Executive Summary

Digital sovereignty is a term widely being used by policymakers across the world. But there is little consensus about what it actually means, with cyber sovereignty, technological sovereignty and data sovereignty used interchangeably and yet having different connotations and significance for different actors. Overall, the debate on digital sovereignty cannot be divorced from the idea of sovereignty in international affairs.

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), with major differences in how countries pursue these objectives.

The competition over approaches to 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, with major powers, namely the United States of America (US), China and the European Union (EU), promoting competing visions. Competition over technological innovation and development, backed by industrial policies, has deepened the geopolitical fault line between the US and China, and more recently fuelled a subsidy race between the US and the EU. Digital governance, and particularly data governance, has increasingly become an area of contention, coupled with a growing focus on *who* provides the basic infrastructure of the digital economy. These dynamics have spillover consequences for the rest of the world.

While the US's vision of a borderless cyber world where information flows freely without state interference is viewed with increasing unease even by its closest allies, China's conception and promotion of its vision of cyber sovereignty is also seen as controversial and enhancing state surveillance. As a third way between the US's 'surveillance capitalism', where largely unregulated firms harvest data to monetise it through targeted advertising to influence behaviours, and China's 'surveillance state', which uses technology like facial recognition, social credit systems, and censors the internet to monitor and surveil its citizens' activities, the EU had a more regulatory approach which puts individual rights front and centre in its conception of digital sovereignty. Its two-prong approach to digital sovereignty, which has accelerated since the beginning of the von der Leyen Commission in 2019 seeks to increase the robustness of the EU's regulatory toolkit and leverage the 'Brussels Effect' to shape global standards and the regulatory environment, while gradually embracing an active digital industrial policy to stimulate the development of European digital champions.

Developing countries want to develop their own approach to digital sovereignty based on their development needs and interests without having to choose between the US or China. Geopolitical competition and related tensions however are reducing the policy space for countries to do this. 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. Nevertheless, discussions are growing, with African and Latin American theorists and activists also raising the risks of digital colonialism or data colonialism, and advocating for ways to achieve their own digital sovereignty.

India's approach to digital sovereignty aims to find a balance between national security, economic growth and development, and privacy concerns by, among other things, unrolling the digital public infrastructure 'India Stack'. African countries have also begun to emphasise their digital sovereignty through a variety of different measures. At the continental level, the Digital Transformation Strategy reflects an emerging interest in digital sovereignty, although it does not develop on what this concept means for Africa in any great detail. The African Union's (AU)

Data Policy Framework begins to provide a more comprehensive vision on data governance that supports innovation and the better provision of public and private services.

Countries' approaches to the governance of personal and non-personal data are seen as an extension of their sovereignty, and an essential part of their approach to digital sovereignty. Governments approach it in different ways given their unique social, economic and political environment, technological capabilities, domestic priorities and digital foreign policy, indicating that there is no 'one size fits all'. Other factors such as increasing (digital) geopolitical tensions, risks of foreign government surveillance, and concerns of digital colonialism also impact national data governance frameworks.

The regulation of personal data and non-personal data is also handled quite differently from one government to the other. Governments usually develop data protection laws to protect their citizens' personal data in line with clearly defined principles with safeguards to prevent the abuse, including by big tech. The EU's General Data Protection Regulation (GDPR) is a comprehensive law protecting personal data and widely seen as an international best practice, with the EU seeking to influence international standards and norms with the GDPR. The EU is also leading the way by developing new legal frameworks such as the Data Act and Data Governance Act which regulate the sharing, processing and innovative use of non-personal data while facilitating data sharing among trusted actors, strengthening mechanisms to increase data availability and overcoming obstacles to the reuse of data. For the EU, an important aspect of digital sovereignty is about leading in norms and standards setting, while advancing the protection of fundamental rights and values.

The US and China have contrasting approaches. While most big tech companies are from the US, the country does not have a data protection law at the federal level and instead, some states have promulgated their own data protection laws. Not only is it unclear to external players how personal data is treated once it is transferred into the US, transfer of personal data outside the US also does not have restrictions in line with the ethos of free and open data flows, which makes it easier for US firms to do business at a global level. More broadly, the US reliance on corporate self-regulation and support for multi-stakeholder initiatives that gave US firms an outsized role, has been viewed with suspicion by China, where the state has played a more prominent role. In line with the growing trend on data protection, China recently adopted a data protection law, though it still leaves room for the government to exercise surveillance. Further, Chinese laws place strict restrictions on cross border data flows, with mandatory requirements for local storage of data, which may conflict with laws from other countries as shown by the 2021 Data Security Law which does not allow foreign law enforcement authorities to access data stored in China unless the Chinese authorities have approved whereas the Clarifying Lawful Overseas Use of Data (CLOUD) Act authorises US authorities to demand access to data held by US companies overseas regardless of where it is located.

Developing countries have also been making some progress in defining their data governance approaches. India is in the process of developing its own data protection law, which is modelled along the GDPR principles as well as Singapore's data protection law, but allows greater exceptions to access data for security purposes than the GDPR. This is timely considering the amount of personal data processed under its Aadhaar digital ID system. African countries are also developing their own data protection laws, with some leaving more room than others to exercise discretion in processing data, along with sometimes unclearly defined national security exceptions. The African Union's Convention on Cyber Security and Personal Data Protection can potentially create the basis for a unified continental approach to data protection once it comes into operation. The AU's Data Policy Framework seeks to create an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation, collaboration between in-country sectors, institutions, and stakeholders, and harmonise policies across the continent in a manner that provides the scale and scope required to create globally competitive markets.

Governments are investing in local data centres as there is a growing perception that whoever controls the physical infrastructure exercises sovereignty over data, with fears that foreign control on such infrastructures would invite foreign surveillance. National security interests and economic benefits have motivated the adoption of data localisation measures but countries also have competing approaches to data localisation. The US approach is opposed to data localisation and advocates for free flow of data. China, on the other hand, exercises a strong version of digital sovereignty with strict data localisation rules as well as stringent security assessments for cross-border transfer of data. The EU, driven by its human-centric approach to data, allows for conditional transfer of data with requirements of data protection principles and safeguards in line with the GDPR. India and Africa have a hybrid approach which seeks to promote local storage of data while permitting data transfers against defined rules.

Though there are differences in data governance frameworks which are shaped by broader visions of digital sovereignty, cooperation on, and development of, principles on data processing and data sharing is necessary because ultimately the value of data is generated not from local storage but from sharing and using it.

As digital sovereignty has come to encompass technological sovereignty or indigenisation to build and/or strengthen domestic technological and manufacturing capabilities, digital and industrial policies have also become closely intertwined. While for some, it may be about boosting the national industrial production through domestic champions, for others it may be about risk mitigation and securing the supply of inputs, with digital industrial policies having a strong element of geopolitical considerations.

Although the US, China and the EU approach digital sovereignty very differently, their digital industrial policies and instruments have similarities, with a prominent role played by the state combined with experimentation and substantial investments in research and innovation. The motivations for these policy actions were very different, however. For instance, defence and military spending played a critical role in propelling the US to its leading position in digital technologies by enabling investments in research and development into several critical digital innovations. China's digital industrial policies on the other hand were motivated by the need to have domestic rivals to foreign giants, by learning along with the private sector rather than being in the driver seat. Given the tensions of managing the role of the state, especially its subsidies in a confederation of states, the EU has instead focused on ensuring free and fair competition in the past decades, although more recently it has started to focus on developing European digital champions and lessening critical dependencies.

As its dominance is challenged by a rising China, there is a strong bipartisan support for industrial policy in the US with the Inflation Reduction Act (IRA) and the Creating Helpful Incentives to Produce Semiconductors and Science (CHIPS) Act. China on the other hand, with a changed approach from the 'hide your strength and bide your time' under Deng Xiaoping to greater assertiveness under Xi Jinping, has its Made in China 2025 policy complemented by Internet Plus, which is in turn reflected in its 14th five-year plan. The EU has several policy documents which reflect its ambitions to enhance its strategic autonomy and strengthen its technological leadership while leveraging its core regulatory competences. Its Digital Markets Act (DMA) seeks to tackle the network effects of large online platforms to ensure a fairer business environment, while the European Industrial Strategy aims to support the EU's twin digital and green transition and is complemented by a host of other regulations and policies.

Nevertheless, there are important differences in their approaches, with a significant element of competition. The race to build domestic manufacturing capabilities for semiconductors has become one of the major geopolitical fault lines between the US and China. Current US policies aim to support the domestic industry, but coercive sanctions also highlight the growth of a 'China-proofing' strategy in light of the current geopolitical tensions and tech war. In that sense, there are some similarities with the US-Japan rivalry in the 1980s when the US's hegemony was challenged. In contrast, to escape a potential 'middle-income trap', and counter its negative image of engaging in intellectual property theft, China has increasingly focused on building advanced domestic capabilities to transform

itself from the assembly and manufacture of individual components into a production hub of high-tech products. The EU has a distinct regulatory approach that seeks to rein in the powers of platform giants, and as mentioned above, lead on setting global norms and standards, while also pushing for more investments into building their own digital capabilities.

The effects of digital technologies and digital industrial policies in the above established powers has significant implications for developing countries. Rather than technological leadership which seems the objective of digital industrial policies among the established powers, developing countries need policies suited for technological catch-up. In most cases, their development needs may not neatly fit in any of the models followed by the established powers, and in fact their economic and political relations straddle multiple blocs to meet their varied developmental needs. While countries are increasingly adopting digital policies and regulations to govern the flow of data to achieve broader objectives such as national security or personal data protection, their links to development objectives of conventional industrial policies, of creating and shaping markets to raise production and productivity, are unclear.

Although digital industrial policies in established powers are more about innovation and building digital hardware and software, in developing countries the focus should be to acquire key (digital) technologies to support strategic sectors like agriculture and manufacturing. This is because digital technologies can be deployed to enable efficiency gains in production - faster and customised production processes, optimisation and waste reduction, and improved product quality and safety. This is necessary in order to avoid a further widening in the productivity gap between these countries and the established powers. This can be sought through greater linkages to lead firms in global value chains (GVCs) for technology transfer and incremental learning, rather than by creating national rivals to global giants.

Lessons can be drawn from rising powers such as India which has sought to innovatively balance competing objectives and priorities. Spurring digital innovation by using free and open-source software (FOSS), India's technological advances are embodied in its digital public infrastructure which provides government services through India Stack which is a comprehensive digital identity, payment, and data-management system. In contrast, the development of the digital economy in Africa will have to start by increasing access to the internet, with a focus on not just the consumption of digital technologies but also their productive use. From that perspective, the use of digital technologies to upgrade value chains has been limited in many African countries with structural challenges around infrastructure, finance, and a limited productive base. As mentioned above, navigating the current geopolitical tensions adds another layer of complexity and challenges for countries in seeking digital development for economic prosperity.

The European approach to digital sovereignty is increasingly evoked in EU foreign and security policy, as well as in the EU's wider international partnerships, but the EU remains vague about defining this term when using it at multilateral fora or in its relations with other countries. The domestic usage 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, a growing interest in supporting European businesses.

For more effective cooperation at the international level, working more closely with others in a collaborative and open-minded way. The EU would need to demonstrate how its policies back up its promise of supporting digital sovereignty in partner countries, and developing more respectful and mutually beneficial partnerships. At present, with intense 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 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.

In order to begin to do this, the EU should demonstrate consistency between the concept of digital sovereignty in its internal and external policies in line with the aims of the so-called "Geopolitical Commission." As it focuses more and more on industrial policy to respond to the geopolitical environment in which it operates, the EU should also integrate partner countries' interests and ambitions with regard to industrialisation in its engagement with them, supporting local technology hubs and funding research and innovation partnerships. It will also need to show an openness to compromising with, and learn from, partners across the world to come up with common approaches to key concepts that are central to the European approach to digital sovereignty, 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 given the vastly different development contexts and political interests.

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. Such cooperation, which entails cross-learning rather than a simple externalisation of EU regulations, can help avoid accusations that EU actors preach to partner countries in the Global South. Such an approach is beginning to emerge vis-a-vis certain partners, and could be extended to wider partnerships with the Global South.

We look 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. For instance, despite many differences, the EU and US largely enjoy a relationship of mutual respect, finding common cause where they do have clear shared interests, including increasingly in the desire to support investments in the Global South. Over the past years, the EU and India too have been strengthening 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. Despite its autonomy and arguably differentiated approach compared to the EU's GDPR, India stands to be a strong partner for the EU when seen through a holistic rather than a solely normative lens. The EU partnership with the African Union and key African states on digital transformation is very new and should entail a real negotiation around what digital sovereignty means for policymakers on each side and how this can actually be implemented in practice.