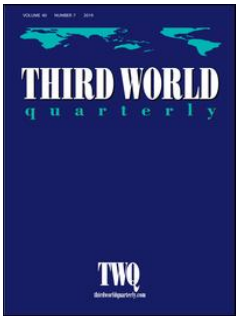

Third World Quarterly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ctwq20

Data securitisation: the challenges of data sovereignty in India

Maximiliano Facundo Vila Seoane

To cite this article: Maximiliano Facundo Vila Seoane (2021): Data securitisation: the challenges of data sovereignty in India, Third World Quarterly, DOI: 10.1080/01436597.2021.1915122

To link to this article: https://doi.org/10.1080/01436597.2021.1915122

Published online: 03 May 2021.

THIRD WORLD QUARTERLY
https://doi.org/10.1080/01436597.2021.1915122

Data securitisation: the challenges of data sovereignty in India

Maximiliano Facundo Vila Seoane

School of Politics and Government, National University of San Martín, Buenos Aires, Argentina

ABSTRACT

The rules employed to govern cross-border data flows are in dispute, the outcome of which will certainly affect digitalisation policies in the so-called Global South. Against this backdrop, data localisation has become one of the most prominent and disputed policy measures for states seeking to regulate cross-border data flows. This article argues that data localisation can be understood as the product of a new type of resource securitisation, namely data securitisation. This process is shaped by a range of state-specific political and economic issues, and by the outcome of the pressure exerted by national and foreign interest groups. Specifically, the article examines the case of India, where a set of policy measures and initiatives introduced in 2018 began a set of strict data securitisation moves; however, their results were ambivalent. On the one hand, economically driven data localisation requirements have been softened by the stark lobby of foreign governments and transnational corporations, in tandem with local actors, illustrating the structural limits faced by Global South states' sovereign digitalisation policies. On the other hand, a geopolitically driven data securitisation move against Chinese firms has been successful. The article concludes by outlining what lessons Global South actors can draw from this case.

ARTICLE HISTORY
Received 13 June 2020
Accepted 2 April 2021

KEYWORDS
Data securitisation
data sovereignty
data localisation
data politics
India

Introduction

Digitalisation,[1] understood as the ongoing process of turning every type of interaction into digital data, is a fundamental driver of data capitalism, which is characterised by the accumulation of capital by technology firms through the extraction and use of data for multiple purposes. This data capitalism has paved the way for new data-based business models that have generated new opportunities and challenges across the world (Schia 2018; Vila Seoane and Saguier 2020). However, there are no international agreements on cross-border data flows, which are at the heart of the global digital economy. This is problematic, because there are contending visions on how to govern them. Indeed, Big Tech firms and their home states that benefit the most from cross-border data flows are trying to advance new digital trade norms that ensure the free flow of data (Azmeh, Foster, and Echavarri 2020). In contrast, other states perceive such unrestricted data flows as a threat to their digital sovereignty.

CONTACT Maximiliano Facundo Vila Seoane mvila@unsam.edu.ar

Similarly, many civil society organisations (CSOs) oppose the free flow of data for hampering other states' development policies and further concentrating power in just a few transnational corporations (CSO Letter Against E-commerce Rules in the WTO 2019). Hence, the rules employed to govern cross-border data flows are in dispute, the outcome of which will certainly affect digitalisation policies in the so-called Global South.

Against this backdrop, data localisation has become one of the most prominent and disputed policy measures for states seeking to regulate cross-border data flows. In its strictest form, this policy requires that organisations retain data only within the territory from which they have been extracted, while a softer approach is to demand that a local copy is kept, while cross-border transfers remain permitted (Selby 2017). Another alternative is to allow cross-border data flows only to other countries that ensure a similar level of data protection. Analysts have categorised the main factors driving the introduction of data localisation (Liu 2020; Panday and Malcolm 2018; Selby 2017), namely to prevent foreign surveillance, to ensure that foreign firms protect citizens' data, to help law enforcement agencies access data more easily for investigations, to encourage national information technology (IT) firms or for geopolitical reasons, among others. In contrast, the US considers such measures form a trade barrier that hinders the 'free flow of data' (Office of the United States Trade Representative 2019), a new kind of digital protectionism. This criticism has been aimed mainly at China and Russia (Aaronson 2019), the US's main strategic rivals, which have used national security concerns, among other factors, as a justification to introduce strict data localisation requirements (Liu 2020; Nocetti 2015). In both cases, the widely held allegation in the West is that data localisation facilitates the violation of citizens' data rights by such authoritarian states. Consequently, the US has been advocating for the inclusion of provisions in free trade agreements to prevent partner countries from passing such policies, such as in the United States-Mexico-Canada Agreement. Likewise, liberal academics reject the assertion of sovereignty by states in cyberspace through data localisation, because it may neither provide the expected economic benefits nor be technically feasible (Aaronson 2019; Mueller 2019; van der Marel et al. 2016).

In the midst of these disputes, democracies of the Global South, such as Brazil, India, Indonesia and Kenya, have been exploring and experimenting with whether or not data localisation policies may be convenient for encouraging digitalisation. This article explores the puzzling case of India, which surprisingly has been introducing and discussing these measures since 2018; after all, India does not fall into the pattern of an authoritarian state demanding data localisation vilified by the West. Furthermore, India's IT sector is highly interdependent with that of the US, which begs the question: why would it endanger such a productive relationship by introducing policies conflicting with the American position? Analysts have systematically examined the main actors and interests involved, in order to shed light on these policies (Panday and Malcolm 2018; Sinha and Basu 2019), yet these thorough contributions have not established a theoretical connection with the broader academic literature investigating the link between security and resource politics, which might otherwise help to understand a recurrent call by multiple actors for sovereign digitalisation policies in the Global South.

Drawing from the literature on the international political economy of resources (Wilson 2015, 2017), this article argues that data localisation can be read as the product of a new type of resource securitisation, namely data securitisation. This process is shaped by a range of state-specific political and economic issues, and by the outcomes of pressure exerted by national and foreign interest groups. In the case of India, a set of policy measures and initiatives introduced in 2018 began a strong series of securitisation moves underscoring the importance of a data sovereignty frame advocated by both state and non-state actors alike, which pushed the government towards strict data localisation. Specifically, this case exemplifies how data securitisation may contribute to nation-building projects and, in the case of India, to its identity as a rising digital power. However, the results have been ambivalent. On the one hand, the economically driven data securitisation moves have been softened by the stark lobby of foreign governments and transnational corporations, in tandem with local actors, illustrating the structural limits faced by Global South states' sovereign digitalisation policies. On the other hand, a geopolitically driven data securitisation move against Chinese firms has been successful in excluding them from India's digital market.

This article will proceed through five main sections. The first section introduces a conceptual framework to understand data securitisation, whilst the second looks at the main state-specific economic and political issues driving data localisation policies in India and the significant actors supporting it. The third section outlines the action of national and foreign interest groups that have limited India's data localisation requirements, while the fourth section details how a data securitisation move was successfully achieved against Chinese apps. Finally, the article concludes by outlining what lessons other Global South actors can draw from this case to encourage fairer digitalisation policies.

Data securitisation as a new kind of resource nationalism

Perspectives used to comprehend the international political economy of resources can be divided along the lines of mainstream international relations theories, namely realism and liberalism. On the one hand, realist perspectives understand that states compete for control over natural resources as if it were a zero-sum game, and hence conflict is highly likely (Wilson 2017). An example of this perspective is the reading that rare earth elements, which are critical for many civilian and defence high-tech supply chains, may be weaponised by China, its main exporter, to achieve foreign policy aims. On the other hand, liberal approaches stress that international regimes, norms, rules and institutions will pave the way for cooperation, thus avoiding the pessimistic conflict scenarios feared by realists. Indeed, this view accepts that interdependence between resource exporters and importers, mediated by global markets, will foster more cooperation amongst countries (Goldthau and Witte 2010; Verrastro and Ladislaw 2007).

Yet these systemic and state-centred perspectives neglect other factors of utmost importance to comprehending the political economy of resources, such as domestic politics and the role of business. To address this gap, Wilson (2017) has proposed that the level of securitisation is the key variable explaining whether a state follows economic nationalist or liberal policies. This concept is drawn from the Copenhagen School of security studies and its understanding of security as a speech act, which if it convinces relevant audiences that a given referent object is under existential threat, thus justifies emergency measures (Buzan, Waever, and de Wilde 1998). Within this approach, it is important to distinguish between the securitisation move – that is, the act of saying some referent object is under threat – and the successful achievement of securitisation, which requires the inter-subjective acceptance by other significant actors of the urgency of the threat (Buzan, Waever, and de Wilde 1998, 25). If the economy is the referent object in danger, economic nationalist policies are usually the exceptional measures taken in the name of security. In the case of natural resources, these policies are known as resource nationalism. Although the concept lacks consensus in terms of a definition (Arbatli 2018; Childs 2016; Wilson 2015), it nevertheless conveys the idea that policies are needed to ensure that the exploitation of resources advances national goals, such as benefiting the people instead of large national or foreign enterprises (Koch and Perreault 2019, 2). In practice, resource nationalism covers a wide range of policies, such as limits on the ownership of firms in resource-based sectors, nationalisation, the introduction of fiscal and tax policies that increase state revenues from the sector, etc. (Arbatli 2018; Wilson 2015).

According to Wilson (2017), two factors influence whether resource securitisation policies are present or not. The first is the market cycle of the resource under consideration; in other words, in a boom, it may lead to securitisation, whereas this is less likely in a boost cycle (Joffe et al. 2009). Second, Wilson hypothesises that a range of state-specific economic and political issues may drive securitisation. This broad tag covers multiple subfactors that vary from state to state, namely economic, regime type and geopolitical subfactors (Wilson 2017, 39). For example, existing political institutions, such as developmental, liberal market or rentier regimes, shape the types of resource policies that a state may implement (Wilson 2015), with rentier regimes far more inclined towards resource nationalism. Likewise, the securitisation of resources is also driven by the geopolitical environment, in that the more unstable it is, the higher the probability it may lead to exceptional measures by governments to instrumentalise them (Wilson 2017, 40). Economic security is also an issue of chief concern for both resource consumer and producer states: the former due to their dependence on access to the resource, and the latter because of the profits extracted from its export. Hence, different stakeholders lobby for the economic securitisation of resources (Wilson 2017, 32). Overall, if these factors are intense enough, they may drive resource nationalism, thereby pressuring states to adopt unilateral policy decisions that will lead to tensions and even conflict with others, hence undermining cooperation and politicising the international markets of a given resource.

This conceptual framework is a useful device with which to analyse the nascent politics of data securitisation. However, at least four adaptations are needed for the analysis of data as a resource, and these are synthesised in Figure 1 and explained below. First, although there are proposals to put a price on data, it is not yet an asset class traded in global financial markets; consequently, the market cycle is not a relevant factor driving data securitisation. Second, resource nationalism is a kind of discourse also employed by the state for its nation-building project (Koch and Perreault 2019), thus shaping its identity. This is even more pronounced with data as a resource, since there are different contending models for digitalisation policies (Vila Seoane and Saguier 2020). Therefore, the link between resource nationalism, discourse and identity politics needs to be further stressed in the analysis of data securitisation. Third, although Wilson mentions the role of different interest groups in influencing resource securitisation, these different national and foreign non-state actors need to be explicitly incorporated in the conceptual framework to avoid state-centrism in the analysis. After all, in many other cases of resource nationalism, social movements and other interest groups have played a key role in mobilising such frames (Kohl and Farthing 2012). Fourth, recent critical scholarship has argued that the boundaries between normal politics and the exceptional measures that the securitisation process requires are not so clear cut (Campion 2020; Mavelli 2013). In this regard, I propose considering data securitisation as a process that may lead to policies within a gradient varying in the continuum of

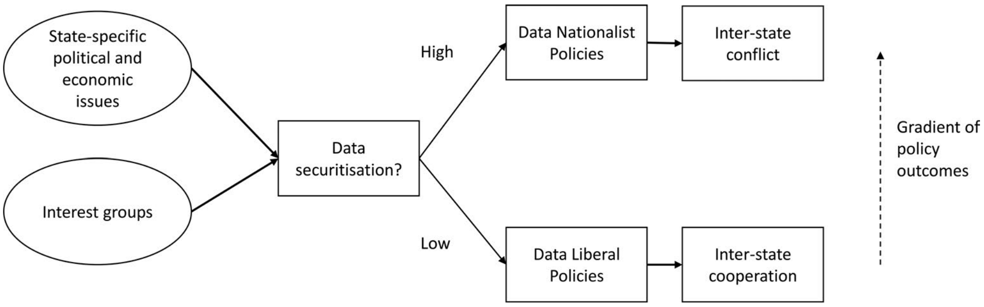

Figure 1. Conceptual framework (adapted from Wilson 2017) to explain data policies as an outcome of securitisation dynamics.

exceptionality–normality, leading to outcomes located between data nationalist and data liberal policies.

Data securitisation in India: data localisation

To appreciate the political and economic issues driving data localisation in India, we must consider that since 2014, the country has been ruled by the Bharatiya Janata Party (BJP), a spin-off of the Rashtriya Swayamsevak Sangh (RSS), a right-wing volunteer organisation founded in 1925 that has several Hindu nationalist affiliated branches. The BJP, being one of them, has cultivated the Hindutva ideology, which puts Hindu identity above others in the country, and this has raised serious concerns among ethnic minorities in India, mainly Muslims. The BJP's political identity has historically been linked to economic nationalist policies; however, since taking power, the party's record has been far more mixed (Mehta and Chatterjee 2015). Likewise, before becoming prime minister (PM), Narendra Modi had governed the state of Gujarat since 2001, articulating a discourse that advanced neoliberal policies (deregulation, market liberalisation, the privatisation of infrastructure and services, the promotion of entrepreneurship, etc.), without disregarding the strong ethnocultural elements of Hindutva to win elections through the incitement of stark social polarisation (Bobbio 2012; Jaffrelot 2015).

Following his election to power in 2014, Modi promised high economic growth levels, an increase in labour-intensive manufacturing jobs and a strengthening of India's manufacturing sector. Digital industries also became a priority, which is why the Government of India (GoI) launched several strategies to strengthen the country's move towards digitalisation. As examples, the Digital India Initiative aims to modernise state bureaucracy through the active use of information and communication technologies, while the Make in India programme encourages the production of technologies in the country. Furthermore, in 2017 India established an Artificial Intelligence (AI) Task Force with the aim of outlining a national policy in this area. Yet the results of PM Modi's economic policies during his first term in office have lagged behind the promises made (Sharma 2019). In this context, a year before the 2019 national elections, the GoI began introducing bills and implementing policies with data localisation requirements that signalled a new policy orientation towards increasing economic nationalism in digital policies. The main justification for such initiatives was that data was a new type of valuable strategic resource that would contribute to much-needed economic growth. In PM Modi's words, 'data is the new gold' (quoted in Hindustantimes 2019). Among the policies and bills requiring data localisation (Basu, Hickok, and Singh 2019), the following three introduced before the 2019 elections are the most illustrative cases of data securitisation moves, in that they exemplify the drivers of data localisation identified in the literature (Panday and Malcolm 2018; Selby 2017).

The first policy was introduced on 5 April 2018 by the Reserve Bank of India (RBI), which passed a resolution requiring all system providers to store all payment transactions data only within the country. The directive argued that digital payments had grown considerably, yet, according to the RBI, security and safety measures for supervising such systems were not in place (Reserve Bank of India 2018). Therefore, the RBI demanded data localisation to fulfil such a goal. Against potential criticism of this decision, the directive also mentions that if the transaction has a foreign element, it can also be copied abroad.

The second initiative to introduce data localisation requirements was India's Data Protection Bill. This follows India's 2017 landmark Supreme Court judgement ruling privacy as a fundamental right, aligned with multiple incidents of data breaches affecting Indian citizens. In this context, the GoI requested a report be filed to a committee led by the retired Supreme Court Judge Justice B. N. Srikrishna to discuss a new Data Protection Bill. The final report notes that 'the protection of personal data holds the key to empowerment, progress, and innovation' (Srikrishna Committee 2018, 3). In its most polemic recommendation to achieve these goals, it advises the prohibition of transferring of 'critical personal data' beyond India's borders (Srikrishna Committee 2018, 97), thus requiring strict data localisation – although the category was never defined, raising concerns about what would fall under such a provision. The report hypothesises that such a measure would spur the development of local digital infrastructures and data-processing capabilities, all central to the growth of India's AI ecosystem (Srikrishna Committee 2018, 91). Furthermore, it underscores that data localisation is necessary to enforce future privacy law; otherwise, the free flow of data across borders could undermine its protections (Srikrishna Committee 2018, 85). The report also observes that 'critical personal data' should be processed exclusively in India to avoid foreign surveillance, which in the view of the authors is based not on fearmongering (Srikrishna Committee 2018, 92) but on Snowden's revelations that US intelligence agencies have been collecting such data.

The draft e-commerce policy released on February 2019 is the third relevant initiative, and it includes provisions supporting data localisation (Department for Promotion of Industry and Internal Trade 2019). In this case, the data securitisation move is justified on the economic benefits to be derived from data. For instance, the draft policy states:

> Unlike in the case of oil, data flows freely across borders. It can be stored or processed abroad and the processor can appropriate all the value. Therefore, India's data should be used for the country's development. Indian citizens and companies should get the economic benefits from the monetization of data. (Department for Promotion of Industry and Internal Trade 2019, 16)

These data localisation requirements have been supported by a constellation of local and foreign interest groups; BJP's members defending its historical nationalist economic policies have been at the forefront of promoting such measures. Likewise, the Swadeshi Jagran Manch (SJM), an organisation affiliated with the RSS that focuses its agenda on economic self-reliance, also strongly backs data localisation. Furthermore, large national firms and small and medium-sized enterprises support data localisation. Chinese and Russian transnational corporations, such as Alibaba, Gionee, TikTok and Kaspersky Lab, have quickly claimed that they will fully comply with the provision. Unsurprisingly, these companies are based in states where data localisation is accepted, in direct opposition to the liberal free flow of data that the US and other countries want to spread as the globally hegemonic norms. India's data localisation measures certainly equally challenge such hegemonic norms, but its securitisation process exhibits distinctive features. Apart from the fact that it emerged in a democracy, resource nationalism in India also exemplifies the mobilisation of the data sovereignty frame by state and non-state actors to advocate for data localisation.

Data sovereignty as a defence against data colonialism

The fear of foreign firms abusing citizens' data is already present in multiple countries, and academics have denounced such practices as a kind of data colonialism (Couldry and Mejias 2019). Politicians such as Angela Merkel have also warned of the threat of excessive data concentration in a few American and Chinese corporations, stressing the need for European digital sovereignty (Chazan 2019). Several incidents have contributed to a similar trend in India. For instance, Facebook's Free Basics project, which aimed to give Internet access to the poor for free, offered a limited version of the Internet centred on its services that violated the principle of net neutrality, and is why it raised concerns that the company was actually seeking the poor's data. After a vigorous campaign by many interest groups that understood the project as a form of digital colonialism (Prasad 2018a), the GoI prohibited the project. Likewise, Indian citizens were also affected by the Cambridge Analytica scandal. The spread of fake news facilitated by WhatsApp has been another cause of dramatic mob-lynching in many Indian villages, and yet the company has rejected state demands to provide access to the encrypted data, in order to limit such outbursts. Despite the global nature of the challenge, it is important to bear in mind that the fear of data colonisation or data imperialism has far more resonance in the Indian context than in Europe, not only given the traumatic historical experience with colonialism, but also in terms of the success of the anti-colonial movement.

In this context, politicians and businessmen have made statements where there is a referent object under threat, namely, India's sovereignty, which must be securitised through data localisation. One of the most prominent examples is the popularisation of the term 'data sovereignty' by Vinit Goenka, a BJP politician that at the time of the statement was co-convener of the national Information Technology cell of the party. In 2014, on a blog post on his personal website, Vinit Goenka argued that to become a truly sovereign nation, India could not afford to ignore 'data sovereignty', meaning that 'information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located' (Goenka 2014). This definition captures very well the type of narrative that has emerged in India that imagines data to be another key strategic resource belonging to Indians, instead of being used for the benefit of foreign firms, which is precisely the type of imagination present in resource nationalism more generally (Childs 2016, 2). Furthermore, Vinit Goenka, believes data sovereignty is essential for avoiding this new type of colonisation, which will go beyond economic domination, in his view, likely leading to 'the enslavement of mind, body, and soul of the affected people' (Goenka et al. 2019, 19). Consequently, from this viewpoint, data localisation is indispensable in ensuring India's data sovereignty.

Some Indian businessmen have also incorporated such a frame against data colonisation in their public statements. Take the case of Paytm, one of India's payment gateways, which criticised the Internet and Mobile Association of India's opposition to data localisation, affirming that 'this is the moment for us to support our nation and promote "data sovereignty" over "data monopolisation", which is possible through data localisation' (Bhakta 2018). Likewise, in 2017, the chairman and managing director of Reliance Industries, Mukesh Ambani, proposed that PM Modi should create a 'Keep in India' programme to preserve the nation's data within its borders (Punj 2017). During his speech at the Vibrant Gujarat Summit, Ambani urged Modi to strengthen the Make in India programme through data localisation, noting:

> […] Gandhi led a political movement against political colonisation. Today, we have to collectively launch a new movement against data colonisation. In this new world, data is the new oil, and data is the new wealth. India's data must be controlled and owned by Indian people and not by corporates, especially global corporations. (Economic Times 2019)

These statements illustrate how state and non-state actors have constructed a data sovereignty frame, which deems data localisation indispensable for fighting against data colonialism. Against the pressure of these interest groups, the state may be compelled to adopt more stringent data nationalist policies, that deviate from the free flow of data. However, another important factor in India's case, underplayed in the literature, needs to be accounted for, namely the relevance of data nationalist policies in contributing to its nation-building project and its identity as a rising digital power.

The threat to India's identity as a rising and influential digital power across the Global South

Data colonisation is framed as a threat to the construction of India's identity as a rising digital power. Several statements made by Indian policymakers reveal the peril of lagging behind the technological edge that the US and China have in the digital economy. Take the case of India's telecommunications secretary, Aruna Sundararajan, who, after supporting data sovereignty, said that:

> The US has its own data and other peoples' data as well; China has built its digital economy, its search engines and machines on the back of its own data. India must look carefully at who has access to our data, what they're able to do with it, and what returns Indians will get for it. (Sengupta and Aulakh 2018)

Likewise, at the 4th Global Technology Summit, India's External Affairs Minister, Subrahmanyam Jaishankar, stressed the importance of data security as part of national security, and observed that 'if our aspiration is to be a leading power one day, we have to be a leading power in also harnessing data' (The Print 2019, 4:17). These statements have to be understood as a consequence of a paradox in the Indian economy. Despite the country having a strong IT sector that in 2017 contributed approximately 7.7% of its gross domestic product (GDP; Press Information Bureau 2019), India still lacks influential digital platforms that can operate globally, such as Google or Alibaba. This is particularly worrisome if we consider that AI, 5G and the Internet of Things will spur even more data-based business models. Thus, even though projections estimate that the nation will become the third largest economy by 2030 (Henry and Pomeroy 2018), just behind China and the US, those defending data sovereignty fear that data colonisation will undermine its ability to benefit fully from data produced in its territory. Understandably, they stress the importance of building local data ecosystems and digital infrastructure, such as data centres, to promote India's capabilities in these strategic areas (Goenka 2017; Srikrishna Committee 2018, 92). In their view, data localisation would help accomplish these nation-building objectives.

Statements about India's identity as a rising digital power distinguish it from the US and China. As regards the latter, such utterances emphasise that India will not follow China's path, since its democratic system and values demand a more open process for data governance. As regards the US, India highlights its links to other developing countries; for example, during the 2019 G20 meetings at Osaka, it opposed Japan and the US's proposal for advancing with a global initiative on a Data Free Flow with Trust governance model. Besides promoting economic growth, India's Foreign Secretary, Mr Vijay Gokhale, underlined that 'data also needs to take into account the requirements of developing countries' (Press Trust of India 2019). During the press conference presenting the report for a Data Protection Bill, the acting Minister for Electronics and Information Technology, Ravi Shankar Prasad, said that India had become an important digital power, noting: 'we would like India's data protection law to become some kind of a model for the global world also, which is a blend of security, safety, privacy and innovation' (Prasad 2018b, 4:17).

The ambition to become a role model for the Global South is not new, for example, India already leads states opposing proposals for the free flow of data at the World Trade Organization (WTO). Under the electronic commerce programme initiated in 1998, WTO members agreed to put a moratorium on custom duties for electronic transmissions (in other words, cross-border data flows), to help the development of the nascent industry. Since then, the moratorium has been renewed annually, but consensus in this regard is now under pressure. In 2017, before the 11th WTO ministerial meeting in Buenos Aires, a group of countries led by the US had been advocating to extend the moratorium permanently in a clear attempt to benefit American technology companies (Kelsey 2018). However, the initiative faltered, because India and the African Group of countries opposed it, arguing that as more products and services become digitised, any constraint on taxing cross-border data flows would seriously harm developing states' capacities to raise revenues (Banga 2019). In line with this position, India's draft e-commerce policy opposes making the moratorium on taxing cross-border data flows permanent (Department for Promotion of Industry and Internal Trade 2019, 10). In addition, the country has also refused to accept bans on data localisation provisions in free trade agreements; indeed, media reports claim that this was one of the reasons why the country finally pulled out of the Regional Comprehensive Economic Partnership.

On the whole, these examples show that the GoI aims to present itself as a democratic advocate of the policy space of developing countries to better manage the transition towards digitalisation. Thus, India's data sovereignty frame seeks to contribute to nation-building and to reinforce an identity distinct from that of the US and China.

The global economy and the limits of data sovereignty

India's data localisation requirements have received widespread criticism and opposition from national and international interest groups. These critics have used both arguments and threats of coercion to urge the GoI to back down from its strict data localisation policies. The pressures examined in this section cast light on the structural limits that a data sovereignty vision faces when departing from the norms that the US government and its corporations, together with the European Union (EU), attempt to internationalise for data governance.

Different national and foreign interest groups, such as the US–India Strategic Partnership Forum and the US–India Business Council, have questioned the economic benefits of data localisation. These criticisms echo the findings of articles using trade models to estimate the negative consequences of data localisation policies on GDP growth (van der Marel et al. 2016). Businesspeople, media and foreign stakeholders have repeated such arguments in India, such as the need of firms to invest in local cloud infrastructures to fulfil data localisation requirements, which would significantly increase their operational costs and the costs that consumers would have to pay. Technically, critics have also expressed doubt over India's ability to provide data storage services as cheaply, efficiently and securely as those offered by foreign firms (Basu, Hickok, and Singh 2019). Consequently, they believe that India's IT industry, particularly SMEs, will suffer the most from data localisation. Furthermore, Indian businesses advocating data localisation have also been severely criticised and tagged as mere opportunists planning to displace foreign competitors, rather than altering unfair digital accumulation business models. Such is the case of Ambani's Jio Platforms, or Paytm, suspected of defending the interests of the Alibaba Group, which has a significant stake in the firm.

In opposition to the data sovereignty frame, critics claim that data localisation is a threat to human rights. One of the reasons for this view is that barriers to the free flow of data hinder free trade (Office of the United States Trade Representative 2019, 253), which would go against the liberal principles on which India's IT sector depends (Srikrishna Committee 2018, 208). Furthermore, digital rights organisations have expressed serious concerns about the hollowing of citizens' civil and political liberties if data were stored and processed only in India without adequate legislation limiting state surveillance (Basu, Hickok, and Singh 2019). These criticisms expose the paradox that the use of data localisation to protect citizens from foreign surveillance may end up exposing them to the surveillance power of the state. This is an issue of grave worry, considering the well-documented problematic practices of state surveillance in India (Arun 2017; Thomas 2019), which would be particularly damaging to minorities under pressure from the Hindutva ideology. Finally, foreign firms, such as Facebook, claim that even if India is not and may not ever become an authoritarian state, accepting data localisation measures would send the wrong signal to those encouraging the spread of a model that would limit Internet freedoms.

The US and the EU actively lobbied for India to accept their preferred norms, and they even threatened coercive measures if stakes were ignored (Kalra and Kumar 2019). Indeed, data localisation has become an issue in the bilateral relation between the US and India (Office of the United States Trade Representative 2019). In March 2019, then President Trump announced that from 5 June onwards, India would lose access to the Generalized System of Preferences (GSP), a programme that removes tariffs from selected developing countries exporting to the US. This decision was made on the grounds that India did not assure 'equitable and reasonable access' for American firms to Indian markets, affecting over US$5.6 billion worth of Indian exports (Beech and Dasgupta 2019). Reporters observed that the exclusion of India from the GSP was in response to its policies discriminating against US firms, such as data localisation requirements (Beech and Dasgupta 2019). Furthermore, Reuters' journalists informed that the US State Department was planning to limit the amount of H1B visas issued to Indians, unless they dropped data localisation measures (Dasgupta and Kalra 2019). Although sources later denied such a threat, it nevertheless caused more uproar in the media coverage of bilateral relations.

In a similar vein, during the joint press conference with Narendra Modi at the 14th EU–India Summit, the president of the European Commission, Jean-Claude Juncker, stated that the EU would only continue to negotiate a free trade agreement with India if the free flow of personal data between them converged towards European standards (Juncker 2017). At the time, the EU was getting ready to implement its ambitious General Data Protection Regulation (GDPR), which aims to shape how data is processed by firms, leveraging the rights of citizens vis-à-vis foreign digital platforms, rather than forcing strict data localisation. Unsurprisingly, the EU has been a vocal opponent of India's data localisation requirements in India (Gencarelli 2018), since it would not pass an adequacy decision under the GDPR. Hence, the condition put forward by the EU is an example of the extension of market power Europe to digital policies (Vila Seoane 2020), with access to the EU market used as leverage to persuade other actors to accept, adopt and internalise its preferred norms.

After the strong opposition of these influential foreign and national interest groups, Modi's government has reconsidered the securitising move towards strict data localisation, indicating the search for a middle position that balances relevant interests with other government policy priorities. For example, data localisation was finally removed from the e-commerce policy, which has understandably raised objections from the groups supporting it, such as the SJM. Likewise, the last version of the Data Protection Bill that was introduced in the Lok Sabha on 6 December 2019 for further debate does allow the cross-border flow of sensitive data, as long as a copy is kept in India. Barring a few exceptions, the bill prohibits the still undefined – but far more bounded – category of critical personal data, which will be specified by the Central Government (The Personal Data Protection Bill 2019, 18). However, the bill also included a provision for the government to access non-personal data. Along this line, a committee of experts recommended to the GoI that this type of data should be shared, with critical non-personal data subject to data localisation (Ministry of Electronics and Information Technology 2020, 38). Unsurprisingly, this report received the same staunch opposition from global and local actors opposing data localisation for personal data. Furthermore, the bill has been seriously criticised, because in the name of protecting or preventing offence against the 'sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order' (The Personal Data Protection Bill 2019, 19), it exempts any agency of the GoI from its provisions. This again displays the alarming contradiction of justifying data localisation to prevent surveillance from foreign actors, while leaving national actors beyond the law, which is in line with Thomas' (2019) characterisation of the GoI's digital policies as ambivalent, since in some cases they may be progressive, while in others, such as in the increase of state surveillance capabilities, they certainly are not.

India is not the first democratic state to have experienced external pressures to withdraw proposals for data localisation policies. In 2013, in the wake of Snowden revelations, President Dilma Rousseff accelerated the passing of an Internet Bill of Rights in Brazil that initially required foreign firms to locate their servers in the country. This intended retaliation promptly received robust opposition from US firms, which made similar arguments to those put forward against India's data localisation provisions (Kshetri 2016). In the end, the Brazilian government dropped all data localisation requirements. In comparison, the GoI faced similar intense external and internal pressures against data localisation – and many with good reasons. But this will likely water down, rather than completely eliminate, such provisions, because there are far more actors supporting them than in the Brazilian case. In any case, this weakening of data localisation requirements seems a reasonable decision if we take into account that India's IT sector exports US$117.9 billion, of which 72.1% goes to the US and Canada, and 30.2% goes to Europe, of which almost half goes to the UK, and 69.5% of these exports are achieved via the cross-border supply of services (Reserve Bank of India 2019). Therefore, the current success of India's IT sector depends on such data flows, and endangering it would damage what has thus far been a successful industry. Yet, as the following section shows, data localisation is not the only example of data securitisation in India.

A geopolitical turn to data securitisation: the digital strike

During the last decade, India and China have been able to cooperate economically and even politically through the informal group of states known as BRICS, which also comprises Brazil, Russia, and South Africa however, their bilateral relationship remains quite fraught. Besides the competition between a rising India and a rising China, or China's support of Pakistan, both countries have persisting border disputes along the Line of Actual Control established after the 1962 Sino–Indian war. In this context, after a month of skirmishes, on 15/16 June 2020, violent clashes took place at the Galwan River Valley between soldiers from the Indian Army and the Chinese People's Liberation Army, resulting in the deaths of 20 Indian soldiers. The GoI was under pressure to strike back, but instead of dangerously escalating the conflict militarily or using traditional trade barriers against Chinese firms, it retaliated in an original way. On 29 June, the Ministry of Electronics and Information Technology announced it was blocking 59 mainly Chinese-owned apps, including TikTok, WeChat and QQ International (Press Information Bureau 2020). In the official communication, invoking section 69 of the Information Technology Act, the GoI articulated that

> The compilation of these data, its mining and profiling by elements hostile to national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India, is a matter of very deep and immediate concern which requires emergency measures. (Press Information Bureau 2020)

This statement exemplifies very clearly a securitisation move, where the reference object under threat – India's national security and defence – must be protected from the threats to privacy and data security that the alleged list of 59 malicious apps represents. The official communication did not provide any public technical details to substantiate the suspected threats, nor did it mention China directly. However, BJP public officials made clear it was in retaliation to China's aggression, even naming it a digital strike. Although a hyperbolic statement, the ban is similar to revoking the licence of firms of a given country that extract natural resources from another, resulting in disputes with the firms and home states involved.

The official communication further detailed that 'there has been a strong chorus in the public space to take strict action against Apps that harm India's sovereignty as well as the privacy of our citizens' (Press Information Bureau 2020). Indeed, the national press and citizens in social media widely praised the retaliation, and even more in the context of the COVID-19 fallout that many in India blame on China. The decision was also well received by the SJM, which had already asked PM Modi to ban TikTok in 2019, because they believe the platform spreads anti-national content among Indian youth. Internationally, the decision made explicit the closer bilateral relation of the BJP with the Trump administration in security affairs (Thomas 2019), which later implemented a similar executive order to ban TikTok and other Chinese apps. Apart from the Chinese firms, Indian users and influencers who made money from these apps were the clear losers.

By the end of 2020, the GoI had made three more announcements that added a total of 267 apps to the banned list, including AliExpress and PUBG, a widely popular game developed by Tencent. Apart from consolidating the offensive against the internationalisation of Chinese digital firms to India, these subsequent prohibitions further reinforced an economic side to the data securitisation process of the GoI, which envisions a unique opportunity to grow 'Made in India apps'. Returning to the conceptual framework, the ban of Chinese apps exemplifies how a geopolitically driven data securitisation process may lead to data nationalist policies in order to retaliate against a rival state. In contrast to the more contentious process of advancing data localisation policies, this securitisation move was successful, because most relevant audiences in India accepted the threat that Chinese digital firms pose to the country's data sovereignty, despite the lack of publicly available evidence proving the allegations.

Conclusion

Inspired by Wilson's contributions, this article has argued that the literature on the international political economy of resources offers conceptual tools to understand data nationalist policies as the outcome of a new type of resource securitisation process, namely data securitisation. These data nationalist policies portray data as a new strategic resource that should not be governed by a liberal market approach. Driven by state-specific economic and political issues, together with the pressure of varied national and foreign interest groups, data securitisation moves attempt to ensure that the main benefits drawn from data remain within the boundaries of the political community from which they are extracted. Since 2018, India has been a leading example of a democratic state of the Global South advancing with data nationalist policies. Indeed, state and non-state actors alike have mobilised a data sovereignty frame in the country for both economic and political reasons. Likewise, limits to cross-border data flows have been justified to protect India's state identity as a rising digital power challenging the US and China, illustrating how data nationalist policies also contributes to nation-building projects. Nonetheless, the results of the data securitisation processes driving these policies in the country have been disparate. While initially stringent data localisation proposals have been watered down due to the strong opposition offered by foreign and national interest groups, the ban of Chinese apps triggered by a border dispute have received widespread support. This contrasts notably with the case of China or Russia, where data sovereignty has been invoked to swiftly introduce data localisation provisions, mainly due to the nature of their political systems that are less prone to the external and internal pressures seen during the debates in India and Brazil.

Furthermore, India's case offers lessons for other Global South democracies' digitalisation policies. Perhaps the most evident in this regard is that the data sovereignty frame is not limited to authoritarian states; in fact, contrarily, it can be mobilised by non-state actors in democracies and be linked to development goals, though not without problems if adequate privacy protection laws are missing. Despite its appeal, the translation of India's data sovereignty frame to other countries as a new kind of resource nationalism faces significant structural barriers. Data-based firms are not as easy to nationalise or to regulate as firms operating in natural resource-based industries, since many of the leading data-based firms do not even need to be established in a country to extract and process data from citizens across the globe. Thus, the regulatory toolbox of traditional resource nationalism is far less applicable to data value chain business models. As with any market power, India leverages access to its huge consumer base to persuade transnational corporations to implement data localisation measures, whereas countries with small populations are not in such a good negotiating position. Additionally, democracies in the Global South attempting to reassert sovereignty in digital policies will equally face bi- and multilateral pressure from foreign interest groups, but very few of these states are in a position to resist such pressures alone. Some sort of coordination at the regional level may balance such asymmetries. Finally, although it can be argued that the BRICS are in a good position to challenge US-led cyberspace governance, it remains to be seen whether the tensions between India and China described in this article, and the ongoing ones between Brazil and China, will undermine the potential coordination of the BRICS on digital policies.

The Indian data sovereignty frame is also problematic for reasons barely discussed to date. For example, the debate has been polarised between a model where foreign corporations control data and another where the state and national firms lead, both of which neglect citizens' initiatives, such as decentralised data management networks. In part, this bias is a product of the vulnerabilities of a state-centred approach to challenging hegemonic norms for data governance. An alternative could be the building of a coalition of states and social movements that questions the uncritical adoption of the free flow of data. The 315 civil society organisations that sent a letter to WTO members opposing the liberalisation of electronic commerce, and demanding policy space for developing countries, are a good example of an inchoate counter-hegemonic global movement supporting such a goal (CSO Letter Against E-commerce Rules in the WTO 2019). Similarly, thinking of data as a resource accepts an extractive model of accumulation, which neglects the huge environmental impacts of such business models in the context of our contemporary environmental crisis. Although organisations such as Greenpeace have already criticised the excessive global energy consumption of data centres, these concerns have been notoriously absent in the Indian debate.

Although data securitisation processes may not lead to the most desirable data governance policies, the challenges posed by digitalisation to states in the Global South suggest they may be here to stay. Indeed, social distancing measures introduced to control the COVID-19 pandemic have accelerated processes of digitalisation worldwide, resulting in huge profits and more market power for just a few digital technology firms. Moreover, the structural tensions over the governance of cyberspace between China and the US seem likely to persist, putting pressure on the digital policies that other states may adopt. In this challenging scenario, more research will be needed to understand these data securitisation processes and contribute to reorienting global development agendas towards a form of digitalisation that works not just for the privileged few.

Ackowledgements

I thank the reviewers and the editors for their helpful comments. All remaining shortcomings are my own.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Maximiliano Facundo Vila Seoane is a postdoctoral researcher at the National Scientific and Technical Research Council (CONICET), Argentina. He is also a professor at the School of Politics & Government of the National University of San Martín, where he teaches courses on international relations, cyberpolitics and international communication. His research interests and publications focus on digitalisation, international politics and development studies.

Note

1. Sometimes, digitisation is used interchangeably with digitalisation. In this article, the former is considered a more restricted concept than the latter, because it refers solely to the turning of analogue data into digital, whereas digitalisation further covers the broader political implications of these processes and their connection to capitalism.

ORCID

Maximiliano Facundo Vila Seoane http://orcid.org/0000-0002-0134-7714

Bibliography

Aaronson, S. A. 2019. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* 18 (4): 541–577. doi:10.1017/S1474745618000198.

Arbatli, E. 2018. "Resource Nationalism Revisited: A New Conceptualization in Light of Changing Actors and Strategies in the Oil Industry." *Energy Research & Social Science* 40: 101–108. doi:10.1016/j.erss.2017.11.030.

Arun, P. 2017. "Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalisation." *Surveillance & Society* 15 (3/4): 456–464. doi:10.24908/ss.v15i3/4.6618.

Azmeh, S., C. Foster, and J. Echavarri. 2020. "The International Trade Regime and the Quest for Free Digital Trade." *International Studies Review* 22 (3): 671–692. doi:10.1093/isr/viz033.

Banga, R. 2019. *Growing Trade in Electronic Transmissions: Implications for the South*. 29, UNCTAD Research Paper. United Nations Conference on Trade and Development. https://unctad.org/en/PublicationsLibrary/ser-rp-2019d1_en.pdf

Basu, A., E. Hickok, and C. A. Singh. 2019. *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*. Working Paper, 19 March. Bangalore, India: The Center for Internet & Society.

Beech, E., and N. Dasgupta. 2019. "Trump moves to scrap trade privilege for India, Delhi plays down impact." Accessed 22 August 2019. https://www.reuters.com/article/us-usa-trade-india/trump-moves-to-scrap-trade-privilege-for-india-delhi-plays-down-impact-idUSKCN1QM007

Bhakta, P. 2018. "Paytm says it's time to back data sovereignty over monopolisation." https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/paytm-says-its-time-to-back-data-sovereignty-over-monopolisation/articleshow/65881580.cms?from=mdr

Bobbio, T. 2012. "Making Gujarat Vibrant: *Hindutva*, Development and the Rise of Subnationalism in India." *Third World Quarterly* 33 (4): 657–672. doi:10.1080/01436597.2012.657423.

Buzan, B., O. Waever, and J. de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Campion, A. S. 2020. "From CNOOC to Huawei: Securitization, the China Threat, and Critical Infrastructure." *Asian Journal of Political Science* 28 (1): 47–66. doi:10.1080/02185377.2020.1741416.

Chazan, G. 2019. "Angela Merkel Urges EU to Seize Control of Data from US Tech Titans." *Financial Times*, November 12. https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca.

Childs, J. 2016. "Geography and Resource Nationalism: A Critical Review and Reframing." *The Extractive Industries and Society* 3 (2): 539–546. doi:10.1016/j.exis.2016.02.006.

Couldry, N., and U. A. Mejias. 2019. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20 (4): 336–349. doi:10.1177/1527476418796632.

CSO Letter Against E-commerce Rules in the WTO. 2019. "Civil Society Letter against digital trade rules in the World Trade Organization (WTO)." Accessed 7 July 2019. http://www.thefutureworldofwork.org/media/35568/cso-letter-digital-trade-2019-04-01-eng.pdf

Dasgupta, N., and A. Kalra. 2019. "Exclusive: U.S. tells India it is mulling caps on H-1B visas to deter data rules - Sources." Accessed 5 February 2020. https://www.reuters.com/article/us-usa-trade-india-exclusive/exclusive-us-tells-india-it-is-mulling-caps-on-h-1b-visas-to-deter-data-rules-sources-idUSKCN1TK2LG

Department for Promotion of Industry and Internal Trade. 2019. *Draft National e-Commerce Policy: Indians' Data for India's Development*. New Delhi, India: Ministry of Commerce and Industry. https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

Economic Times. 2019. "Mukesh Ambani urges PM to take steps against data colonisation." Accessed 10 July 2019. https://economictimes.indiatimes.com/tech/ites/mukesh-ambani-urges-pm-to-take-steps-against-data-colonisation/articleshow/67585615.cms

Gencarelli, B. 2018. "Submission on draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY)." European Commission. https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

Goenka, V. 2014. "IT Sovereignty in India – The Data Centre Dimension." https://vinitgoenka.wordpress.com/2014/04/11/it-sovereignty-in-india-the-data-centre-dimension/

Goenka, V. 2017. ""Keep In India": Why It's Absolutely Vital For Us To Ensure That Our Data Stays Within Our Shores." *Vinit Goenka's Blog*. https://vinitgoenka.wordpress.com/2017/06/10/keep-in-india-why-its-absolutely-vital-for-us-to-ensure-that-our-data-stays-within-our-shores/

Goenka, V., Patil V. M., Shekatkar D. B., Khandare, V., Bhatia, V., Ranade J., and B. Panchal. 2019. *Data Sovereignty: The Pursuit of Supremacy. Kindle*. Delhi, India: Penman Books.

Goldthau, A. and J. M. Witte, eds. 2010. *Global Energy Governance: The New Rules of the Game*. Berlin: Global Public Policy Institute; Washington, DC: Brookings Institution Press.

Henry, J., and J. Pomeroy. 2018. *The World in 2030. Our Long-Term Projections for 75 Countries*. HSBC Global Research. https://enterprise.press/wp-content/uploads/2018/10/HSBC-The-World-in-2030-Report.pdf

Hindustantimes. 2019. "'Data is the new oil, new gold,' says PM Modi in Houston." New Delhi, India. https://www.hindustantimes.com/india-news/data-is-the-new-oil-new-gold-says-pm-modi-in-houston/story-SphHDPQadvF1dJRMXHCkwK.html

Jaffrelot, C. 2015. "What 'Gujarat Model'? – Growth without Development – and with Socio-Political Polarisation." *South Asia: Journal of South Asian Studies* 38 (4): 820–838. doi:10.1080/00856401.2015.1087456.

Joffe, G., P. Stevens, T. George, J. Lux, and C. Searle. 2009. "Expropriation of Oil and Gas Investments: Historical, Legal and Economic Perspectives in a New Age of Resource Nationalism." *The Journal of World Energy Law & Business* 2 (1): 3–23. doi:10.1093/jwelb/jwn022.

Juncker, J.-C. 2017. Remarks by President Jean-Claude Juncker at the joint press conference with President Donald Tusk and Prime Minister Narendra Modi on the occasion of the 14th EU-India Summit. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3747.

Kalra, A., and M. Kumar. 2019. "India to Review Data Storage Rules That Irked U.S. Tech Firms." Accessed 5 February 2020. https://www.reuters.com/article/us-india-data-localisation/india-to-review-data-storage-rules-that-irked-us-tech-firms-idUSKCN1TJ0WN.

Kelsey, J. 2018. "How a TPP-Style E-Commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)." *Journal of International Economic Law* 21 (2): 273–295. doi:10.1093/jiel/jgy024.

Koch, N., and T. Perreault. 2019. "Resource Nationalism." *Progress in Human Geography* 43 (4): 611–631. doi:10.1177/0309132518781497.

Kohl, B., and L. Farthing. 2012. "Material Constraints to Popular Imaginaries: The Extractive Economy and Resource Nationalism in Bolivia." *Political Geography* 31 (4): 225–235. doi:10.1016/j.polgeo.2012.03.002.

Kshetri, N. 2016. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. New York, NY: Springer Berlin Heidelberg.

Liu, J. 2020. "China's Data Localization." *Chinese Journal of Communication* 13 (1): 84–103. doi:10.1080/17544750.2019.1649289.

Mavelli, L. 2013. "Between Normalisation and Exception: The Securitisation of Islam and the Construction of the Secular Subject." *Millennium: Journal of International Studies* 41 (2): 159–181. doi:10.1177/0305829812463655.

Mehta, P. S., and B. Chatterjee. 2015. "India in the International Trading System." In *The Oxford Handbook of Indian Foreign Policy*, edited by D. M. Malone, C. R. Mohan, and S. Raghavan, 636–649. Oxford, UK: Oxford University Press.

Ministry of Electronics and Information Technology. 2020. *Report by the Committee of Experts on Non-Personal Data Governance Framework*. 111972. Government of India. https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

Mueller, M. L. 2020. "Against Sovereignty in Cyberspace." *International Studies Review* 22 (4): 779–801. doi:10.1093/isr/viz044.

Nocetti, J. 2015. "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy." *Internet Policy Review* 4 (4) doi:10.14763/2015.4.380. Available at: https://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy [Accessed: 23 Apr. 2021].

Office of the United States Trade Representative. 2019. *National Trade Estimate Report on Foreign Trade Barriers*. March. Executive Office of the President of the United States. https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf

Panday, J., and J. Malcolm. 2018. "The Political Economy of Data Localization." *PAartecipazione e COnflitto* 11 (2): 511–527. doi:10.1285/i20356609v11i2p511.

Prasad, R. 2018a. "Ascendant India, Digital India: How Net Neutrality Advocates Defeated Facebook's Free Basics." *Media, Culture & Society* 40 (3): 415–431. doi:10.1177/0163443717736117.

Prasad, R. S. 2018b. Data Protection Committee Press Conference, Youtube *V*ideo. https://www.youtube.com/watch?v=chtyzyfsBk4

Press Information Bureau. 2019. "Commerce & Industry Minister holds discussions with CEOs of Indian IT Companies; urges them to explore new markets." Accessed 2 October 2019. https://pib.gov.in/newsite/PrintRelease.aspx?relid=192427.

Press Information Bureau. 2020. "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order." Accessed 15 December 2020. https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206

Press Trust of India. 2019. "India Counters Donald Trump on Digitisation, Calls Data 'New Form of Wealth'." *Ndtv*, June 28. New Delhi, India. https://www.ndtv.com/india-news/india-counters-donald-trump-on-digitisation-calls-data-new-form-of-wealth-2060832.

Punj, S. 2017. "India Today Conclave 2017: Mukesh Ambani pitches for 'keep in India'." *India Today*. https://www.indiatoday.in/conclave-2017/day-2-march-18-17/story/mukesh-ambani-india-today-conclave-2017-841016-2017-03-18.

Reserve Bank of India. 2018. "Storage of Payment Systems Data." Accessed 12 November 2019. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

Reserve Bank of India. 2019. "Survey on Computer Software and Information Technology-Enabled Services Exports: 2018-19." November 8. New Delhi, India. https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=48664

Schia, N. N. 2018. "The Cyber Frontier and Digital Pitfalls in the Global South." *Third World Quarterly* 39 (5): 821–837. doi:10.1080/01436597.2017.1408403.

Selby, J. 2017. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" *International Journal of Law and Information Technology* 25 (3): 213–232. doi:10.1093/ijlit/eax010.

Sengupta, D., and G. Aulakh. 2018. "Data belonging to Indians must reside within the country: Aruna Sundararajan." *Economic Times*, July 30. New Delhi, India. https://tech.economictimes.indiatimes.com/news/internet/data-belonging-to-indians-must-reside-within-the-country-aruna-sundararajan/65192468

Sharma, S. D. 2019. "Modinomics in India: The Promise and the Reality." *Asian Survey* 59 (3): 548–572. doi:10.1525/as.2019.59.3.548.

Sinha, A., and A. Basu. 2019. "The Politics of India's Data Protection Ecosystem." *Engage*, December 14. Accessed 20 March 2020. https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem

Srikrishna Committee. 2018. *Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. New Delhi, India. Accessed 5 October 2018. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

The Personal Data Protection Bill. 2019. 373. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

The Print. 2019. *Data Security Is Linked with National Security: Foreign Minister S Jaishankar*. Bengalaru, India. https://www.youtube.com/watch?v=1QARUTlLbG4.

Thomas, P. 2019. *The Politics of Digital India: Between Local Compulsions and Transnational Pressures. Media Dynamics in South Asia*. New Delhi, India: Oxford University Press.

van der Marel, E., M. Bauer, H. Lee-Makiyama, and B. Verschelde. 2016. "A Methodology to Estimate the Costs of Data Regulations." *International Economics* 146: 12–39. doi:10.1016/j.inteco.2015.11.001.

Verrastro, F., and S. Ladislaw. 2007. "Providing Energy Security in an Interdependent World." *The Washington Quarterly* 30 (4): 95–104. doi:10.1162/wash.2007.30.4.95.

Vila Seoane, M. F. 2020. "Normative Market Europe? The Contested Governance of Cyber-Surveillance Technologies." In *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*, edited by A. Calcara, R. Csernatoni, and C. Lavallée, 88–101. London, UK: Routledge.

Vila Seoane, M. F., and M. Saguier. 2020. "Cyberpolitics and IPE: Towards a Research Agenda in the Global South." In Vivares, E. (ed.), *Routledge Handbook of Global Political Economy: Conversations and Inquiries*, 702–718. New York and London: Routledge.

Wilson, J. D. 2015. "Understanding Resource Nationalism: Economic Dynamics and Political Institutions." *Contemporary Politics* 21 (4): 399–416. doi:10.1080/13569775.2015.1013293.

Wilson, J. D. 2017. *International Resource Politics in the Asia-Pacific: The Political Economy of Conflict and Cooperation*. Cheltenham, UK: Edward Elgar Publishing.