirect impacts or implications of EU domestic policies for partner countries. The external dimension should be considered in all new domestic digital and industrial policies, including both how to mitigate harms and to extend benefits (for example, Digital Services Act, Digital Markets Act, AI Act, Cybersecurity Act, EU Chip Act, etc.).

In external action, the EU is currently strongly focused on creating digital norms and standards as one of the key elements of its digital sovereignty model (Burwell and Propp 2022), and yet the external dimension of new policies is not always sufficiently considered in the texts of new policies and laws. The EU is keen to promote the so-called "Brussels effect" through its digital diplomacy and international cooperation. For example, the EU hopes that the recently adopted Digital Markets Act (DMA) and the Digital Services Act (DSA) will increase the influence of the internal market and its regulatory power internationally (Broeders et al. 2023). Yet, the positive external impact of these new laws is assumed rather than studied in-depth. For example, in the impact assessment for the Digital Services Act, a short section on "Trade, third countries and international relations" briefly discusses the obligations that the Act would place on third country service providers, whether the proposals are in line with international obligations and includes one paragraph on the potential impact on relations with third countries. However, while it hints at the potential for this Act to put the EU in a leadership role, it does not really consider how this might be achieved and the wider potential impact for third countries, including notably in the Global South (EC 2020a).

There is a need to integrate the external dimension into all domestic strategies and to carry out real impact assessments with regard to the impact of domestic regulations externally. While it is understandable that the EU is eager to move quickly with new regulations designed to protect its citizens and to improve the competitiveness of its single market, a greater consideration of the external impact of new regulations would demonstrate a less unilateral approach. Taking into consideration potential impacts on partner countries amongst the least developed and lower-middle income countries would be particularly important in order to ensure coherence with EU development policy goals.

At the same time, the EU should pay attention to the indirect impacts of domestic policies, notably around industrial policy, and not ignore the potentially negative impacts. The EU's rhetoric vis-a-vis partners in the global south largely ignores the ongoing technology race - and consequent subsidy race - taking place between established powers that may leave the global south even further behind (See Karkare 2023 in this report).

The EU should thus clearly lay out ideas about how its growing focus on domestic industrial policy can also integrate partner countries' interests and ambitions. The EU should try to integrate partner countries into new initiatives in a positive way in line with their national development ambitions, including potentially integrating them into European value chains, thereby showing the real benefit of partnering with the EU. There are hints of this in certain policies, such as the recently published Critical Raw Materials Act (EC 2023a) that aims to support partners "to promote their own economic development in a sustainable manner through value chain creation in their own countries" alongside the aim of creating diversified value chains for the EU. Another interesting example is EU support to the AU’s Data Policy Framework, with its aim of creating an African data market. Yet, there is room to be more deliberate about this.

In order to ensure follow-up on these policies, the Global Gateway should gradually develop a stronger focus on industrialisation, supporting local technology hubs and funding research and innovation partnerships (the vaccine manufacturing hubs are a good example in another sector). New EU policies should be supported by realistic projects under the Global Gateway, such as the aforementioned investments in critical raw materials processing hubs under the EU’s Critical Raw Materials Act. It will also be important that the Global Gateway is not limited to supporting the externalisation of EU industries, but that it plays a role in supporting the development of local industries through research and innovation partnerships, integrating local players into value chains, and allowing for a certain amount of technology transfer. This might include further efforts to support joint research and to stimulate innovation partnerships between businesses in Europe and the Global South. This might include reinforcing Horizon Europe’s external dimension and extending the Digital Europe programme beyond Europe’s borders, and potentially integrating a wider number of countries into some of its initiatives.

3.2. A common understanding of ‘human-centric’ digital transformation

As mentioned above, the EU aims to promote its vision of digital sovereignty based on what it calls ‘human-centric’ digital governance, and it has increasingly been referring to this in various policies on digital for development and at multilateral fora. Although this term is widely used by a number of different international actors, it remains very unclear as different actors understand and see that they can promote it in different ways such as through digital governance and data protection or through increasing investment in digital infrastructure. The EU has started to increase its engagement on the human-centric approach to digital governance, including via the appointment of a Digital Affairs Officer at the EU Delegation to the UN in Geneva, by bringing up the concept at multilateral fora such as the ITU and by calling for stronger partnerships for more inclusive, secure and sustainable digital transformation and opening a new EU office in San Francisco to strengthen digital cooperation with the US (Teevan and Domingo 2022: EEAS 2022).

The EU can lead discussions to develop a common understanding of the concept rather than imposing its own term after it has found a common and clear European view and clarified how it will operationalise the concept (CONCORD 2023). There are already good examples of how the EU is building digital partnerships based on similarities around this concept, as it seeks partners to create and shape global standards on internet governance. For example, in 2020, during the EU-India Summit, which gave the EU-India partnership a more strategic dimension, the EU and India agreed to ‘harness human-centric digitalisation to develop inclusive economies and societies’, marking the first time that the terms were used to refer to their ambition to enhance convergence between their respective regulatory frameworks to ensure the protection of personal data and privacy (EC 2020b).

Given that there are multiple digital governance models, the EU’s concept of ‘human-centric’ digital transformation is a distinctive mark that is used to help the bloc to differentiate itself from alternative offers. However, the EU should embed its human-centric approach to technology in its partnerships as well as multilateral organisations with concrete definitions. Civil society organisations have even suggested to exchange the term ‘human-centric’ to ‘people-centred’ as an attempt to help narrow the scope of the concept to make it more implementable and measurable (ETGovernment 2023). A study conducted by CONCORD states that it is better to refer to “people-centred approach” rather than to a ‘human-centric approach’ because it is a term that best reflects the value of each individual person. They claim that the concept ‘Human’ is neutral and disconnected from individuals. Although Amnesty International has raised concerns that ‘people’ as a category defined by states (for example, China) can result in the prioritisation of economic groups’ interests over individual’s rights and exclude them from necessary consultation processes (Amnesty International 2023), the term “people centred” can be found in AU policy documents (alternated with ‘human-centred’ or ‘user-centred’ digital technology) and in UN initiatives, and thus may also provide an interesting basis for negotiation with third countries. A letter following the 2021 High-Level Digital Debate of the General Assembly on Connectivity and Digital Cooperation, signed by a mix of actors from the private sector, international organisation and civil society in Europe, the US and the Global South called for: “the international community to put people at the centre of our approach to ensure no one is left behind without affordable access, skilling, and basic public services.” (UN 2021).

The AU Digital Transformation Strategy, focused on deepening digitalisation for development, uses the term ‘people - centred digital transformation’, which is a starting point for a common view on the concept. Nevertheless, while at the regional level, the strategy stresses that ‘any capacity development effort to digitise the African society must be people-centred….’, at the country level, economic needs might be prioritised over the need to protect citizens and their data. Understanding the bargaining process between economic needs and human rights will be essential as the EU promotes a ‘human-centric’ digital governance model including the benefits of strong data protection.

To promote its vision of human-centric digital transformation, the July 2022 Council Conclusions on strengthening the EU’s Digital Diplomacy set commitments for the EU to expand its network of diplomats on digitalisation and to improve coordination with its member states. The EU has made significant progress in its bilateral relations with the US and at multilateral fora. **Yet, it needs to accelerate its digital diplomacy vis-a-vis developing countries to build more significant digital partnerships across the world.** In Africa, as part of the programming of the Neighbourhood, Development and International Cooperation Instrument - Global Europe (NDICI - Global Europe), most EU delegations improved their capacity by appointing focal points to act as their experts on digital policy. These could be coordinated under a regional framework for a more coordinated engagement with African digital partners on digital questions.

3.3. Data sovereignty as data for public good

The EU’s data governance model emphasises citizens’ and businesses’ control over the data they contribute to generate, based on fundamental values and fundamental rights in all data-sharing. As Musoni discusses in her chapter, the EU’s GDPR sets high data adequacy standards for businesses targeting EU consumers, which prevents countries that do not match the GDPR’s requirements from entering the EU market. But many countries do not ensure the same level of protection for European businesses and citizens as the GDPR requires. For many developing countries, it may be difficult to achieve these levels of data protection, while for others competing interests mean that they may prefer to only partially replicate the EU’s model. This has led to countries questioning the EU’s approach, thereby looking to alternative options that are more flexible and context-based. This means that in order to continue to have the widest possible influence in the area of data protection - and in other areas of regulation moving forward - the EU should adopt a more flexible approach that embraces multiple strategies.

To promote its vision of data sovereignty, the EU should understand that a very strict approach to the adoption of its regulatory framework might go against its geopolitical ambitions given its partner’s diverse social values and economic realities. In India for instance, there is a clear interest to collaborate with the EU to set global standards on digital governance and to ensure an open, free, stable and secure digital space, even if there are differences in their data protection policies, especially on the issue of ownership of data. Since the launch of the EU’s GDPR in 2016, there has been strong criticism about the EU imposing its view of data protection on third countries. This resonated in Africa, where governments have been developing national data protection laws but that are far from being ready to fully comply with the GDPR data obligations (Mannion 2021). Some African governments simply don’t have the infrastructure nor the expertise to do so. Even if many African governments agree on the principles under the GDPR, poor implementation of data privacy laws has weakened the protection provided and limited innovation needed to support economic growth and development.

Together with continuing to play a role in shaping data protection and privacy norms by expanding its partnerships, the EU should support its partners in developing their own approach to regulating the use of data in a way that also carefully accounts for local priorities, needs and capacities (Pisa and Nwankwo 2021). An increasing number of African governments are developing data protection policies to respond to local needs (for example, attract investment, as well as address the abuse of data of vulnerable communities which is becoming a domestic issue) as a result the discourse around data privacy has increasingly been focusing on the idea of basic rights. Yet, discussions on the externalisation of the GDPR have revolved around difficulties in implementing the EU's regulatory framework, challenges for data protection authorities to comply with its principles, and the responsiveness of the regulation to partners' social and economic values. This means that the EU's success in promoting its data sovereignty lies in focusing on how it can support the development of data protection policies that promote the growth of local economies and that can ensure a win-win solution. This is especially important for partners that are looking at the EU model but operate in resource-constrained contexts.

The EU should consider working with key partners in the Global South to start discussions around a potential multilateral initiative on data protection allowing for wider dialogues on data transfer from one region to another, rather than simply relying on the very high data adequacy standards of the GDPR. As mentioned above, this would imply creating strong alignment with partners who have some shared understanding around human-centric digitalisation and are already pushing for multilateral discussions on data policy such as India, South Africa, Kenya, organisations like Smart Africa, the AU, regional economic communities (RECs) in Africa, etc. The EU is a strong believer in multilateralism and has been one of the main forces driving the Digital Compact at the UN, which it hopes will set a minimum shared approach to digital governance. Similarly, the EU is enthusiastically supporting UNESCO's initiative on Platform Regulation, which it hopes will play a role in developing standards globally in much the way that the Digital Services Act seeks to do within the EU. However, to date, there has not yet been a realistic multilateral initiative on data sharing, and the EU relies on its own data adequacy agreements with third countries. A multilateral approach would allow for a more level playing field and shared rules. It is unlikely that such an initiative could bring together the very opposing approaches of certain global powers, but it might begin to build a base for a new approach to data sharing between a wider range of countries that live up to a certain standard of data protection.

This suggests that the EU should emphasise a vision of data sovereignty that does not only uphold high standards, but that also focuses on data for public good (DPG) and building local data economies. This means that while the EU sets standards on regulating the digital space, it should also promote the implementation of digital public goods: open-source, interoperable digital solutions that can then be used in partner countries to build digital public infrastructure such as e-ID, payment systems, etc. ensuring that these are built with a human-centric approach in a way that benefits all citizens and their economies. There are already positive examples of European initiatives supporting data for public goods in partner countries including the German Ministry for Development (BMZ) supporting the FAIR Forward project, which makes AI training services available in three African languages including Swahili. Another initiative is GovStack, which uses open-source tools, sandbox for testing and communities of practices to build inclusive and safe digital public infrastructure (World Economic Forum 2022).

4. Working with other global and regional actors

Developing shared approaches to digital sovereignty - both with traditional partners, such as the other G7 members, as well as with emerging powers like India, and regional blocs such as the African Union, will be essential to the EU's geopolitical aims regarding digital governance. The EU has long struggled with accusations that EU actors preach to partner countries in the Global South, rather than truly treating them as partners. When it comes to digital governance, and to the question of digital sovereignty, the EU cannot afford to be seen as preaching its vision without consideration of the needs and visions of others. The rhetoric around the “Brussels Effect” and the externalisation of internal EU regulations risks doing just this and alienating potential allies by focusing too much on them replicating EU regulations. It also risks undermining the EU’s claims about supporting the digital sovereignty of others. Thus, while the EU’s experiences are certainly worth sharing with partners, this should be done in a way that shows mutual respect and that relies on a more sophisticated digital diplomacy vis-a-vis partners. Such an approach is beginning to emerge vis-a-vis certain partners, but should be extended to wider partnerships with the Global South.

Here we look briefly at EU-US collaboration in the Global South, and at relations with India and Africa - notably the African Union - in order to illustrate different kinds of partnerships with different kinds of actors. Yet, there are a wide range of other actors with which the EU might collaborate further with around building shared approaches to digital sovereignty, including notably other G7 partners, members of the Association of Southeast Asian Nations (ASEAN) and countries in Latin America and the Caribbean.

The United States

The EU’s relationship with the **United States** around technology has been a fraught one and continues to experience highs and lows. Despite many commonalities, the different approaches to both digital regulation and on industrial policy, including most notably on data protection, the Digital Markets Act and Digital Services Act, and the Inflation Reduction Act, mean that the approaches of the two blocs are rarely in harmony (See Karkare 2023 and Musoni 2023 in this report). This is intimately connected to the very different approaches that the two are taking on questions of digital sovereignty - the EU more explicitly, the US implicitly - and notably their different visions for their own leadership role internationally.

Yet despite many differences, the EU and US largely manage to enjoy a relationship of mutual respect, finding common cause where they do have clear shared interests, such as in the recent ITU elections in 2022, which saw the election of American candidate, Doreen Bogdan-Martin as Secretary-General and Lithuanian Tomas Lamanauskas as Deputy Secretary-General. They also developed the Trade and Technology Council (TTC) as a forum to discuss some of the most tense issues around regulating, developing and promoting technologies. **The focus at the TTC on joint investments in digital infrastructure projects in third countries also offers an interesting example of bilateral cooperation, and if expanded could also allow for scalable and impactful projects.** Already, the EU and the US have agreed to jointly support the Kenyan government in developing its 2022-2032 National Digital Masterplan, as well as contribute in expanding Jamaica’s connectivity (EC 2022). It could also offer a valuable example for wider cooperation under the G7’s Partnership for Global Infrastructure and Investment, announced in 2022.

India

Over the past years, the EU and **India** have been tightening their bilateral relationship, driven by the changing geopolitical environment and India’s growing ambition to balance competition over critical technology supply chains and a reduced reliance on China (Kranenburg and Okano-Heijmans 2023). The culmination of this was the 2020 India-EU summit and the announcement in February 2023 of the establishment of a Trade and Technology Council (TTC) (EC 2023a) in the coming months as an attempt to make the relationship more strategic. There is clearly political will to push the partnership forward - each hopes to access the other market to support their strategic autonomy. The EU also hopes to achieve greater alignment with India in debates on global internet governance. Despite a certain degree of convergence of data regulation as a result of India slowly moving to view privacy as a fundamental right, their contrasting views on data protection have limited the relationship.

India stands to be a strong partner for the EU as it aims to ensure its own autonomy and takes a differentiated approach to China, however, it is not clear whether India’s data protection bill is compatible with the EU’s GDPR

(Voelsen and Wagner 2022). This is in part because the Indian government has made very close links between data protection and national security issues as well as putting emphasis on protectionist policies to drive the growth of the domestic industry for self-reliance. Further, India has also been criticised for being ambivalent on digital governance at the multilateral level. The EU is taking positive steps in institutionalising its partnership with India, but it will have to strengthen consultation with India via sustained dialogue to align their positions before debates at multilateral fora. Stronger consultations can also help them align their domestic policies with the international dimension. Furthermore, in the face of these opposing views, the EU needs to make concessions to be able to leverage other areas of the digital partnership. In particular, the EU's focus on norms and the differentiated approach to China remain key concerns for India (idem. 2022).

As the EU focuses on building a more strategic, and long-term relationship with India, it will be important for the EU to look at their digital partnership holistically rather than through a solely normative lens, which will also be key for the EU to promote a mutually reinforced and shared technological sovereignty with its partners (ETGovernment 2023). For example, it should leverage India's growing digital economy sector and work together to curb the dominance of the US and China in the platform economy. **There are also opportunities to work together in promoting digital public goods (DPGs) and digital public infrastructure (DPI) on the international stage, given India's strengths in these areas and the EU's own ongoing experiences developing interoperable cross-border DPI.**

Africa with focus on The African Union

The EU partnership with the **African Union** on digital transformation is very new. The EU strongly integrated digital transformation in its 'Comprehensive Strategy with Africa' in 2020, and this focus was further strengthened by the EU-AU investment package under the EU €300 billion Global Gateway connectivity initiative. There is ample room for improving the partnership, which at the moment is focused on planning a series of digital infrastructure projects and building out the digital component of the EU's development cooperation with Africa, including providing technical support to various digital policy processes in the continent. Through the GIZ Datacipation project and the Team Europe Initiative on Data Governance in sub-Saharan Africa, the EU is supporting the development of the AU Data Policy Framework, which states that 'the AUC, member states, RECs, African institutions and international organisations shall cooperate to create capacity to enable African countries to self-manage their data, take advantage of data flows, and govern data appropriately' (AU 2022). The framework reflects the AU's ambitions to achieve greater digital sovereignty for its Member States by building a common data market that could fuel African innovation ecosystems. It also shows the ambition to participate in multilateral discussions on data governance with one unified voice. Therefore, strongly anchoring the concept of digital sovereignty into the EU's fundamental rights framework and bringing it in firmly in its digital partnerships could be a major step towards better digital partnership and coordination at multilateral fora. This should entail a real negotiation around what the term means for policymakers on each side and how this can actually be implemented in practice.

To make the partnership truly mutually beneficial, there are a few aspects that need to change. First, the debates on digital transformation have been characterised by a strong imbalance between the two sides, although at the bilateral level (for example, Kenya), the relationship is evolving fast from traditional development cooperation to economic cooperation, based on investment for hard and soft infrastructure to push the country's own digital positioning in the region (Sergejeff et al. 2023). In particular, a shortage of strong technical expertise on the AU side has allowed the EU to remain assertive in its negotiation with African counterparts, often failing to consult them on key initiatives (Domingo 2022). **The EU should refrain from such unilateralism in its relations with Africa, instead supporting capacity building and encouraging the AU to invest more in digital expertise.** Secondly, **as the EU works for more policy coherence between its domestic and external domains, it should make sure that there is space to harmonise with Africa's regulatory frameworks.** For example, considering how to bring in the EU sphere countries who are not data adequate or that are shifting away from its model (for example, Kenya). Thirdly, **the EU should follow through on the promise of Global Gateway in Africa, although this will be a gradual process over several**

years. As discussed by Musoni in this report, safe and secure digital infrastructure is an essential element of achieving a certain degree of digital sovereignty and ensuring data is secure. Thus, supporting a major uptick in EU investment in reliable digital infrastructure is a key element of showing real support to Africa's digital sovereignty, although this is not simply a question of new money now, but of a sizable increase in public and private investments over the coming years (Teevan 2023).

5. Conclusion and summary of recommendations

In this chapter, we have started to lay out certain elements that the EU would need to address in order to develop an approach to digital sovereignty that appeals at the international level, and can support EU digital partnerships with developing countries in the Global South. Firstly, we have argued that the EU will need to demonstrate how its policies support and do not hinder the digital sovereignty of partner countries, notably by demonstrating that its domestic policies are consistent with its international rhetoric on building stronger partnerships and alliances with countries in the Global South based on mutual respect and real dialogue. Secondly, we have argued that the EU will need to work with others to develop joint approaches to key concepts behind its vision of digital sovereignty, notably the notion of human-centric digital transformation if it hopes to truly make this a shared driver of policy discussions with partners and at multilateral fora. Thirdly, we argued that the EU should take a more flexible approach in its partnerships with third countries, including notably on data governance, so as to develop a wider range of partnerships and thus have greater influence. Finally, we briefly looked at how the EU might work with certain countries and regions to come up with a shared basic understanding of digital sovereignty. This shared understanding would seek to identify some common principles while acknowledging that there will be some divergences based on different levels of development and different national interests. This might in turn allow the EU to work with others to negotiate certain international rules and standards.

Below, we summarise some of the recommendations that were developed throughout this last chapter:

1. **Consistency between internal and external policies:**

- Integrate the external dimension into all domestic strategies, and carry out real impact assessments with regard to the impact of domestic regulations externally. The EU has adopted a host of measures to strengthen its own digital ecosystems through digital regulation and industrial policy. Yet, in order to truly live up to the ideals of the geopolitical commission and reflect the external dimension of these domestic policies, they should be backed up by more detailed studies looking at what the effects of these policies are for third countries, and particularly for developing countries in the Global South. An initial step might be to carry out a broad study looking at how the external dimension has been integrated to date, and what steps might be taken to strengthen the external dimension of existing policies.
- Develop plans for how the EU's growing focus on domestic industrial policy can also integrate partner countries' interests and ambitions, potentially integrating them into EU value chains through further Global Gateway flagships. The TEI on vaccine manufacturing is one good example of this, which will both strengthen European industry and African resilience in the face of future epidemics or pandemics. Similarly, efforts are underway to integrate North African countries into European plans around the development of green hydrogen. As mentioned above, the reference to supporting processing of materials in partner countries in the Critical Raw Materials Act also offers an important opportunity to support industry in partner countries, and for the EU to differentiate itself from China. Most importantly for digital industries perhaps will be support to the data economy, and to demonstrating how the data economy can work for developing countries. For example, the TEI on Data Governance in Sub-Saharan Africa will need to deliver on not just strengthening digital governance in partner countries, but on developing practical use cases in a range of industries that demonstrate the economic utility of strengthening digital governance. Given the low rate of

adoption of digital technologies in developing countries, the focus should be on increasing the demand for technologies as well as their supply.

- In line with the above, the EU should also scale up support to local technology hubs, and offer more funding for research and innovation partnerships with developing countries. For example, concerted efforts to include universities and research institutes from developing countries in Horizon Europe projects could play an important role in supporting more joint initiatives that address developing country needs.

2. A common understanding of 'human-centric' digital transformation

- The EU should strongly embed its human-centric approach to digital transformation in its digital partnerships, but most importantly in its advocacy at multilateral organisations with concrete definitions and benchmarks to measure its impact.
- The EU can lead discussions to develop a common understanding of the concept of 'human centric' digital transformation together with partner countries, rather than focusing only on sharing its own still sometimes vague terminology. Understanding some of its partners' bargaining process between economic needs and human rights will be essential as the EU promotes a 'human-centric' digital governance model, including emphasising the benefits of strong data protection.

3. Data sovereignty as data for public good

- Understand that a very strict approach to the adoption of its regulatory frameworks, such as GDPR, might go against its geopolitical ambitions to promote its vision of data sovereignty given its partner's diverse social values and economic realities. Adopting a more varied approach may ultimately serve the EU's interests better, including continuing to support partners in developing their own approach to regulating the use of data, integrating local priorities, needs and capacities, expanding initiatives such as the AU-EU Data Governance programme, and also pursuing a new approach at the multilateral level. While the EU should continue to promote high data protection standards, it should also be open to coupling this with more flexible approaches that can potentially enable it to expand its reach.
- Consider working with key partners through bilateral dialogues, including India, ASEAN countries, key Latin American and African countries, as well as multilateral dialogues with the AU, Smart Africa, ASEAN, and leading private sector actors in the Global South to start discussion around a potential multilateral initiative on data sharing, complementing the work that the EU is doing with the UN Tech Envoy on the Global Digital Compact. For instance, this might include expanding on the Africa-Europe Digital Regulators Partnership by working with the Network of African Data Protection Authorities (NADPA) to develop a holistic understanding of the priority needs for African data protection regulators and developing frameworks which align with these needs. This might also entail working with partners to ensure that there is a common approach to guide key partners on how data should be processed, shared or transferred, and encourage key partners to reflect these guiding principles throughout bilateral and multilateral agreements.
- Emphasise a vision of data sovereignty that does not only uphold high standards, but that also focuses on data for public goods (DPG) and building local data economies. This is a key aspect of the AU-EU Data Governance programme that will need to be further elaborated through the development of practical use cases that have wide relevance and interest for African citizens, businesses and governments.

4. Building partnerships with key partners on digital sovereignty

- US:
  - Given a joint interest in offering alternatives to a Chinese model of cyber sovereignty in the Global South, the EU and US should expand the focus on joint investments in third countries at the TTC. This could offer an interesting example of bilateral cooperation, potentially allowing for more scalable and impactful projects. They would also provide valuable examples for wider cooperation under the G7's Partnership for Global Infrastructure and Investment, announced in 2022.

  - As the joint advocacy of the EU, US and other like-minded partners around the ITU elections in 2022 demonstrated, joining forces at multilateral fora can lead to positive outcomes. However, the fundamental differences in terms of the approaches to data sharing and data sovereignty ultimately weaken potential cooperation, and will need to be overcome in order to develop a truly effective joint approach at multilateral fora.

- India:
  - There are opportunities to work together in promoting digital public goods (DPGs) and digital public infrastructure (DPI) on the international stage, given India's strengths in these areas and the EU's own ongoing experiences developing interoperable cross-border DPI. ECDPM will be doing more work looking at what might be possible in this area over the coming months.

- Africa:
  - The EU should continue to work with the AU and its members to ensure the flow of data between Africa and Europe, and ultimately work towards the closer integration of their respective digital single markets as stated in the EU-Africa Global Gateway Investment Package. For this, we have argued that the EU could open negotiations with African countries on a potential Data Privacy Framework. This could be accompanied by a new TTC with key players such as the Network of African Data Protection Authorities (NADPA), while deepening its understanding of the continent's digital ecosystem needs and context.
  - Meeting the commitments made under the Global Gateway Initiative, including mobilising EUR 150 billion in investment for digital infrastructure for Africa, will be crucial for the credibility and relevance of the EU as a valued global digital partner. However, the implementation of the Global Gateway initiative will be a gradual process over several years, and in this sense the mid-term review of the NDICI programming will also be crucial to assess whether the EU's digital diplomacy efforts are helping achieve its goals and adjust partners' expectations in the process. Developing a genuinely new approach in the way the EU, member states and private sector actors work together will also be essential to developing Global Gateway into something that truly delivers in the medium to long-term, going above and beyond initial commitments (Teevan 2023). This may include putting in place new innovative joint financing mechanisms - something ECDPM will explore in future work.

References: Chapter 3

Amnesty International. 2022. 1. “Community of common destiny” or “community of shared future”. Amnesty International.

AU. 2022. AU Data Policy Framework. Addis Ababa: African Union.

Bauer, M. 2020. Europe’s Quest for Technology Sovereignty: Opportunities and Pitfalls. Brussels: European Centre for International Political Economy (ECIPE).

Broeders, D., Cristiano, F. and Kaminska, M. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. Journal of Common Market Studies (JCMS).

Burwell, F. and Propp, K. 2022. Digital sovereignty in practice: The EU’s push to shape the new global economy. Washington DC: Atlantic Council.

CoEU. 2022. Council Conclusions on EU Digital Diplomacy. Brussels: Council of the European Union.

CONCORD. 2023. Demystifying the people-centred approach for the digital transformation. Brussels: CONCORD.

Domingo, E. 2022. Bringing African digital interests into the spotlight. ECDPM commentary. Maastricht: ECDPM.

EC. 2020a. Impact assessment of the Digital Services Act. Brussels: European Commission.

EC. 2020b. Joint Statement - 15th EU-India Summit, 15 July 2020. Brussels: European Council and Council of the European Union.

EC. 2021a. Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions. 2030 Digital Compass: the European way for the Digital Decade. Brussels: European Commission.

EC. 2021b. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank. The Global Gateway. Brussels: European Commission.

EC. 2022. EU-US Joint Statement of the Trade and Technology Council. Brussels: European Commission.

EC. 2023a. Critical Raw Materials: ensuring secure and sustainable supply chains for EU's green and digital future. Brussels: European Commission.

EC. 2023b. EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade. Brussels: European Commission.

EEAS. 2016. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union’s Foreign And Security Policy. Brussels: European External Action Service.

EEAS. 2022. US/Digital: EU opens new Office in San Francisco to reinforce its Digital Diplomacy. European External Action Service.

ETGovernment. 2023. EU signs tech tie-up with India, to set up Trade & Technology Council for deeper cooperation in digital governance. ETGovernment.

EUCO. 2020. Special meeting of the European Council (1 and 2 October 2020): Conclusions. Brussels: European Council.

Kranenburg, V. and Okano-Heijmans, M. (Eds). 2023. How strategic tech cooperation can reinvigorate relations between the EU and India. Clingendael Report. The Hague: Clingendael.

Mannion, C. 2020. Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. Vol. 53. Vanderbilt Law Review.

Pisa, M. and Nwankwo, U. 2021. Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development. Washington DC: Center for Global Development.

Pons, A. 2023. Digital Sovereignty: for a Schuman Data Plan. European Issue n°652. Fondation Robert Schuman.

Rimbaud, E. 2021. Le peuple souverain et l'espace numérique. Paris: Le Grand Continent.

Sergejeff, K., Domingo, E. and Veron, P. 2023. The EU, geopolitics and human development: Insights from Zambia, Kenya and Guinea. ECDPM Discussion Paper 340. Maastricht: ECDPM.

Teevan, C. 2019. Geopolitics for dummies: Big challenges await the new European Commission. ECDPM Commentary. Maastricht: ECDPM.

Teevan, C. 2023. Global Gateway as new approach, not simple funding pot. EURACTIV.

Teevan, C. and Sherriff, A. 2019. Mission possible? The Geopolitical Commission and the partnership with Africa. ECDPM Briefing Note 113. Maastricht: ECDPM.

Teevan, C. and Domingo, E. 2022. The Global Gateway and the EU as a digital actor in Africa. ECDPM Discussion Paper 332. Maastricht: ECDPM.

United Nations. 2021. Leave No One Behind: A People-Centered Approach to Achieve Meaningful Connectivity. United Nations.

Vestager, M. 2022. Speech by Executive Vice-President Vestager on the Declaration on Digital Rights and Principles. Brussels: European Commission.

Voelsen, D. and Wagner, C. 2022. India as an Ambivalent Partner in Global Digital Policy. Potential and Limits of Cooperation in the Digital Economy and Internet Governance. Stiftung Wissenschaft und Politik (SWP).

World Economic Forum. 2022. Inclusive digital infrastructure can help achieve the SDGs. Here's how. World Economic Forum.