Setting the scene

Digital sovereignty, and the related concepts of cyber sovereignty, technological sovereignty and data sovereignty are being employed more and more widely by policymakers across the world. There is little consensus about what these terms actually mean, and indeed for different global actors, it often has very different connotations and policy consequences.

Broadly speaking, digital sovereignty refers to the need for control over the physical layer (infrastructure, technology), the code layer (standards, rules and design) and the data layer (ownership, flows and use). It may be motivated by different interests such as protecting individuals (data protection), increasing the competitiveness of domestic firms (local content requirements or other industrial policy considerations), and protecting core democratic values or strategic public interests (maintaining sovereignty in critical infrastructure, national security).

However, while global actors appear to be broadly on the same page in terms of the perceived need to stimulate homegrown industries, notably in high-tech areas with potentially significant national security consequences, there are major variations in how these actors approach the governance of these technologies, and particularly in their approaches to data governance.

Competition over technological innovation and development, backed by industrial policies, has become the major geopolitical fault line between the United States (US) and China today, while it is also fuelling a subsidy race between the US and the European Union (EU). These domestic efforts to incentivise cutting-edge technologies and to become self-sufficient in vital components of the digital economy - notably chips - will undoubtedly have spillover consequences for the rest of the world.

Digital governance, and particularly data governance, has increasingly become an area of contention, with a growing focus on *who* provides the basic infrastructure of the digital economy, including in third countries across the world. Fearing data colonialism, where data is extracted by foreign firms from marginalised communities without their knowledge or consent for profit and to feed their own technological development, a growing number of countries are grasping for ways to protect citizens' data and ensure national security. Other motivations such as spurring local innovation for economic development have also made data governance a key policy issue. Yet, approaches vary greatly - both amongst the global powers and in the Global South - from no controls to strict data localisation.

The competition over approaches to digital technologies and digital sovereignty is playing out at multiple levels. In domestic industrial and governance strategies, in foreign policy and external infrastructure strategies and at multilateral institutions, major powers have been actively promoting competing visions - they have been vying for positions in top jobs down to very technical working groups. Some emerging powers, such as India, have developed relatively sophisticated visions of their own, while many countries in the Global South are still struggling to position themselves and develop a coherent approach to digital sovereignty.

This work will examine: (i) why digital sovereignty has emerged as such a geopolitically charged term, (ii) how the different approaches of different global and emerging powers are playing out, and (iii) the implications for EU policy and digital partnership with developing countries in the Global South, including in Africa, Latin America and the Caribbean (LAC), and Asia-Pacific. It will delve into two interrelated areas of policy with major ramifications for digital sovereignty - data governance (chapter 1) and industrial policy (chapter 2). It argues that a realistic assessment of the international implications of both will be necessary to offer an attractive and meaningful view of digital sovereignty in international affairs. Finally, it will propose a series of policy recommendations for policymakers in the EU in engaging with counterparts in the Global South (chapter 3).

Origins of the debate

The debate about digital sovereignty cannot be divorced from wider debates about sovereignty in international affairs. The question of sovereignty is itself a complicated one, and one that has long been a central bone of contention in international affairs. For China, and many postcolonial countries, protecting full state sovereignty continues to be a core tenet of their position in international affairs, and China has sought to use the United Nations (UN) system to defend its vision of sovereignty. The interventionism engaged in by the US and some allies in the 1990s and 2000s in the name of liberal internationalism, most notably with the invasion of Iraq in 2003, was thus anathema to many countries across the world. The question of sovereignty is, of course, also central to current debates about the Russian invasion of Ukraine, raising this question to the forefront of international affairs once again.

In the area of digital technologies and internet governance, the liberal internationalism of the US was taken even further, promoting a cyber world without borders, where information would flow freely across the world with no state interference. This vision was always viewed with suspicion by states such as China for which state sovereignty should also apply to the online world, but in more recent years, this ideal of a completely open and unregulated internet has come to be viewed with unease even by the US's closest allies in Europe, Japan and elsewhere. Edward Snowden's revelations on the US government's practices under the US Cloud Act and growing concerns about 'surveillance capitalism,' where (US) firms harvest data to monetise it through targeted advertising to influence behaviours have added to the concerns. This has led to a growing focus on regulating the online space and developing indigenous technologies across the world, albeit with varying approaches from different established and emerging powers.

China introduced the concept of 'cyber sovereignty' (wangluo zhuquan 网络主权) and with its Great Firewall sought to preserve a strong idea of state sovereignty: "With territorialisation, Beijing seeks to delineate its national boundaries in cyberspace, ensure that online processes affecting important Chinese interests take place within those boundaries, and unwanted activities can be barred from entering" (Creemers 2020: p.10). At the same time, the blocking of major US companies allowed for the emergence of local champions, providing more or less identical services in a process of 'indigenisation' (Ibid.).

Over time, this largely domestic process was coupled with a growing externalisation process as China sought to develop markets for its technology abroad, by developing the Digital Silk Road. At the same time, China and Russia increasingly adopted a more proactive cyber diplomacy at international institutions that was intimately connected with their domestic visions regarding cyber sovereignty and state control. China developed sophisticated cyber diplomacy at institutions such as the International Telecommunication Union (ITU) that allowed it to defend its vision and interests on the international stage. This included China's promotion of the controversial New IP (internet protocol) proposal at multilateral fora, which would have created a new internet based on new standards and protocols with a view to responding to potential future challenges with the existing architecture. However, the proposals were viewed by critics as a way of putting greater control of the internet architecture in the hands of states, thereby enhancing potential state surveillance. Critics from the EU and elsewhere also consider it not to be sufficiently developed in terms of the technical specifications, and to not include sufficient consideration around interoperability with the existing internet (Murgia and Gross 2020; Degezelle et al. 2022). While the original proposal was rejected, China continues to promote New IP via other channels. Russia also tabled resolutions on cyber sovereignty at the UN General Assembly that managed to garner substantial support across many parts of the Global South.

Although the EU had already adopted the General Data Protection Regulation (GDPR) in 2016, it was the election of Emmanuel Macron in France in 2017, and the subsequent agenda of the von der Leyen Commission, appointed in late 2019, that really began to bring the debate around digital sovereignty into the mainstream policy debate in Europe. Although the focus of different actors in Europe tends to vary, the European approach broadly encompasses a strengthening of its digital governance model, coupled with a growing focus on developing home-grown European technologies. On the governance front, the EU is seeking to build on GDPR to develop an approach that puts European citizens' individual rights front and centre of its conception of sovereignty, and at the same time, it seeks to build on existing antitrust laws to improve competition and create greater space for innovation. This has gradually been accompanied by a growing focus on industrial policy, although there are still many debates around the appropriate role for states and the EU in driving forward industrial strategy.

India, like other developing countries, does not want to choose between the US and the Chinese digital sovereignty models and is developing its own approach based on its own interests and development context. India's approach to digital sovereignty, supported by Digital India and Make in India, aims to find a balance between national security, economic growth and development, and privacy concerns. Yet, this approach is also quite distinct from the EU's approach, allowing a much stronger role for the state and less strenuous standards of data protection. It aims to boost the growth of its domestic tech industry, which includes the unrolling of the digital public infrastructure India Stack, to respond to growing Chinese influence on its market and (cyber)security threats in the region. These have been driving forces of its digital sovereignty approach, and in turn of its digital diplomacy (Basu 2021). For example, the Indian Digital Personal Data Protection bill draws principles on data regulation from both the EU's GDPR and Singapore's data protection law and has been considered by some African countries as a model that would respond to some of the challenges they encounter when trying to adopt a GDPR inspired data protection policies, especially the issues related to data adequacy (see Musoni 2023 in this report for more). However, India still needs to strike a balance between security and economic interests given its reliance on foreign, especially Chinese, firms for its infrastructure (Burrows and Mueller-Kaler 2021). India has been strengthening its role in debates on digital governance at multilateral forums despite being criticised for being ambiguous when it comes to its selective alignment. The Digital India Act, which will govern all digital aspects, and its data protection bill, both in review, will be key policy tools that will strengthen the country's digital sovereignty and make it a key partner, including with the EU, on setting standards around regulating artificial intelligence (AI) and machine learning (ML) technologies (Chin 2023).

Discussions about digital sovereignty are growing across other parts of the world also. African and Latin American theorists and activists have increasingly raised the risks of digital colonialism or data colonialism, and begun to advocate for ways that their countries or regions might take steps towards achieving their own digital sovereignty. This has notably included the drafting of a letter to then-presidential candidate Luiz Inácio Lula da Silva by activists and researchers in Brazil in August 2022, entitled 'Emergency Program for Digital Sovereignty,' denouncing the data extractivism at the heart of contemporary digital development, and calling for the country to address its dependencies (Bosoer 2022). Japan, South Korea and Taiwan have each made themselves indispensable nodes in global value chains (Pons 2023).

A number of African countries have also begun to emphasise their digital sovereignty through a variety of different measures. At the continental level, the Digital Transformation Strategy gave some initial hints of an emerging interest in digital sovereignty but did not develop this concept in any meaningful way. The African Union (AU) Data Policy Framework begins to provide a more comprehensive vision on the side of data governance and its potential to feed emerging digital and industrial sectors. Yet, at present, the approach tends to be somewhat fragmented with different African countries adopting very different approaches to questions such as data localisation and digital taxation. It will now be essential to step up the actual implementation of the Data Policy Framework in order for African countries to work together towards achieving a shared vision for data governance as part of a wider pursuit of digital sovereignty.

References: Summary

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

Basu, A. 2021. Sovereignty in a ‘Datafied’ World. Issue Brief 501. October 2021. Observer Research Foundation.

Bosoer, L. 2022. Digital Sovereignty: Voices from Latin America. European University Institute (EUI).

Burrows, M. and Mueller-Kaler, J. 2021. India’s quest for digital sovereignty. In: Smart Partnerships amid Great Power Competition: AI, China, and the Global Quest for Digital Sovereignty. Washington DC: Atlantic Council.

Chin, K. 2023. What is the Digital India Act? India's Newest Digital Law. UpGuard.

Creemers, R. 2020. China’s Approach to Cyber Sovereignty. Berlin: Konrad-Adenauer-Stiftung.

Degezelle, W. with Yahmadi, H., Mackenzie, T., Fathy, N. and Kummer, M. 2022 (Stantec). The Open Internet as cornerstone of digitalisation. The Global Gateway Partnership Opportunities between the European Union and Africa. Brussels: European Union.

Murgia, M. and Gross, A. 2020. Inside China’s controversial mission to reinvent the internet. London: Financial Times.

Pons, A. 2023. Digital Sovereignty: for a Schuman Data Plan. European issues policy paper n°652. Brussels: Foundation Robert Schuman.