6

Digital Statecraft of Middle Powers

Tech Landscape and Digital Sovereignty in Brazil and India

Vashishtha Doshi* and Henrique Estides Delgado

6.1 INTRODUCTION

Power, in international relations, comprises autonomy and influence. Influence is the ability to affect others, while autonomy is the ability to prevent others' actions to affect oneself. As argued by Benjamin Cohen, "power must begin with autonomy, which generates a potential for leverage. Influence – the deliberate activation of leverage – should then be thought of as functionally derivative" (2019a, p. 23). In this logic, states must possess autonomy before they can influence those outside their borders. This materializes in the ability to enact policy at home without outside constraint or preserve and enhance a policy space. Autonomy then becomes a necessary, but not sufficient, condition for influence (Cohen, 2019a, p. 23). Great powers such as the US possess both autonomy and influence. However, middle powers such as Brazil and India do not possess both. Rather, they are seeking to enhance autonomy.

In this chapter, we argue that autonomy is a foundational element of digital sovereignty. Autonomy is important to preserve democracy and state security as well as to protect and advance local innovation and economic interests. This chapter argues that in a world of weaponized interdependence, middle powers such as Brazil and India have policy choices that can enhance their autonomy. However, having this policy space is not enough. In order to turn the potential for policy space into policy enactment, domestic politics has to align in a particular way. In this chapter, we argue that when the independence of institutions' interests are taken into or not usurped by the parliamentary process, we observe autonomy inducing policy enactment. We try to explain this using the case study of data localization policy in Brazil and India.

* Vashishtha Doshi would like to thank Henrique Estides Delgado, Aaron Schneider, and SUNY Press for graciously allowing parts of the chapter titled "Building Digital Sovereignty in Middle Powers: The Role of Intended and Spillover Effects" by Vashishtha Doshi from the edited book Popular Sovereignty in the Digital Age (2024) to be reprinted in this chapter.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

Farrell and Newman (2019) describe weaponized interdependence as an influence on the entire network of interdependence, arguing that it works through two mechanisms: panopticon effect and chokepoint effect. They classify panopticon effect as such where "states[1] that have physical access to or jurisdiction over hub nodes can use this influence to obtain information passing through the hub," while chokepoint effect involves "states'[2] capacity to limit or penalize use of hubs by third parties" (p. 56).

Middle powers,[3] with mid-level international power, capacity, and influence in the international system (Jordaan, 2003), do not enjoy the systemic ranges of action achieved and maintained by great powers; however, they still have the wherewithal to pursue autonomy and safeguard their sovereignty in narrower measures and fields. The paradigm of economic statecraft has largely focused on the actions, institutional setups, and structural asymmetries enjoyed by the great powers who utilize them for their own foreign policy goals (Narlikar, 2021). Much less attention is given to the role of middle powers such as Brazil and India.

This chapter seeks to answer two broader questions: (1) what agency do middle powers have in a world marked by weaponized interdependence to safeguard their digital sovereignty[4] and (2) how does domestic politics structure the outcome of this agency?

We seek to answer these two global questions using the case studies of India and Brazil. In the realm of technology, both countries are similar in the way their domestic industry is structured, yet we have observed key differences in policy outcomes. This chapter is an example of the agency and policy space middle powers such as Brazil and India have but the enactment is mediated by domestic politics. In short, this study provides an example of the missing link between capability and outcomes in middle powers policy, and how they can achieve autonomy even under conditions of weaponized interdependence.

To answer the above questions, first, we discuss the role of firms in weaponize interdependence by great powers, using the fields of finance and

[1] As of now, according to Farrell and Newman (2019), only the United States possesses both these capacities in the realm of finance and technology.

[2] For example, global financial interbank messaging occurs through the SWIFT network. Due to the preponderance of dollar in the world economy, only the United States can weaponize SWIFT messaging for its own foreign policy goals cutting the target country's access to the entire world's financial network as Iran found out in 2012. Thus, a multimember global organization can be utilized for US foreign policy goals.

[3] We define middle powers using Jordaan's (2003) definition as "states that are neither great nor small in terms of international power, capacity and influence, and demonstrate a propensity to promote cohesion and stability in the world system." We argue, according the framework of Cooper, Higgot, and Nossal (1993) and Holbraad (1986), that middle powers policy behavior is a product of their contextually located deliberate action emanating from their position in the world order.

[4] Utilizing Pohle and Thiel's (2020, p. 8) framework, we define the concept of "digital sovereignty" as the "idea that a nation or region should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment."

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

digital technology as examples. Second, we examine the variables along which middle powers can attain autonomy in the above two fields, thus strengthening their digital sovereignty. Third, we explore how the range of policy outcomes varies among middles powers due to the constraints and opportunities emanating from domestic politics.

Utilizing the framework set forth by Farrell and Newman (2019) and Cartwright (2020), we argue that great powers weaponize interdependence through their firms. They internationalize state power by exercising jurisdictional authority over their market-dominant firms. Within this overarching architecture, middle powers have agency to seek autonomy for themselves along a set of variables that helps block the most adverse effect of weaponized interdependence, that is, the chokepoint effect. We argue that data localization is one such policy through which middle powers can achieve autonomy from weaponized interdependence. Data localization policies help eliminate the chokepoint effect by keeping the jurisdiction over the stock of data at home. We argue that data localization then becomes a necessary but not sufficient condition on the path to state-led digital sovereignty. In this chapter, we inquire the reason for observed variation in data localization policy in India and Brazil despite similar domestic interests.

We define data localization as "mandatory requirements of local storage of data, whether exclusively or in the form of mirror data copies, thus fundamentally steering, and altering, data flows" (Bailey & Parsheera, 2018).[5] Brazil has no data localization policies, whereas India has a fractured outcome with sectoral data localization (Burman & Sharma, 2021).

In August 2023, India passed its Digital Personal Data Protection Act (DPDP Act). Through this act, India cemented the debate on data localization in the country. This act allows for cross-border transfers of data to all countries unless specifically restricted by the Indian government. Thus, India's data protection bill is now in line with Brazil's in removing almost all barriers to free cross-border flow of data. However, the key difference that remains and reinforces this paper's argument is that in passing the Bill, the Indian government did not usurp the data localization mandates set by sectoral regulators.[6] Section 16 (2) of the DPDP Act states, "Nothing contained in this section

[5] In practice, policies with regards to data localization differ widely. For example, China's data localization policies require Apple to store all iCloud data not only in China but on servers run by Chinese state-owned entities (Nicas et al., 2021). In Russia, data localization in practice means storing of Russians' data on servers located in Russia, but not necessarily on servers owned and operated by Russian state-owned enterprises (SOEs) as in China (Reuters, 2021). India's data localization mandates require only certain forms of data to be stored within India; however, the data is allowed to be transferred abroad for processing (Burman & Sharma, 2021).

[6] The DPDP Act continues to uphold sectoral data localization mandates set forth by the Reserve Bank of India (RBI), Securities and Exchange Bureau of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI), Ministry of Consumer Affairs (MCA), and the Department of Telecommunications (DoT).

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof." Industrial sectors can still maintain their own sectoral data localization mandates.

We argue that these divergent outcomes in data localization policies between Brazil and India stem from the difference in whether the interest of independent institutions was incorporated into the decision-making process. India's sectoral data localization stems from independent institutions allowed to exercise their jurisdictional authority without explicit interference from the political process. However, in Brazil, independent institutions' sectoral interests were subordinated to those of the Brazilian congress.

In this chapter, we argue that data localization is one such autonomy-inducing policy choice to enhance digital sovereignty. However, the availability of data localization policy is not enough. Domestic politics must align in a particular way to enact them through meaningful digital statecraft. The novelty of our argument is that we examine the role of middle powers in the world under weaponized interdependence. We argue that middle powers face two sets of constraints – the international sphere and domestic sphere (politics and institutional design) – that eventually determine the outcomes of their sovereignty enhancing policies.

6.2 US HEGEMONY IN FINANCE AND TECHNOLOGY

Our theoretical argument begins with an emphasis on the role of US hegemony. This hegemony is manifested here as extraterritorial exercise of digital sovereignty at global scale. In this section, we argue that the US – and as of now only it[7] – exercises hegemony in fields of finance and technology that are analogous and important for comparison. Section 6.3 will address how to limit this in order to build up the digital sovereignty of Brazil and India. We begin this section by listing the variables and mechanisms through which the US exercises power in the field of finance benefiting from the centrality

[7] Even though China is to some extent replicating the US strategy and challenging the latter's monopoly in these areas, the very consternation provoked by Chinese incursions is an example of an exception that proves the rule. China has reached autonomy and has different tools of influence, but the US still is in a different level in the fields of finance and technology. The other great power, the mighty political and economic network that is the European Union (EU), also has some important firms that serve as tools to project influence, but is still having to deal with the fact that European states, firms, and citizens are "gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment" (European Parliament, 2020, p. 1). The EU is still trying to secure "strategic autonomy in the digital field," something discussed around three building blocks: "(i) building a data framework; (ii) promoting a trustworthy environment, and (iii) adapting competition and regulatory rules" (p. 5).

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

of US firms in the global financial system, which may end up enjoying what this book considers as a form of corporate digital sovereignty or even acting as proxies for state digital sovereigns (Belli, 2022). The discussion on finance will be brief as finance is not the core topic of this chapter but a useful comparison. We then discuss the variable through which power resides in the technology industry and the centrality of US firms within it. Finally, we discuss how the US externalizes its power through the centrality of US technology firms.

The US can exercise influence through the networks that have been formed because of the dominant role of its firms in fields of both finance and technology (Babic et al., 2017; Birch et al., 2021; Farrell & Newman, 2019; Starrs, 2013). There is now substantial research on how the US is able to exercise influence over the international financial system through two distinct actors: public institutions (de Goede, 2021; Helleiner, 2019; Murau et al., 2021; Schwartz, 2019) and private activity (Fichtner, 2016, Fichtner & Heemskerk, 2020; Petry et al., 2019; Winecoff, 2015).[8] US centrality in both is reinforcing. For the purposes of our study, we highlight how the US is able to exert influence through the activities of its firms. The international financial system is a complex network that is hierarchical in nature, with the only core nodes being the US and UK (Fichtner, 2016; Oatley et al., 2013; Winecoff, 2015). This high level of international market dominance coupled with US authority over domestic firms allows the US to internationalize state influence through its firms (Cartwright, 2020).

Centrality of US firms exists in the technology sector as well (Starrs, 2013, p. 822). Out of the top 100 technology companies in the world, 35 are US firms (Forbes, 2019). Further, out of the top 100 websites visited in the world 60 of them are US firms' websites (Routley, 2019). None are Brazilian or Indian firms (Jawaid, 2023). "A huge fraction of the global data traffic is channeled through the servers of a handful of US companies" (Farrell & Newman, 2019, p. 64). Some estimates suggest that up to 70% of global web traffic passes through servers in Northern Virginia (Mekouar, 2020). Similarly, Google dominates worldwide search engine market share (over 85% market share). Facebook and other US firms dominate social

[8] It is interesting to note here that another kind of authority is emerging through the creation of private standardization bodies that regulate by proxy entire sectors (Belli, 2022; Bruner, 2008). The global regulation of credit risk through the creation of private credit rating agencies and the regulation of the domain name industry through the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) are just some of the examples (Sinclair, 2008; Bruner, 2008). However, it is important to note that home states of these private bodies can and do utilize the centrality of these private actors' regulatory position to satisfy state goals. For example, despite ICANN's removal from under the aegis of US Department of Commerce, it is still subject to regulation by the California attorney general's office and all federal laws that apply to nonprofit entities registered in the US. Should there be a need, it is not inconceivable to imagine US government mandating ICANN to deregister an enemy country's websites.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

media market share. Further, as these firms grow bigger, they will funnel more global data within their ambit. Majority of these firms' business model is dependent on extraction of value from personal data processing (Birch et al., 2021; Zuboff, 2019a). This requires the immense collection and storage of personal data, and then the ability to monetize it for profits (Birch et al., 2021, p. 9).

The global dependence on US technology firms, their need to accumulate data, coupled with US legal framework – which includes the lack of a general data protection law matched with legislation allowing both international surveillance and access of data treated or stored domestically and abroad by US firms – allows the US government to create a panopticon effect on global information flows.[9] As stated by General Hayden, former CIA director, "because of the nature of global communications, we are playing with a tremendous home field advantage, and we need to exploit this edge. We also need to protect this edge and those who provide it." (Hayden, 2006).

The Snowden leaks revealed how the US utilizes the dominant position of its internet firms to conduct mass surveillance in the world. At the time, there was an upheaval in Brazilian politics and diplomacy. In wake of the Snowden leaks, President Dilma Rousseff wanted all internet companies operating in Brazil to store data of Brazilian clients in the country (i.e., data localization) (Douglas, 2013). Cartwright (2020) provides many examples of how the US government has utilized the dominant position of its technology companies to create a panopticon effect. For some analysts, unless there is a decline in the usage of US digital technology companies for most of the global internet traffic and personal data, it seems highly unlikely that US's panopticon effects can be curtailed in any meaningful way. There is also the pathway for different jurisdictions to design stronger and better enforced regulation on local data, matched with enhanced investments in cybersecurity that curtail data leaks and cyberespionage. As Farrell and Newman (2019) describe – for reasons of the US's own industrial policy goals together with specificities of history and context – the US government has not yet turned this advantage of panopticon effect into more than small-scale chokepoint effect. However, it is not an inconceivable scenario where one day the US could order its firms to exercise a chokepoint effect on the data of extraterritorial entities (whether it be public or private).[10] As discussed earlier, the requisite recipe – concentration of data on US soil, US firm's market dominance, and legal framework – is in place to exercise this option at large scale with the potential of major disruption to others' national security, as well as economic and human rights.

[9] See Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. § 2701 (1986) and FISA Amendments Act Reauthorization Act of 2012.

[10] This scenario is actually not very far from what happened when Android was prohibited from supplying software to Huawei in 2019 (Quinn, 2019).

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

While we are not arguing that data in the possession of or passing through US technology firms is the sole basis of US's ability to weaponize interdependence, we believe that having US technology firms at the core of the global data economy – some providing services presented as "free" but in reality paid with data – is one of the ways in which the US maintains the upper hand in the digital age. Moreover, data concentration follows from such centrality and makes it impossible for other firms to compete.[11] Through a combination of centrality of US firms, provisions (and practice) for US government agencies to access data that flows within the ambit of these firms and willingness of the US to utilize this privilege to achieve state goals has meant that the US enjoys extraterritorial projection of its digital hegemony while other countries face constraints on their digital sovereignty stemming from this. Moreover, the levels of data concentration in a few US tech giants are such unsurmountable barriers to entry that even in US home markets other firms find it hard to compete. Hence, awareness about the importance to break these barriers and level the playing field are behind the efforts to enact data localization measures.

Currently, we can think of several other ways through which the US can weaponize interdependence.[12] For example, most of the world's location-based devices are connected to the US's GPS system. It is not inconceivable that the US can block a country's access to the GPS system.[13] Another variable is undersea cables. A significant amount of data that passes through US firms' servers in the US goes through undersea cables. It is possible that the US can utilize this privileged position to block access to these cables for certain entities. Protection of undersea cable is such a significant part of US geopolitical strategy that the country even forced a joint Facebook–Google undersea cable to not have a landing site in Hong Kong. The US State Department's Clean Network, an initiative publicly delineated in 2020, provides insight into the technology industry variables that the US considers geopolitically relevant. In short, there exists *potentiality* for the US to weaponize interdependence along other variables of the technology industry as well.

The above discussion delineates how the US exercises both forms of power – autonomy and influence – in the fields of finance and technology. And, in turn, middle powers have responded with measures to counter some

[11] See reasoning behind EU efforts to "open" access to US tech giants' data bases via the Digital Service Act and Digital Markets Act.

[12] Middle powers have instituted measures ranging from data localization to nationalizing the cloud to GPS alternatives (see footnote 14) to creating alternatives to SWIFT (such as China's CIPS and Russia's SPFS).

[13] In order to minimize the potentiality of weaponization of interdependence by the US, countries such as Russia (GLONASS), China (BeiDou), and India (NavIC) have deployed their own global navigation satellite system (GNSS) analogous to the US's GPS system and mandate that mobile phones sold in the country either have to run on their GNSS or both GPS and domestic GNSS. Russia ("GLONASS to be," 2013); China (Global Times, 2020).

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

of these variables of hegemony such as developing their own alternatives to GPS, nationalizing the cloud, developing more subsea cables, and promoting data localization measures. In this section, we have focused on the role of US firms as conduits through which the US state can exercise power and highlighted some of the measures undertaken by middle powers. Combining the concepts of Farrell and Newman (2019) and Cartwright (2020), we argue that the high international market dominance of US firms in finance and technology combined with US jurisdictional authority over them allows the US to weaponize interdependence (both panopticon and chokepoint effects) over the entire network. In Section 6.3, we begin to look at how middle powers operate under this environment.

6.3 CONSTRAINTS AND OPPORTUNITIES FOR MIDDLE POWERS

In this section, utilizing the "dual faced nature of power" framework, we discuss the opportunities and constraints faced by middle powers as it relates to US hegemony. We briefly discuss the strategies middle powers utilized in the field of finance. Then, we argue middle powers have similar opportunities in the field of technology. Finally, we look at one such opportunity – data localization – and how it can enhance the autonomy of middle powers.

Power hierarchies pervade the international system (Lake, 2011), in which a set of countries are engaged in subordinate relationships with the hegemon (Lake, 2007). International hierarchies exist in various facets of the international economic system as well (Cohen, 2000). If hierarchy was a pyramid with the US at its apex, the countries that occupy space between the apex and bottom would classify as middle powers. Our understanding of middle powers is not that dissimilar to how semi-peripheries are described in world systems theory (Wallerstein, 1976). Middle powers are still engaged in a subordinate relationship with the hegemon but have significant market dominance in their home countries and presence in the countries surrounding them (Wallerstein, 1976, p. 464). The difference is that instead of deterministic outcomes – derived from an "antipossibilist" policy orientation as once criticized by Hirschman (1980) – we emphasize further possibility of agency and statecraft as able to create apertures and innovation in the system.

Considering the dual faced nature of power – autonomy and influence – these countries certainly cannot exercise influence in fields of finance and technology like the hegemon. However, due to their large internal markets, relevant levels of human capital, and financial capacity they are not completely subordinated either.[14] They still retain a modicum of agency

[14] Countries such as Mexico, Brazil, India, and Indonesia would be perfect example of such middle powers. They each have over $1 trillion in GDP, a large population, the requisite technical know-how, and large internal markets.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

(Narlikar, 2021). This means that middle powers can ward off potentially adverse effects emanating from the panopticon and chokepoint effects exercised by the hegemon on the network. However, they are not able to influence the entire network as the hegemon does. Their power is thus only limited to autonomy and not influence, that is, middle powers can carve out policy spaces in a world of weaponized interdependence should they want to bear the costs. In essence, they have the potential to safeguard their sovereignty but not have the ability to undermine the sovereignty of others by influencing the network.

Middle powers have utilized defensive financial statecraft to shield the domestic economy from external financial pressure (Armijo & Katada, 2014a, p. 8). They have utilized the strategies of capital controls, state-owned banks, and foreign currency reserve accumulation “to shield their country not against a particular foreign state but rather against systemic influences, whether coming from global markets or from the rules and institutions of global financial governance” (Armijo & Katada, 2014a, p. 169). The authors label this as “defensive but systemic financial statecraft” (Armijo & Katada, 2014b). As we have seen before, US financial institutions are central to the global financial system, and US interests are executed through them. Thus, even if the actions (under the measures that constituted systemic but defensive financial statecraft) were not targeted against a particular government, they amounted to carving out policy space (autonomy) from the weaponized interdependence effects of the US.

In the technology industry, some of the most prominent variables through which countries have sought to limit the effect of US’s weaponized interdependence include: promoting data localization (Burman & Sharma, 2021), developing other GNSS, blocking access to US firms in the home market, indigenizing the cloud, and developing an entire tech ecosystem largely independent of the US system as in the case of China. Among middle powers, Brazil partnered with Europe to create the subsea cable connection for internet traffic called EllaLink that connects the two continents directly to bypass US surveillance (González, 2017). The list of variables is by no means exhaustive, but indicative of how countries have sought to undermine the effects of US’s weaponized interdependence in digital technologies.

For the purposes of this chapter, we are looking at one variable – data localization – and how it connects to US’s weaponized interdependence.[15] Countries that enact data localization policies can jurisdictionally assert control of the data stored within the country, which means that the access to and processing of data would be governed by local laws. The physical and legal

[15] The US is used here as an example, but the same set of weaponization of interdependence dynamics can be potentially enacted by other foreign powers. China is the closest that comes to US’s example, but certainly there can be more.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

shifting of jurisdiction of the data from the US to the home country allows for the minimization of US extraterritorial reach.

Data localization would severely limit or remove the ability of foreign states to block access to data generated by the countries themselves.[16] Key mechanism through which the chokepoint effect works – states' capacity to limit or penalize use of hubs by third parties (Farrell & Newman, 2019) – would be limited as the jurisdictional control over hubs of information would become either transient or nullified. If the dominant internet firms in the concerned countries are still US firms, data localization policies would largely limit although perhaps not block entirely the panopticon effect as the US can still conduct surveillance operations through these firms. Putting this in generalized economic terms, the US would still be able to access the flow of data (panopticon effect), but data localization policies would limit access to the stock of data, thus curtailing the chokepoint effect. But, if the dominant internet firms in the concerned countries are national champions, then both the chokepoint effect and the panopticon effect would be curtailed or eliminated as hubs of information flow would be outside of US jurisdiction and so will be the storage of the stock of information.

The physical location of where data is stored is so important that in fact there are proposals in the US congress pushing for the US to follow explicit data localization strategies while using US economic diplomacy to advocate for the opposite abroad. Thus, access to global personal data is important not only for US industrial policy but also for the exercise of weaponized interdependence over the network. Hence, data localization has become the heart of global information geopolitics. Thus, we argue that attaining digital sovereignty for middle powers would be impossible without the curtailment or elimination of the most basic exposure to weaponized interdependence, that is, the chokepoint effect. Data localization policies then become necessary but not sufficient conditions to attain digital sovereignty for nation-states.

[16] From an economic point of view, data localization would help ameliorate some of the inequity that is generated due to the enormous value captured within servers located in the US servers while not paying any taxes in the countries where data is extracted. However, it seems that countries such as India who are putting in mixed data localization measures are not intent on forcing foreign cloud companies (who host would most of the data on their servers located in India) to share their data with local market players, so that the local players are able to extract value and grow. But, rather, they are mandating localization because of lack of access to data (if needed) in criminal investigations (since the US MLAT process is very arduous) and for national security rationales. For countries such as India, it is more about ease of access (a national security concern) than an economic value extraction concern. Please see page 41–42, Report of the Joint Committee on the Personal Data Protection Bill, 2019 published in December 2021. In all, in both India and Brazil, the institutional framework of data privacy would need to be reviewed for a further step of creating data pools to be accessible and commercially exploitable for the advancement of local firms, as well as research and policy institutions.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

6.4 OVERVIEW OF DIGITAL TECHNOLOGY INDUSTRIES IN INDIA AND BRAZIL

In the area of digital technologies, a characteristic of middle powers is manifested by the presence of relevant domestic players in a given industry. These countries can carve out some space for their firms at the frontier of the expanding digital economy. A closer look at the landscape reveals how a pattern of partial autonomy emerges, one in which business sectoral interests are essentially similar between India and Brazil.

Tech landscape in any country can be analyzed at three levels: infrastructure, multi-sector platforms, and single-sector platforms. While this classification is not perfect, it does allow us to group services provided by different internet companies into relevant and comparable bins across countries. Before beginning the discussion of these three layers, it is important to note that the boundaries between these layers are distinct but porous, activities of firms can often include functions in all three layers. For example, in general, there has been trend toward vertical integration between access providers and content and app providers at least since the late 2000s (Guo, et al., 2010).

Infrastructure refers to the core of technology, the backbone on which other services rest. This includes not only telecom providers but also core operating system providers, cloud service providers, and logistical providers (UNCTAD, 2019). It also includes the "under the hood rails" of certain key economic activities such as payments. The middle level is what we colloquially think of as multi-sector platforms. They provide a sort of virtual meeting place (or marketplace) for actors to interact and conduct commerce (Belli, 2019). Finally, the outer layer is composed of other consumer facing digital services that are single-sector platforms.

Some key roles of platforms are: the ability to create and shape markets, benefit from "network effects" (where the value of the service increases with the number of users), and capturing and monetizing value through data accumulation (Belli, 2022). Using this standard definition of platforms begs for further explanation about the distinction between our usage of the term "multi-sector platforms," and "single-sector platforms." After all, both are consumer facing. However, there are distinct analytical differences. In this chapter, we refer to multi-sector platforms as the (i) e-commerce companies involved in the transaction of a wide range of products and services and (ii) platforms of digital banking, financing, and instant payment. Often (i) has (ii) as an important and growing part of their business. Platforms – both the internationally established large ones such as Walmart and Mercado Libre and the rising ones still inscribed to a domestic market such as Magalu – are either actually or potentially at a higher level of data-driven power than other consumer facing applications and websites that are single-sector platforms.

Moreover, platforms are at a lower level than core infrastructure, even though some players at the core also occupy multi-sector platforms and

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

single-sector platforms services. For example, there is certain level of irreplaceability that happens due to positive feedback loops between organization of consumer behavioral data across different sectors on the one hand and data accumulation and targeting on the other by Amazon that is not replicated by Uber or Lyft. Khan (2017) argues that Amazon's structural dominance stems from, inter alia, expansion into multiple business lines (p. 754), its logistics dominance and leveraging of that to disadvantage rivals (p. 774),[17] and premature acquisition of rival firms (p. 768). Further, regulators have found that once Amazon moves into a particular business line it disadvantages sellers on its platform and organizes consumer behavior toward its own product by gleaning off consumer data on their rivals' products, eventually leading to rivals leaving that business (Mattioli, 2020). This entire hydra-like business strategy is cemented by accumulation and targeting of data that organizes consumer behavior in ever more sectors on Amazon's platform, further entrenching the irreplaceability of Amazon. Nothing of this sort exists with, say, a company like Uber.

Uber is a single-sector platform. Consumers are able to switch out of Uber relatively easily, should they want to, into a rival service without facing significant and sometimes irreplaceable switching costs that they would with Amazon. Thus, in our classification, Amazon is a multi-sector platform, whereas services such as Uber are single-sector platforms. This distinction between the traditional broader definition of platforms and how we outline their functioning is important to keep in mind as it highlights an essential difference between digital market players in India and Brazil, which we will outline in the following sections.

6.4.1 India's Tech Landscape

India's tech landscape is populated with a collection of US big tech firms, Indian conglomerates, a vibrant start-up ecosystem, and digital public infrastructures (DPIs).[18] DPIs, as the term suggests, represent the digital variant of nonexcludable and non-rivalrous public infrastructures (Sukumar, 2021). Like other infrastructures, DPIs are the tools and systems required to make digital life function. US big tech firms are the only ones that span all three layers of the tech landscape in India.

6.4.1.1 Infrastructure Level

Three US tech giants dominate in India: Google, Facebook, and Amazon. They provide cloud infrastructure for businesses and the government. Google Cloud and Amazon Web Services (AWS) dominate India's cloud market.

[17] The EU and Italian regulators judge this practice anticompetitive and hit Amazon with massive fines for this precise reason (Bodoni et al., 2021).

[18] We define infrastructures as the technologies and systems necessary for society to function. Infrastructures are backbones on top of which other services can be provided.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

Cloud, despite the oxymoronic name, is located in a physical environment. It requires servers, coolers, and an entire industrial setup. Without cloud services, it would be impossible to imagine a networked tech economy where even small players can rent space on these servers to start their online presence. AWS has the largest contract with Indian governmental agencies.

Finally, Google's Android is the dominant mobile operating system in India. Most Indians who have a connection to the internet do so through their mobile phones. Google's Android has a 96% market share. This means that Indian businesses must continuously monitor their compliance with Google's standards, which indirectly allows Google to play the standard-setting role within India's technology industry. Furthermore, this dominance in operating system deployment allows Google to exclusively deploy its platforms.

The only Indian companies that possess infrastructural roles in the technology sector are telecom operators Reliance Jio and Bharti Airtel. The third telecommunications company – Vodafone Idea – is still majorly owned by UK's Vodafone. These three telecom operators deliver internet connection to most Indians. In fact, Reliance Jio has been credited for single handedly bringing 400 million previously disconnected Indians online in a span of two years and for dropping India data charges to the lowest in the world (Purnell, 2018).

However, such achievements are not enough and do not cover enough issue areas to really propel the vision of Digital India. This ambitious agenda stands on three legs: Jan Dhan (roughly translated to mass financial inclusion), Aadhaar (unique identity provision to every Indian to avail of government services), and Mobile. India calls this the JAM trinity (Ravi, 2018). To provide infrastructural support for the J & A aspect of the JAM trinity, the government decided to step in with the provision of DPI. This is also colloquially referred to as the India Stack.[19]

6.4.1.2 Multi-Sector Platform Level

The second layer of the tech landscape is populated by multi-sector platforms. The whole idea of an internet platform is to provide centralized spaces for multiple parties to interact in a trusting manner. However, platforms do not act in a neutral manner (Mattioli, 2020). Platform power rests on *data-centric models* and *network effects* (Rolf & Schindler, 2023). Even if they are providing a

[19] "IndiaStack is a set of APIs that allows governments, businesses, startups and developers to utilize an unique digital infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery. It consists of 4 layers: presenceless layer, paperless layer, cashless layer, and consent layer. Presenceless layer is where a universal biometric digital identity allows people to participate in any service from anywhere in the country. The paperless layer is where digital records move with an individual's digital identity, eliminating the need for massive amount of paper collection and storage. Cashless layer is where a single interface to all the country's bank accounts and wallets to democratize payments. Consent layer allows data to move freely and securely to democratize the market for data." For more on India Stack, please see www.indiastack.org/.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

service presented as free, multi-sector platform companies collect vast troves of data on the user, the access to which they sell to third parties and use for many purposes. The more users utilize a multi-sector platform, the more data a multi-sector platform collects, which in turn allows it to outcompete rivals through better product design and more efficient operations. Network effects boosted by 'first-scaler advantage' propel market dominance (Khan, 2017). Once achieved in one sector, market dominance enables companies to influence other sectors through vertical and horizontal integrations. They can leverage their existing user base and accumulated data intelligence to enter new markets. This market power is further entrenched if multi-sector platforms end up providing infrastructural services. As noted earlier, four US firms occupy both spaces in India. However, Indian players do not have a significant presence at the platform level of the tech landscape.

Facebook and its subsidiary WhatsApp's largest user base is in India. This means most Indians converge on a singular digital interface daily and communicate with each other. If users want to switch to another messaging platform, it becomes harder as they would lose access to all their centralized spaces for connections. This captive audience in India and elsewhere gives FB immense user data and an attractive centralized portal for other service providers to link up. Similarly, Amazon and Walmart not only connect buyers with sellers on their portals, but they are able to offer other services that keep users engaged on their respective multi-sector platforms. "Currently, Walmart-owned Flipkart and Amazon dominate the Indian ecommerce space with around 60% share between them. Reliance is a distant third" (The Economic Times, 2023).

Finally, even when these multi-sector platforms allow third-party business to link and do commerce, the multi-sector platforms eventually learn enough about their third-party sellers' services and mimic to undercut them (Mattioli, 2020). This centralizes consumer behavior toward the multi-sector platform. For example, in India, Amazon offers payment services (Amazon Pay), operates an ecommerce platform (Amazon.in), is one of the largest players in the cloud (AWS), offers insurance (Amazon Insurance), operates a digital banking platform, offers a food service delivery, and so on. All these services are then discounted for its Indian Prime subscribers. Thus, once an Indian user enters the Amazon ecosystem, it would be harder for them to escape for Amazon has now become their banker, payment processor, insurer, food deliverer, grocer, and shopper.

Similarly, Google's infrastructural dominance through the Android operating system allows it to nudge users toward using Google Suite of services and the Google Play Store. All Android phones come preloaded with apps ranging from the functional (such as Gmail, Google Drive, and Google Calendar) to the financial (such as Google Pay). Further, to utilize an Android phone, users must create a Google Play account to download other apps. This gives Google immense leverage over consumers and businesses (obey Google mandates or face being deplatformed). In this way, Google gets to set the terms of access

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

and exclusion to most internet-connected Indians and Indian businesses (Kalra & Bhattacharjee, 2020). Without access to Google Play Store, app-based businesses cannot function, and most Indians are only connected to the internet through mobile phones and their apps.

6.4.1.3 Single-Sector Platform Level

At the single-sector platforms level, except for the payment space, India's technological landscape resembles a vibrant competitive market. As one journalist remarked, "this is Indian tech's Belle Epoque." There are homegrown apps in fierce competition with foreign customer-facing apps.

For example, while Netflix and Disney's Hotstar are dominant in the streaming services, Indian players such as Eros with their extensive library of local content have begun to carve out space for themselves. In the education technology sector, homegrown, venture-capital backed BYJU'S is one of the most valued firms in the world. Similarly, the music streaming service provider Gaana now has more listeners than Spotify. At this level of tech landscape, some Indian firms are not just dominating the local market but are competing with Silicon Valley and Chinese behemoths in overseas markets. For example, OLA, a ride sharing app, is now available in Australia, New Zealand, and the United Kingdom. Similarly, OYO rooms, a hotels-aggregator, has successfully expanded in the US.

Just by looking at market share, this space looks like a competitive environment between homegrown startups and American tech giants. Finally, the Indian state does not have any DPI at this level.

6.4.2 Brazil's Tech Landscape

This section overviews the industrial organization of the data economy in Brazil and traces the relationship between economic statecraft and the structure of domestic capital as this relationship evolves and carves out some room for market participation in Brazil's dependent development model–that is, one that is dependent on foreign players. Special attention is given to businesses to which data localization is potentially relevant, as is the case of digital financial transactions and e-commerce in Brazil.

6.4.2.1 Infrastructure Level

Brazil is highly reliant on US and EU core-level providers. In cloud computing, the demand for cloud services rose significantly due to the COVID-19 pandemic, speeding up a trajectory where key players are well positioned to turn products into services, create revenue, and further feed the data economy with granular information. The threefold basic division of cloud computing is represented by the provision of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The five largest players in the world include four US companies – Amazon (through AWS),

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

Microsoft (through Azure), Google Cloud, and IBM – and the Chinese firm Alibaba Cloud. Together, these five are reported to have two-thirds of the world's cloud infrastructure services market.[20] While Amazon dominates IaaS by far – and IaaS is often regarded as the core of cloud and its most promising part – Microsoft is the leader in SaaS, where it is followed by a group of the traditional Silicon Valley players plus Germany's SAP. The main players of cloud computing in Brazil are the same.

While in Europe there is some action to promote local players in cloud computing, that understanding was not reached in Brazil yet. In Europe, the Gaia-X project seemed to add a twist in the EU's long-lasting strategy to simply regulate the digital world. With Gaia-X, the EU affirms that valuable cloud contracts and data should remain within the bloc for both security and economic reasons. Even though the pursuit of data sovereignty through the networked system of cloud providers envisioned by Gaia-X extends participation to players from outside Europe, it is carving out some space for local players, including European players active in the telecom sector in Brazil. Telecom providers such as TIM (from Italy) and network infrastructure providers such as Ericsson (from Sweden) are involved with Gaia-X. They are also involved with the implementation of 5G, which has a cloud-native architecture. TIM for instance is migrating all content from its Brazilian data centers to cloud operated by Oracle and Microsoft.

In all, EU's General Data Protection Regulation (GDPR) and Gaia-X initiatives have a demonstration effect on digital policies in Brazil, not only serving as an inspiration for different actors interested in strengthening the Brazilian digital economy, but also allowing normative diffusion to occur through market leaders operating in both EU and Brazilian markets. In addition, EU's global digital footprint is also enhanced by norm-building exercises such as the "EU-Brazil Digital Economy Dialogue" (European Commission, n. d.). In practical terms, EU's digital sovereignty practices have considerable influence in Brazil. There is also infrastructure underway to serve this influence strategy. In 2021, the submarine cable EllaLink – financed by the EU with the explicit purpose to link the bloc with Brazil to bypass US surveillance – was inaugurated. This new network connects, among other things, cloud services on both sides of the Atlantic.

In the area of mobile operating systems, similar to India, Google's Android is the dominant player in Brazil with 81% of market share. The remaining market share is mostly controlled by Apple's iOS. In 2022, 62% of Brazilians access the internet exclusively through their mobile phones (CGI, 2023). This means Brazilian app providers must continuously monitor their compliance with the standard-setter Google. This is exacerbated by the zero-rating practice that provides free internet access to users under the condition of limited access to a small number of websites or subsidy via ads. The main player is

[20] Microsoft, Salesforce, and Adobe are leading the SaaS (Software as a Service) cloud market.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

Facebook, which attempts to set the standard for communication in a country while collecting personal data from zero-rating users. While India promotes a stronger defense of network neutrality on the basis of which Facebook's zero-rating service has been rejected, Brazilian regulators have been adopting the controversial rationale that zero-rating does not imply a violation of network neutrality (see Belli, 2019).

Finally, nowadays Brazilian telecom has three large players at the national level: they are subsidiaries of Italian (TIM), Spanish (Telefónica), and Mexican (América Móvil) multinationals.

6.4.2.2 Multi-Sector Platform Level

While Brazil is not an exception to foreign dominance in the infrastructure area, local platforms associated with big tech players have carved out some space for themselves in e-commerce and fintech. For example, Magazine Luiza, a retailer with a much bigger market share than Amazon in Brazil, uses Google Cloud technologies to boost its e-commerce platform.

Fintech is advancing in Brazil under the guidance of the Central Bank of Brazil. While the country's central bank allowed Facebook's WhatsApp to initiate financial transactions, it granted permission only after the creation of the Brazilian central bank's own instant-payment system Pix. Recognizing WhatsApp's largest user bases are located in India and Brazil, where WhatsApp's first-mover advantage could potentially lead to its dominance in fintech, the Central Bank of Brazil helped promote broader competition in this area by launching Pix first.

In terms of access to bank accounts, most providers are local. Although fintech expanded in Brazil, 40% of its economically active population still did not have a bank account before the 2020 pandemic. That was drastically changed during the COVID-19 pandemic when welfare payments were attached to the creation of a digital bank account in a state-owned bank CAIXA. It remains to be seen if such digital bank accounts will be used in the future as a comprehensive move toward digital banking and financing in the country.

The Central Bank of Brazil is overseeing three important developments in the country's financial system: the creation of Pix, the issuance of digital currency by 2024, and the Open Banking environment. The latter is another pro-competitive policy reform to reduce information asymmetry among market participants through the sharing of data, thus facilitating innovative digital financial services.

Brazilian platforms differ from their Indian counterparts in certain aspects. For instance, although the supermarket/grocery side of retail is controlled by French players Carrefour and Casino, both online retail and delivery services are dominated by Brazilian players. Firms such as Magazine Luiza, Via (through brands such as Casas Bahia), B2W (through brands such as Americanas and Submarino), and the Argentine Mercado Libre are competitive, even though Amazon arrives with a capitalization that only the world's largest retailer has. However, these online retailors all rely on US technologies to structure their

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

e-commerce platforms. In all, local firms are once more trading "the rents associated with state protection of the local market for those associated with their transnational corporate allies' proprietary technology and global market power" (Evans, 1995, p. 16). However, this time, instead of the state offering protection in the local market, what local firms have to offer is their market shares based on a history of accumulating data and information about the local consumer base.

In the immediate post-WWII era, the Brazilian government deliberately aligned domestic policies with international capital within a growing neoliberal context, allowing Brazilian private capital to associate with leading transnational corporations that would retain the lion's share. Even though this association is once more marked by imbalance, it allows these local businesses to flourish into the next phase of capitalism, evolving into a full-fledged digital economy. What were automotive products in the 1950s and 1960s,[21] now is the data-driven and ICT-controlled knowledge economy in which finance and digital technologies are increasingly merging.

Brazil and India remain *intermediate* cases between predatory states and efficacious developmental states as studied by Evans (1995). They are *intermediate* cases because some "examples of successful intervention could be found even if the broader state apparatus did not approximate the developmental state model" (Haggard, 2018, p. 42).

6.4.2.3 Single-Sector Platform Level

At this level, Brazil's situation is similar to India's in terms of the local competitiveness and greater margin for innovation. Customer-facing apps are created on a competitive basis both to reach niche markets and to compete in larger ones. Even though the most used apps belong or end up being purchased by big techs, venture capital still boosts some local apps. However, different from India, fewer apps have reached one billion dollars in value in Brazil. Among those that do, there is one for general delivery (Loggi), one specifically for food delivery (iFood), one for car hailing (99), which was acquired by the Chinese vehicle-for-hire company Didi in 2018, and one fintech (Nubank). Nubank, which is mainly owned by international investors, is the most valuable unicorn with headquarters in Brazil and has disrupted the very profitable banking establishment.

Google's YouTube is the number one platform to watch videos online in Brazil. In terms of paid streaming services, local player Globoplay has the most subscribers; Netflix comes in second. Globoplay, however, faces limitations to expand to international markets because most of its content is not in English.

[21] Automotive industry was at the core of Brazilian industrialization strategy. The arrangement that would be called the triple alliance (see Evans, 1979) would coordinate state capital and private domestic capital with foreign direct investment (FDI). In this alliance, SOEs produced the heavy inputs necessary to the foreign-owned automotive plants, while the domestic private sector would provide downstream services as well as a network of component suppliers for the factories ran by the multinationals.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

6.5 DATA LOCALIZATION IN INDIA AND BRAZIL

In the digital technology landscape, access to stock and flow of data is of the utmost importance. The stock of data allows technology firms to create better suited products toward consumers, which then creates a network effect of consumer behavior on that platform – the flow part. These two aspects of data work in positive feedback loop that entrenches bigger players at the expense of smaller ones. Beyond high-quality and creative engineering and programming, there is a *quantitative* aspect moving the mechanisms of the digital economy, which gain and sustain advantage through a series of tipping points and accelerating feedback loops (Lee 2018). Complementary, contextual, tailored data is also important. If one wants to put in place microlending apps in Rio de Janeiro or self-driving cars in Bengaluru, specific data from these places will always be superior to all possible data from the rest of the world (Lee, 2018). Accessing and amassing data, both in quantity and in quality, is thus the essence of platform and customer-facing dominance in technology.

Accessing and amassing data acquired new importance for statecraft as well. Beyond the idea that "war made the state, and the state made war" (Tilly, 1975, p. 42), the formation of states is also intrinsically linked to administrative institutions such as the *census* and other myriad of data-driven decision-making mechanisms, which serve as *precondition*s for the Weberian state (Gerth & Mills, 2009). It is no surprise why great powers such as the US and aspiring great powers such as China adamantly defend their advantage in ICT and digital technologies given what is at stake.

Data localization requirements have now appeared in the government's toolkit of actions to boost a country's tech landscape while guaranteeing levels of data sovereignty that serve goals ranging from security to guardrails for local business and economic interests (Cory & Dascoli, 2021). By itself, data localization does not guarantee an upgrade for the tech sector. However, determining that certain data generated in these countries should be stored domestically – even if some could be replicated abroad – can be part of digital policies that seek to enhance both cybersecurity and data sovereignty (Cory & Dascoli, 2021). Sections 6.5.1 and 6.5.2 explain data localization (or lack thereof) policies in both India and Brazil, and the reason for observed variation.

6.5.1 Data Localization in India: A Fractured Outcome

Countries such as India that do not have any domestic multi-sectoral platforms are placed at a disadvantage. Once a foreign multi-sectoral platform becomes relatively successful, the onset of network effects will privilege it over other domestic entities. Birch et al. (2021, pp. 5–6) explain how network effects coupled with exploitation of data allows for a "winner takes all" market. Multi-sectoral platforms combine network effects with exploitation of ever-expanding data within their ambit to utilize advantages from one aspect

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

of their business to entrench consumer behavior in another aspect of their business. For example, Walmart's Flipkart had such a dominance in e-commerce in India that because of network effects on its platform it was able to leapfrog an Indian payments player like Paytm to quickly become the top three payments processors in the country. This bleeding and spreading of dominance into more and more sectors of the economy is what has alarmed India.

India has pursued to limit this loop and privilege of big foreign platforms and thereby limiting the chokepoint effect of US's weaponized interdependence by undertaking data localization policies. India is accused of using "data localization to merely entail a transfer of power to domestic elites and contribute to strengthening India's profile and power in the community of nations" (Kovacs & Ranganathan, 2019, p. 20). The authors argue that policymakers in India "have constructed data as a primarily economic resource to be used in the service of economic enrichment of the country" (Kovacs & Ranganathan, 2019, p. 21).

Despite the overwhelming desire to be a technological powerhouse and limit the chokepoint effect of the US's weaponized interdependence, India has avoided undertaking sweeping data localization measures. What has led the Indian government to make this policy choice?

Before we begin the analysis, it is important to see how India's data storage landscape is governed. As discussed earlier, in August 2023, India passed the DPDP Act. This Act removes all constraints on the free flow of data across boundaries (bar some countries). However, as noted earlier, Section 16 (2) of the DPDP Act allows for independent regulators to enact data localization mandates and cements the mandates already put in place by sectoral regulators. Thus, the main characteristic of India's data localization landscape is sectoral fragmentation. India already has data localization requirements placed through a number of sector-specific measures. Burman and Sharma (2021) compile ten sectoral data localization initiatives in place. They include "payment systems data (Reserve Bank of India (RBI), 2019), subscriber data in the broadcasting sector (Department of Communications & Digital Technologies, 2021), and insurance policyholder data (Insurance Regulatory and Development Authority of India (IRDAI), 2017)" (Kovacs & Ranganathan, 2019, p. 16). Policies that mandate data localization are underpinned by two main considerations: one is Criminal Investigation and Prevention and the other is Economic Gains. But, their effect is in limiting US's weaponized interdependence effects.[22]

So how did this fractured landscape come about? If the Indian government has been aware of the monopolization of data on foreign platforms entrenching their dominance, why did it not pursue a full-scale data localization? In our view, the Indian government tries to strike a balance between appealing to the desires of its own population with demand to access global

[22] We have explained how data localization would amount to limiting of US's weaponized interdependence effects earlier in this chapter.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

standards of tech lifestyle and safeguarding against punitive measures from external actors, chiefly the US.

The interests of domestic conglomerates and government that tend to be in favor of data localization and American tech giants that assume an anti-data localization stance interact through India's institutions. For instance, the Indian supreme court's judgment in *Puttaswamy* v *Union of India* (2017) enshrined that every Indian has the right to privacy. This has meant that interests of both these domestic conglomerates and American tech giants must fit within the framework of privacy. Further, a few independent institutions in India took cue from the judgment to pass their own data localization mandates, namely RBI, SEBI, IRDAI, MCA, and the DoT. This is a key difference vis-à-vis the Brazilian case. In the Brazilian case, the enactment of the data protection bill by the Brazilian congress subsumed the interests and mandates of sectoral regulatory agencies within it; however, in India, the interests of independent regulatory agencies were not subsumed under the DPDP Act. Furthermore, a plan was in the works for localization of health sector data as well, but the proposal has now been withdrawn since the health sector does not have an independent regulatory body like finance or insurance does (Bailey & Parsheera, 2021, p. 139).[23]

So, as we proceed with the complex nature of interactions, we see that the interests of the foreign businesses are getting more and more constrained by the effect of exogenous institutional diktats informed by macropolitical constraints. On the other hand, the need to access funding for elections by political parties from domestic conglomerates (Bardhan, 2023) further fractures this dichotomy (Indian institutions' independent interests and the need to carve out spaces where domestic conglomerates are able to garner some of the user-generated data to compete with American Big Tech). The promotion of India's Reliance Jio into e-commerce and associated IT services can be well understood as a state strategy to promote national champions (and compete against foreign companies) (Subramanian & Felman, 2022).

Further, the impetus behind creating the Data Empowerment and Protection Architecture framework[24] can be viewed through the lens of protection of privacy as guaranteed by the Supreme Court of India, but also as a way to create business sector development opportunities for local firms by carving out lakes of data for them. Regardless of the impetus, the effect of such data localization policies would be the limitation of US's weaponized interdependence effects. While we use this as an example in one issue area,

[23] "The draft Digital Information Security in Healthcare Act, 2018 (DISHA), a now withdrawn proposal, this bill sought to create scope for the proposed National Electronic Health Authority to impose localization requirements with respect to digital health data" (Bailey & Parsheera, 2021, p. 139).

[24] It is a consent-based sharing that reduces the possibility of firms to create walled gardens of data. It allows for individual to permit sharing of their own data held by one firm to another one. One can think of it as a UPI-style infrastructure layer that will facilitate consent-based sharing of personal data.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

such a framework can be applied to other areas of the technology landscape in India to trace how a particular outcome has come about.

6.5.2 Data Localization in Brazil: A Dependent Outcome

The debate about whether Brazil should move toward requiring internet-transacted data related to Brazilian citizens to be stored in the country gained momentum following the Snowden revelations in 2013 about spying activities pursued by the US National Security Agency (NSA). Whether characterized as a whistleblowing about uncivil and undiplomatic panopticon activities or as a treason promoted by a contracted agent against the principal, it is clear that an US agency was dedicated precisely to achieving panopticon advantage. Snowden revelations not only demonstrated the US will and technological capabilities to collect intelligence globally but also ignited recalculations regarding (inter)national security by national governments around the world.

The Brazilian Civil Framework of the Internet, or Marco Civil da Internet, was a bill proposed to the Brazilian Congress by the executive branch of the government in 2011 after extensive multistakeholder discussions held since 2009 under the Ministry of Justice's coordination. When the bill began to be considered in the Chamber of Deputies – the lower house of Brazil's Congress – 36 other projects were attached to it, including some that had been pending in the Chamber since 2001. Following the 2013 Snowden incident, the executive branch used a legal device to request urgency in the appreciation of the bill by the legislature, while legislators close to the executive branch included in the bill a data localization mandate. That was a clear turning point whose impacts will likely go beyond the mere Brazilian Civil Framework of the Internet and all other internet-related legislations that have been approved since then.

At the time, the representative serving as bill's rapporteur considered the data localization rule as a "political answer against a political act that violated our sovereignty" (Israel & Soto, 2013). Perhaps because it was framed primarily as a "political answer" without further strategic considerations of economic interest, the data localization part of the bill did not gather enough support to move forward. Symptomatically, what moved forward became just as quickly undone when there was a change in government. An executive decision in 2013 to transfer to the Federal Data Processing Service (Serpro) the contracts that were with Microsoft was reversed in 2016. Among other services that it was already used to and able to provide, Serpro was commissioned with launching a cloud with IaaS, PaaS, and SaaS facilities, a move that did not receive either macropolitical or material support, thus was short lived.

Arguably, the way that data localization was dealt with as haphazard politics without seeking consensus with clear explanation about its importance to local actors shrunk the margin of maneuverability of the groups supporting the mandate. The entire process lacked a well-designed strategy for achieving data localization while managing the negative reactions from international business

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

lobbies. Originally supporters of data localization included telecom companies, broadcasters, and other domestic copyright holders, together with governmental, judicial, and police authorities. The main and most cohesive opposition was from foreign content and services providers, aided by fractured opinion and interests among representatives of civil society and national content providers (Chamber of Deputies, 2016). In the end, data localization was defeated.

Inspired by the European GDPR, Brazil passed its General Data Protection Law (LGPD) in 2018, which became effective in 2020. Regarding the lack of data localization requirements, the current LGPD is a compromise. At this point, Brazil basically affirms its right to extraterritorial reach to the data in case of domestic contestation of something related to the data, its treatment, and storage, that is, violation on national data protection law by foreign actors. While defeated sectors in Brazil wanted data to be stored in the country at least for some categories of data, a compromise was designed by a winning coalition[25] in which data would be allowed to be stored anywhere. The text of the compromise affirms that Brazil would have extraterritorial reach to its national data stored abroad, as well as the right to define what foreign system is to be considered "adequate" in terms of data protection, that is, to what country Brazil's data can flow freely. Nonetheless, it is clear that this purported extraterritorial reach lacks enforcement power. As for Serpro – the one that was commissioned in 2013 with launching a cloud with IaaS, PaaS, and SaaS facilities and was being privatized in the early 2020s – in 2020, it hired Amazon's AWS directly without a public bidding process to be in charge of those facilities.

Since this issue is being addressed in the Brazilian legislature rather than by independent agencies as in India, interest groups were unable to form a coalition that sees data localization as beneficial and desirable. So far, groups in favor of data localization policies were not able to articulate arguments to either convince the legislator or create a competitive coalition to support policies that would foment a feasible technological upgrading that would address data sovereignty concerns and generate more gains and maneuverability for domestic actors in areas such as artificial intelligence, cloud computation and storage, internet of things, and machine learning. If well explained, this action can arguably be performed hand in hand with some sort of understanding with established (international) interests.

Current Brazilian framework does not limit at all the chokepoint effect of US's or any other eventual superpower's weaponization of interdependence in the digital sector. Given current winning coalitions in Brazil, curtailed sovereignty and economic dependence tend to be embraced as paths of least resistance, differentiating Brazil from India, the latter restricting cross-border flow for certain data as well as defining categories of data that can cross India's border as long as a copy of it is kept in a data center in the country.

[25] See Chamber of Deputies (2016) for a detailed account of these negotiations in Congress between different groups of interest.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press

6.6 CONCLUDING REMARKS

In this chapter, we surveyed the digital technology landscapes of Brazil and India, especially their data localization policies. To a large extent, both middle powers are interdependent on the US-led digitalization of socioeconomic processes. We present support for the idea that data localization is a necessary, but not sufficient, condition on the path to digital sovereignty, and that it can be designed to diminish US chokepoint effects under weaponized interdependence.

We have observed that in both countries, a fractured, technological landscape exists, albeit differently assembled. In India, the core of the technological landscape represents a healthy mix of foreign tech giants, domestic conglomerates, and independent governmental entities. In the Brazilian case, a similarly fractured outcome exists at the infrastructural level. However, at the intermediary level (such as large retail and finance platforms), Brazil's landscape is dominated by local conglomerate players, whereas India's landscape is completely dominated by American tech giants. Finally, at the single-sector level, both India and Brazil represent a vibrant competitive market with a healthy mix of domestic private-sector players and foreign players (including both tech giants and single-sector players); however, with the caveat, India has an advantage due to broader human capital dedicated to these industries.

In general, our note on fractured outcomes fits in well with the existing developmental politics literature on Brazil and India (Evans, 1995). However, when each country's digital technology landscape interacts with other political institutional designs and macropolitical arrangements, such as the US hegemony in digital technologies, different outcomes result, especially in terms of data localization policies. While India reaffirms a fractured outcome, Brazil moves to a more dependent one.

Thus, reiterating our central argument: data localization policies help countries avoid chokepoint effects under weaponized interdependence; however, the enactment of these policies is dependent on domestic politics. The two case studies discussed earlier highlight how countries that are similar in the hierarchy of international relations – middle powers – can have varied outcomes when it comes to critical policies that may enhance their autonomy under weaponized interdependence. We argue that the observed variation in these policies occurs because of a variation in authority of a country's independent institutions. The two case studies of India and Brazil are emblematic of a wider argument about middle powers, autonomy under weaponized interdependence, and domestic institutional authority.

https://doi.org/10.1017/9781009531085.009 Published online by Cambridge University Press