

# Digital Sovereignty: protectionism or autonomy?

BY DEBORAH ELMS, ASIAN TRADE CENTRE



# Contents

<b>INTRODUCTION</b>	3
Explaining digital sovereignty	5
<b>REGULATORY APPROACHES TO THE DATA ECONOMY</b>	6
<b>THE IMPORTANCE OF DATA FLOWS</b>	7
<b>DIGITAL ECONOMIES IN THE ASIA-PACIFIC REGION</b>	9
<b>DIGITAL SOVEREIGNTY IN THE EUROPEAN UNION</b>	10
Implications of European digital sovereignty	11
<b>REGULATORY REGIMES IN ASEAN</b>	13
<b>REGULATORY REGIME IN INDIA</b>	16
<b>REGULATORY REGIME IN CHINA</b>	17
<b>IMPACTS OF DIGITAL SOVEREIGNTY</b>	19
Impacts for large markets in the Asia-Pacific region	19
Impacts for small countries in the Asia-Pacific region	20
<b>CONCLUSION</b>	21
<b>RESEARCHER BIO: ASIAN TRADE CENTRE &amp; DR. DEBORAH ELMS</b>	22
<b>ENDNOTES</b>	23

# Introduction

A new line of thinking has emerged – one that sees the digital world as under-regulated and believes online activities unjustly take place outside government jurisdiction.

The phenomenal growth of the digital economy is nowhere more apparent than in Asia and the Pacific, home to 4.2 billion people. Although the region’s diversity in terms of income level, population size, and geography<sup>1</sup> has varied the uptake of information and communications technology (ICT), its rapid spread has enabled economic growth and development.

A new line of thinking has emerged too – one that sees the digital world as under-regulated and believes online activities unjustly take place outside government jurisdiction. Welcome to “digital sovereignty”, where the internet and the data generated by its use is subject to traditional conceptions of territoriality. As a result, governments are rethinking traditional approaches to the digital economy, risking negative outcomes.

To many – though not all – the internet is ubiquitous. Connectivity is omnipresent in our daily lives, prompting internet traffic to grow 127 times between 2005 and 2021.<sup>2</sup> Today, the internet underwrites essentially every sector of modern society, from communications to entertainment to global commerce and finance.

At its core, the internet relies on information: the data flows that make email, e-commerce platforms, and financial transactions possible. Growing even faster than internet connectivity is the volume of data generated, created, and used to facilitate internet functionality. According to the International Data Corporation, by 2025 the world will enable an estimated 175 trillion gigabytes of data.<sup>3</sup> Data is deeply entrenched in nearly every aspect of the economy.<sup>4</sup>

The Covid-19 pandemic has only accelerated these trends, as everything from commercial activities to education to entertainment have increasingly moved online, especially where pandemic-related restrictions were more severe.<sup>5</sup>

## Definition of data

For the purposes of this paper, the term data refers to digital data, which is information in any interpretable form created, transmitted, processed, or stored via digital means.

The internet also facilitates the transfer of large amounts of data for services such as file transfers and communications platforms. Internet-reliant technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and 5G are profoundly impacting how we conduct business and live our lives. Google CEO Sundar Pichai has even claimed that the impacts of AI on daily life will be “... more profound than electricity or fire.”<sup>6</sup> From AI used for early cancer detection to IoT-enabled smart power grid technology, these next generation technologies are potentially society changing.<sup>7,8</sup>

Unlocking the transformative potential of these technologies relies on free cross-border flow of data.

Until recently, discussions urging for globally consistent regulation for data governance have been limited. In the absence of domestic regulation, companies interacting with users in the digital space were loosely guided by international privacy and data protection principles, such as the Asia Pacific Economic Cooperation (APEC) Privacy Framework, the Organization for Economic Cooperation and Development (OECD) Privacy Framework, and the Council of Europe (COE) Convention of Data Privacy.

Governments and the general public are starting to realize that regulation has not kept pace with the emerging technologies' increasing reliance on data innovation. In general, this concern has been framed around protecting user privacy. Internet users increasingly realize that their information is valuable to the companies with whom they interact online, who use user data to develop their e-commerce strategies. Ostensibly to protect internet user privacy, governments increasingly see data as a target for regulation.

Regulatory regimes around the world are pushing to claim jurisdiction over data. Informed by "data sovereignty," governments are coming to see data as a commodity like any other – one that needs to be owned, controlled, and protected.

Regulatory regimes around the world are pushing to claim jurisdiction over data. Informed by "data sovereignty," governments are coming to see data as a commodity like any other – one that needs to be owned, controlled, and protected. To them, data is an intangible asset no different from other intangible assets like intellectual property.

This perspective can rationalize that traditional concepts of territoriality and jurisdiction apply and justify government imposition of taxes or localization requirements on data flows. Governments can also use the language of digital or data sovereignty as part of an effort to dramatically increase the role of domestic firms or domestically derived technology and data to ensure greater control over the domestic economy.

Such an approach to regulation can complicate and fragment the global digital economy, in which data freely crosses borders for processing or storage. The spread of digital or data sovereignty as a perceived virtue may radically alter the future digital trends that appear to be unstoppable.



Informed by "data sovereignty," governments are coming to see data as a commodity like any other – one that needs to be owned, controlled, and protected.

The vigor with which major economies – including Europe, India, China, and beyond – are pursuing data sovereignty policies is concerning, particularly as research on the issue is still emerging. Policymakers are proposing regulations without understanding their inevitable effect – an internet with borders that threatens to reverse trends in growth and equity. This paper focuses attention on the topic of digital sovereignty and offers insight into the potential consequences of such regulations in Asia and the Pacific.

The concept of digital or data sovereignty is evolving rapidly. The two terms are often used together or merged with other similar labels. This paper examines the increasing use of digital sovereignty as a concept and looks at two aspects that policies address most frequently: cross border data flows and the location of data storage (often called data localization.) The purpose of the paper is not to provide definitive answers to the growing use of sovereignty applied to the digital realm, but to highlight some of the issues that are being tackled or addressed by governments, including the European Union, ASEAN, India, and China.

### Explaining digital sovereignty

As an emerging policy area, digital sovereignty is by nature a “fuzzy” concept. A widely agreed upon definition is difficult to come by, and those who speak of the issue tend to use the term interchangeably with other terms like data sovereignty or cyber sovereignty. As implied in the term, digital sovereignty combines two subject areas – that of the digital realm and that of sovereignty, a term indicating supreme authority over a geographic space. Usually, the term “sovereignty” ties that authority to a specific jurisdiction or territory, and describes self-determinism exercised by individual states. The concept of digital sovereignty blends these previously unconnected concepts, describing a situation in which a government claims supreme authority over the non-territorial realm of cyberspace.

Viewing data as a vulnerability, governments may increasingly pursue restrictions on cross-border data transfers and set security standards for businesses dealing with user data.

While many governments are concerned with the use of citizens’ personal data, cyber sovereignty policies typically have cybersecurity and anti-crime elements as well. Viewing data as a vulnerability, governments may increasingly pursue restrictions on cross-border data transfers and set security standards for businesses dealing with user data.

# Regulatory approaches to the data economy

Approaches to data regulation are informed by the regulators' understanding of the digital realm. Broadly, these perspectives fall into two opposing categories: that of *cyber exceptionalism* and that of *digital sovereignty*.

Approaches to data regulation are informed by the regulators' understanding of the digital realm. Broadly, these perspectives fall into two opposing categories: that of *cyber exceptionalism* and that of *digital sovereignty*. Proponents of the cyber exceptionalism approach argue that the digital realm is distinct and requires a regulatory approach that is fundamentally different from other non-digital elements of society.<sup>9</sup> This perspective has been foundational to the development of the internet as we know it today: a decentralized network accessible by users (almost) anywhere in the world.

Arguably, this perspective still best describes the digital world at present. The internet remains mostly borderless. The physical location of users, servers, and businesses offering digital services remains largely irrelevant. Under this regime, national borders have little effect on data, which flows freely for any use.

This contrasts with the concept of digital sovereignty, which argues for nations to have full control over the digital realm as it exists within their borders. Digital sovereignty seeks to reflect a nation's territorial dimension onto the digital world. Generally, arguments for digital sovereignty posit that because internet infrastructure such as data centers have physical locations, traditional notions of jurisdiction should apply to the data within the centers.



Generally, proponents of digital sovereignty argue that because internet infrastructure such as data centers have physical locations, traditional notions of jurisdiction should apply to the data within the centers.

# The importance of data flows

Existing data networks are complex and often international in scope. Even a simple digital transaction like sending an email requires information or data to be broken down into small “packets” which are sent literally around the world to be reassembled at the final destination.

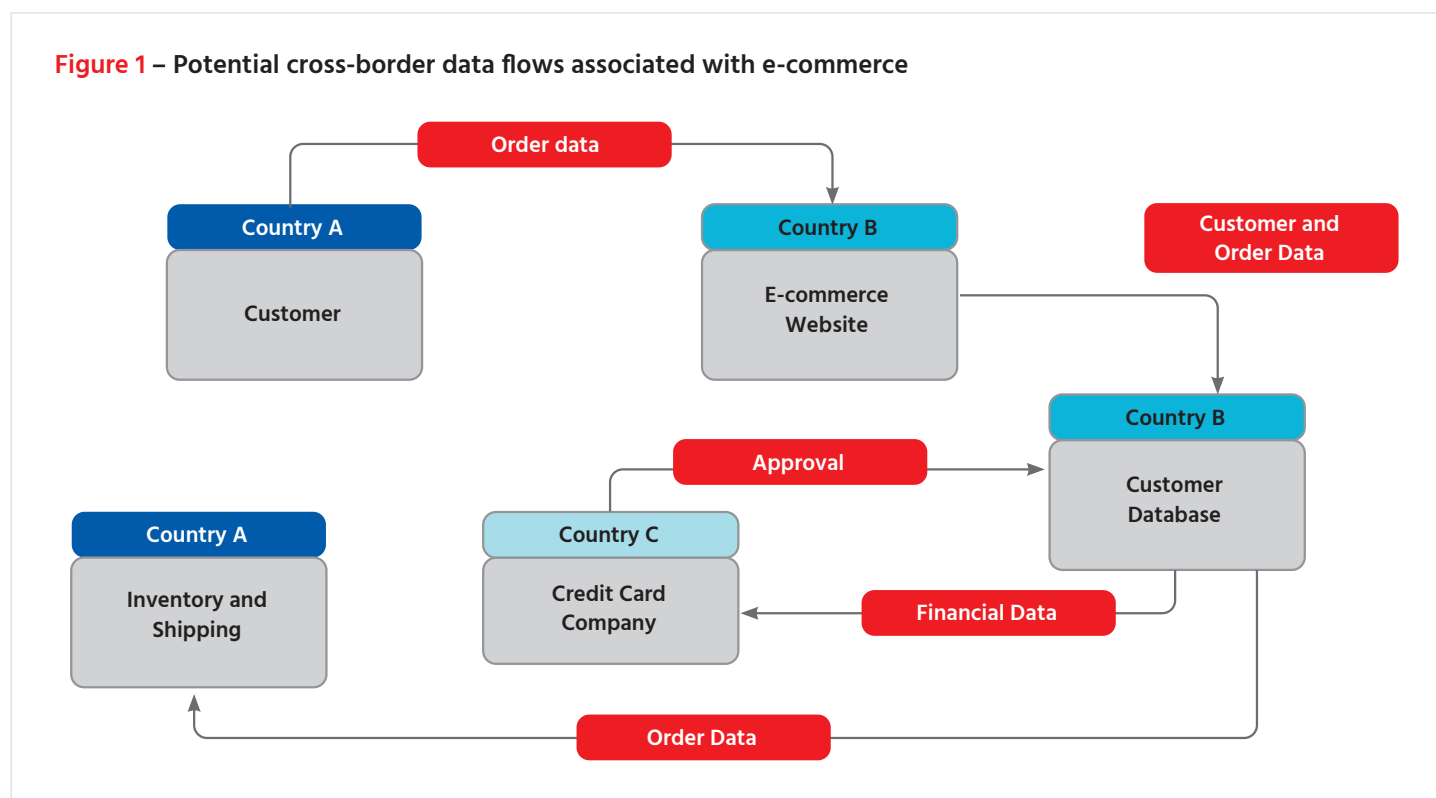
Existing data networks are complex and often international in scope. Companies that provide services such as web hosting and cloud computing need physical locations for servers that store and process data. The homes for these servers are known as data centers. These data centers are distributed across the globe and tend to be located where there is sufficient infrastructure, inexpensive energy, and a local talent pool to meet the centers’ needs.

Hence, based on these criteria, not every country is a suitable site for a data center and cross-border data flows are essential for basic internet functionality. Even a simple digital transaction like sending an email requires information or data to be broken down into small “packets” which are sent literally around the world to be reassembled at the final destination. The distributed nature of the internet helps make it possible for information to continue to flow even if one or more nodes of the transmission chain are suddenly unavailable for use.

Data flows are even more complex when considering digital commerce. A buyer and seller physically located in two different countries may see their data cross several borders to complete a transaction. The company that hosts the e-commerce platform, as well as the relevant financial institutions, data centers, and web hosting companies may all be in different countries.

Requirements for data localization – wherein certain forms of data are not permitted to cross borders – run against current data network arrangements.

**Figure 1 – Potential cross-border data flows associated with e-commerce**



While restrictions on certain types of data flows may be justified for privacy or security reasons, poorly thought-out regulation may burden business or increase costs to consumers, as accessing internet-based services becomes more difficult and expensive.

Internet connectivity is vital for the day-to-day operations of businesses. Even the smallest of businesses in developing countries might use an email account to interact with customers or keep records in the cloud rather than on paper. Using internet tools to interact with customers generates and employs user data. With the growing push for restrictions on data flows, businesses may face difficulties in doing so.

Not only do restrictions on data flows complicate e-commerce, but they also threaten to amplify existing inequalities and dampen ICT uptake in developing countries.

Not only do restrictions on data flows complicate e-commerce, but they also threaten to amplify existing inequalities and dampen ICT uptake in developing countries. Though they can be difficult for businesses to navigate, countries such as China and India may have large enough markets and the technological capabilities necessary to keep data in-country. Ignoring that such an arrangement would make internet services more expensive, these markets probably have the facilities and domestic tech industry talent to run in-country data centers to manage data localization requirements.

In contrast, many developing countries do not. Furthermore, some of these markets – such as small island developing states (SIDS) in the Pacific – are likely too small to encourage internet service providers to maintain a presence. Consequently, small states enacting restrictive data regulations may see e-commerce companies and other internet-enabled services pull out and lose the benefits of ICT-enabled growth.

Data localization requirements, restrictions transferring data across national borders, and laws granting government access to companies' user data may present significant barriers to trade in both goods and services.

Strict data management regimes that impede cross-border data flows may act as non-tariff barriers to trade. Data localization requirements, restrictions transferring data across national borders, and laws granting government access to companies' user data may present significant barriers to trade in both goods and services. These types of laws can severely disadvantage foreign companies in favor of domestic competitors.

Indeed, governments hoping to build up domestic digital industries and shield them from competition from tech giants are clearly pursuing digital sovereignty as a form of protectionism.

As the analysis of data patterns is necessary to detect and address security threats, cross-border data flows are also crucial to efforts towards stronger global cybersecurity efforts.



# Digital economies in the Asia-Pacific region

Measuring the precise size of the digital economy can be challenging. Like e-commerce services, digital platforms may not be physically located where services are bought or sold, and interactions with them are not always financial (although platforms may harvest and resell users' data to turn a profit.)<sup>10</sup> As a result, macroeconomic statistics are unlikely to capture the full value of digital transactions in any given jurisdiction. Current measurements take no account of the benefits from unpriced goods generated as a part of ongoing digitalization, like data and knowledge.<sup>11</sup>

Furthermore, there is no effective mechanism to measure the knock-on benefits from data markets. Although in 2017 the aggregate revenue of European firms in the data economy was valued at €65 billion, the United Nations estimates the total economic impact of the data market to be €335.6 billion.<sup>12</sup> When indirect and induced impacts are factored into estimates, the digital economy becomes much larger than we can effectively measure.

According to the Asian Development Bank (ADB), the digital sector in Asia is expected to grow by US\$3.1 trillion between 2021 and 2025, mainly due to productivity gains and increased demand for digital services.

According to the Asian Development Bank (ADB), the digital sector in Asia is expected to grow by US\$3.1 trillion between 2021 and 2025, mainly due to productivity gains and increased demand for digital services.<sup>13</sup> Sub-regions with small digital economies stand to gain the most as they benefit from accumulating productivity, investment gains, and increased access to internet connectivity in previously unserved areas. The Pacific region for example, may see an average yearly increase of 26.8% in GDP, 15.6% in trade, and 26.1% in employment due to a rapidly growing digital sector.<sup>14</sup>

In 2020, digital platforms such as e-commerce, tele-medicine and online education, and online streaming services saw rapid growth due to the pandemic. With continued restrictions in many jurisdictions, these trends show no signs of abating.

The following sections describe the state and implications of digital sovereignty policies in the European Union, ASEAN, India, and China. The likely effects of these policies are then described, noting that small and large economies are likely to face different consequences in line with market size.

# Digital sovereignty in the European Union

Any account of digital sovereignty must include the European approach. As an example of both early and comprehensive data protection regulation, the European data regime has inspired similar laws abroad and provided a framework for their design and implementation.

For President of the European Commission Ursula von der Leyen, “technological sovereignty” is a key policy priority for her 2019-2024 term.<sup>15</sup> In 2020, she remarked that, “Digital Sovereignty is not just an economic concept. We are a Union of values. One of the greatest questions is: how can we uphold our values?”<sup>16</sup> Driven by concern over the growing dominance of US and Chinese companies over the global data economy, the European Union (EU) has enacted several policies to enhance privacy and boost investment in 5G, Artificial Intelligence (AI), cloud computing, and Internet of Things (IoT) – which are all next generation technologies in which the EU has not kept pace with its competitors.<sup>17</sup>

Central to the EU’s data governance is the General Data Protection Regulation (GDPR), which came into effect in 2018. Comprehensive and restrictive, the law compels businesses – regardless of their physical location – to comply with the regulations when interacting with all “natural persons” under EU law.

Central to the EU’s data governance is the General Data Protection Regulation (GDPR), which came into effect in 2018.<sup>18</sup> Comprehensive and restrictive, the law compels businesses – regardless of their physical location – to comply with the regulations when interacting with all “natural persons” under EU law. Thus, any interaction with EU citizens within the EU is governed by the GDPR. Specifically, businesses must grant users ultimate control over their data by explaining how the data will be processed and providing the option to opt out from data gathering or delete personal data gathered in the past.<sup>19</sup> Penalties for violating the law can be severe and include fines of up to €20 million or 4% of global annual turnover.<sup>20</sup>

Notably, as EU authorities claim extraterritorial jurisdiction, a business outside of the EU and catering to non-EU customers can still be held accountable for gathering user data if an EU resident’s data is gathered when visiting the business’s website.<sup>21</sup>

The EU acknowledges that the cloud services and data storage industry is vital and dominated by non-European companies. Hence the EU plans to develop a Federated Data Infrastructure system called GAIA-X,<sup>22</sup> which will establish common standards for cloud services that fit with “European values” and the GDPR.<sup>23</sup> In effect, the GAIA-X seeks to unite European data markets into a more contiguous bloc and allows for the establishment of a cloud and data storage market not dominated by foreign companies. Additionally, the initiative will protect European data centers from GDPR-like laws abroad that seek access to extraterritorial data hosted in the EU.<sup>24</sup>

The GDPR is widely seen as the world’s most comprehensive data protection regime. When combined with the GAIA-X Initiative, it becomes clear that the EU sees technological sovereignty as essential in protecting European autonomy in the digital world and beyond. European regulators are increasingly aware that data is essential in transformative technologies such as AI and seek to establish global standard-setting rules to govern how and where data can be gathered and used.



Central to the EU's data governance is the General Data Protection Regulation (GDPR), which came into effect in 2018. The GDPR is widely seen as the world's most comprehensive data protection regime.

### Implications of European digital sovereignty

Rather than maintain different websites for different regions, sites catering to markets beyond the EU simply apply EU requirements globally. This demonstrates the *Brussels Effect*, whereby EU regulations extend beyond EU borders as market mechanisms externalize domestic laws.

The GDPR has been largely successful in giving users more control over the gathering, processing, and storage of their data. Those inside the EU accessing nearly any website are prompted to either accept or deny permission for the website to gather their data for certain purposes. Further, rather than maintain different websites for different regions, sites catering to markets beyond the EU simply apply EU requirements globally. This demonstrates the *Brussels Effect*, whereby EU regulations extend beyond EU borders as market mechanisms externalize domestic laws.<sup>25</sup> While user concerns over privacy may extend beyond national borders, the free and unhindered flow of data remains central to the internet and the digital economy.

Importantly, the GDPR drove a strong market concentrating effect, both within the EU and beyond.<sup>26</sup> Ahead of the GDPR coming into effect, regulators predicted that the law would decrease costs for businesses, as harmonized rules would decrease compliance costs. In reality, Google – already a market leader – emerged as a clear winner by providing web tracking technology that is GDPR compliant. Due to the advantages of economies of scale, Google was able to quickly pivot to accommodate the GDPR, subsequently increasing market share by 7.2% in analytics and 5.4% in advertising.<sup>27</sup>

Large firms can reconfigure their data networks and build new data centers within EU territory to satisfy the conditions laid out by the law. Firms without such abilities face significant challenges. The large gains for tech giants may have prompted the proposal for the GAIA-X initiative – an overt attempt to build up Europe's data economy in pursuit of digital sovereignty.

The GDPR complicates the notion of territoriality. It reinforces traditional concepts of territoriality – wherein a national (or in this case, a supranational) government has ultimate rule-making authority within a given territory – but goes further. The law applies to the personal data of all data subjects within the EU, even when

that data is processed, stored, or gathered beyond EU borders. EU authorities are claiming extraterritorial jurisdiction<sup>28</sup> and the GDPR looks to regulate based on the source of the data rather than the location of data storage or processing.

It is worth noting, however, that EU authorities likely have little ability to enforce these extraterritorial claims, especially if regulation conflicts with the data management regime in the country where the data is physically hosted.

It is worth noting, however, that EU authorities likely have little ability to enforce these extraterritorial claims, especially if regulation conflicts with the data management regime in the country where the data is physically hosted.<sup>29</sup>

Through the GDPR and GAIA-X initiative, the EU is likely to make an impact beyond its borders. The global south looks to the EU when drafting their own regulations – and digital sovereignty is no different.

What has emerged is a divergent data regulation landscape. Again, large markets may be able to absorb and compensate for such divergence. In contrast, smaller developing markets may struggle in the face of more difficult and expensive cross-border data transfers. In small markets, e-commerce and tech companies may even prefer to leave a country entirely rather than deal with high compliance costs and raised regulatory risks. In a world of an increasingly “bordered” internet, developing countries with smaller domestic markets stand to lose the most.

# Regulatory regimes in ASEAN

ASEAN member states have varying capacities and priorities in terms of regulating the digital realm. As a result, there is great disparity in terms of the severity of regulatory requirements for data, as well as in buy-in for digital sovereignty. Some states have strict regulations governing how, when, and why data is gathered, while others have no comprehensive laws to address data privacy issues. There are no legally binding data protection laws ASEAN-wide. However, several initiatives are in place to account for data's growing role in the global economy and to best position ASEAN in global digital transformation.

In the ASEAN Digital Masterplan 2025, which seeks to foster greater regulatory convergence, member states are encouraged to pursue alignment on data protection rules, data localization, and cross-border data transfers.

In the ASEAN Digital Masterplan 2025, which seeks to foster greater regulatory convergence, member states are encouraged to pursue alignment on data protection rules, data localization, and cross-border data transfers.<sup>30</sup> The Masterplan further acknowledges the need for interoperability of standards with the GDPR,<sup>31</sup> which has influenced data regulation by inspiring similar regulation broadly and imposing conditions for cross-border data transfers. Regardless of where they operate, the GDPR allows businesses to transfer data out of the EU by using data transfer mechanisms such as Standard Contractual Clauses or an EU adequacy decision.

ASEAN has created two mechanisms for managing cross-border data flows: the use of contractual clauses and a certification mechanism<sup>32</sup> – both of which are voluntary, not mandatory. Future digital plans by ASEAN, including the entry into force of the ASEAN E-Commerce Agreement, may include additional commitments related to data flows and data storage.

At the national level, ASEAN members have different approaches to regulating data flows. Some have no comprehensive data governance policies at all. Of these countries, several have enacted laws that are overtly inspired by the GDPR, although they are not necessarily compatible with EU laws.

In some member states, as is common outside of ASEAN, data restrictions can take place at the sector level, instead of being a broadly comprehensive policy response to data concerns.

In some member states, as is common outside of ASEAN, data restrictions can take place at the sector level, instead of being a broadly comprehensive policy response to data concerns. Often these sectoral restrictions on, for example, health information, can be especially challenging as it is not always clear to other branches of government or to companies, when such restrictions may or may not apply, leading to compliance challenges.

## Brunei

In May 2021, Brunei began consultations on the draft Personal Data Protection Order (PDPO). When implemented, the PDPO will be the country's first comprehensive data protection law and apply to any private sector organization that collects data in Brunei, regardless of its location.<sup>33</sup> Drawing on the GDPR and ASEAN examples, the PDPO will contain provisions that are likely to be treated as *de facto* localization requirements, wherein personal data cannot be transferred out of the country unless PDPO standards are met. Thus, to avoid breaching the incoming law, businesses without a local presence may need to buy into local data centers to meet these requirements.<sup>34</sup>



ASEAN member states have varying capacities and priorities in terms of regulating the digital realm. Some have no comprehensive data governance policies at all.

Data protection laws in Indonesia, Malaysia and the Philippines draw heavily from the EU's GDPR.

### Indonesia

While Indonesia does not have a comprehensive data protection law, strict regulations have been put in place governing elements of the digital economy. Government Regulation No. 71 Year 2019, which draws heavily on the GDPR, overtly seeks to enforce Indonesia's data sovereignty. The regulation stipulates that "Electronic Systems" operators must register with the government, meet expertise requirements by hiring Indonesians, and ensure operators in the public domain process and store data within Indonesian territory.<sup>35</sup> Excluding financial services, companies acting in the private domain are not subject to these requirements.<sup>36</sup>

### Malaysia

The Personal Data Protection Act (PDPA) came into effect in 2013. The law does not apply to data processed outside of Malaysia or to non-commercial transactions, such as a social media company gathering user data for analytics purposes.<sup>37</sup> Instead, the law focuses on ensuring end-user consent for data gathering; hence Malaysians accessing websites must be asked for permission before the website can track user data.<sup>38</sup> Personal data can be freely transferred out of Malaysia to a specific list of countries where the data protection regime is judged as equally strict.<sup>39</sup> The government of Malaysia is currently reviewing the PDPA as it seeks to update the law in line with regional and international standards. Officials have said that they will draw on the GDPR.<sup>40</sup>

### The Philippines

The Philippines has overtly drawn on GDPR principles in designing its domestic data regime, which consists of the Data Privacy Act of 2016 (DPA) and the National Privacy Commission's six Implementing Rules and Regulations (IRR).<sup>41</sup> As in the GDPR, the DPA and IRR are extraterritorial. The regulations cover Philippine citizens, regardless of whether they are in the Philippines or abroad. However, the regulations make no explicit requirements for data localization or transfers to foreign jurisdictions.<sup>42</sup>

### Singapore

Singapore's Personal Data Protection Regulations (PDPR) were first enacted in 2012 and updated in February 2021.<sup>43</sup> The PDPR is mainly concerned with personal data and applies extraterritorially to any organization that collects data from Singaporeans via online mechanisms.<sup>44</sup> As with other ASEAN states, the PDPR binds companies to transferring user data out of the country only where the standard of protection is comparable to the regulations.<sup>45</sup> The Personal Data Protection Commission is responsible for enforcing the regulations and has assessed dozens of fines.<sup>46</sup>

### Thailand

Influenced by the GDPR, Thailand passed the Personal Data Protection Act in 2019. The law has extraterritorial scope and applies to all organizations that collect or process the personal data of Thai residents, regardless of where the organization is physically located.<sup>47</sup> Furthermore, foreign organizations that seek to process Thai data outside of the country must employ a Data Protection Officer and a representative in the country.<sup>48</sup>

### Vietnam

Drawing inspiration from China's Cybersecurity Law, and to a smaller extent the GDPR, Vietnam's 2019 Law on Cybersecurity is perhaps the most overt effort toward data sovereignty among ASEAN countries. Going beyond privacy and cybersecurity rules, the law requires offices to be located in-country and storage of user data in Vietnam, which must be handed over to the authorities when asked.<sup>49</sup> According to the Vietnam Digital Communications Association, the law has the potential to negatively impact the economy – analysts are concerned that GDP growth could fall by an estimated 1.7% and foreign investment by 3.1%.<sup>50</sup>

### Cambodia, Lao PDR, and Myanmar

Currently, Cambodia, Lao PDR, and Myanmar do not have comprehensive data regulations in place.

Drawing inspiration from China's Cybersecurity Law, and to a smaller extent the GDPR, Vietnam's 2019 Law on Cybersecurity is perhaps the most overt effort toward data sovereignty among ASEAN countries.

# Regulatory regime in India

In July 2021, India banned Mastercard from issuing new debit, credit, and prepaid cards in the country. Why? India's rules for data localization.<sup>51</sup> According to the government, by making use of foreign data centers to store and process user data, Mastercard is running afoul of requirements mandated by India's Reserve Bank to store and process payments data in the country.<sup>52</sup>

Critics of India's approach suggest that the regulations are not only about privacy. Arguing that the rules provide a competitive advantage to India's fast-growing domestic payments sector, critics suggest that the regulations reflect the Indian Government's push for digital sovereignty.<sup>53</sup>

Several pieces of concurrent legislation dictate India's regulatory approach. These include the Information Technology Act of 2000, most recently updated in 2011 as the Information Technology Rules, which govern personal data, commonly known as SPDI. The rules constrain companies in what types of data they can gather and prohibit the transfer of such data to countries where similar standards of data protection are not in place.<sup>54</sup>

Together with the IT Act, SPDI seeks to confirm India's constitutional right to privacy. The move reflects the government's ongoing prioritization of digital transformation, which includes the Digital India Initiative, a multipronged government strategy carried out through e-government services such as universal digital identification and digital infrastructure.<sup>55</sup>

In 2019, India proposed the Personal Data Protection Bill (PDPB), which is perhaps the law most like the GDPR in scope outside of the EU. Unlike the GDPR, however, the PDPB forbids transfers abroad for "critical personal data," the parameters of which are vaguely defined.

In 2019, India proposed the Personal Data Protection Bill (PDPB), which is perhaps the law most like the GDPR in scope outside of the EU. Like the GDPR, India's PDPB makes claims of extraterritoriality, permits the government to compel companies access to user data upon request, and requires consent before gathering users' data.<sup>56</sup> Unlike the GDPR, however, the PDPB forbids transfers abroad for "critical personal data," the parameters of which are vaguely defined.<sup>57</sup>

Furthermore, the PDPB enables government audits of data fiduciaries and enforces registration requirements.<sup>58</sup> Businesses are unlikely to be simultaneously compliant with both EU and PDPB rules. This raises the complexity and risks to the types of data transfers that sustain international e-commerce as we know it today. In effect, the proposed law would greatly restrict cross-border data flows and allow the government nearly unrestricted access to user data.

India is also considering a framework to govern non-personal data. Again, the aim is to harness and realize the economic benefit of data in a way that serves India and its people. The Committee's proposals include the notion of mandatory sharing of certain types of datasets for sovereign purposes, public good and business purposes.<sup>59</sup>



# Regulatory regime in China

Central to China's digital strategy is the tightening of government control of the digital realm in terms of online content, data protection, and the preferential treatment of domestic business.

China's policy of "Cyber Sovereignty" has informed the country's stance on data governance and technological development. Central to China's digital strategy is the tightening of government control of the digital realm in terms of online content, data protection, and the preferential treatment of domestic business.<sup>60</sup> The Chinese government seeks to territorialize China's digital space and limit the power of private sector actors, both foreign and domestic. Legislatively, China's approach to digital sovereignty takes several forms: The Cybersecurity Law (CSL) of 2016, the Data Security Law (DSL) that will come into force in September 2021, and the Personal Information Protection Law (PIPL), the second draft of which was published in October 2020.

Together, the laws can be expected to greatly increase government oversight and influence. Along with their like-minded counterparts in Russia, China's government has pushed for reform of key international organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union (ITU), that maintain the status quo of the digital realm.<sup>61</sup> Running against the multi-stakeholder model of internet governance, China seeks to territorialize its online space and limit foreign influence.

## The Cybersecurity Law (CSL)

Enacted in 2017, the CSL is applied to the networked digital realm as it exists within the physical borders of China. The law seeks to protect the sovereignty and security of China's cyberspace, protect the interests of citizens and organizations, and promote the digitization of the economy and society.<sup>62</sup> The law imposes standards for data protection and cyber security obligations for network operators, establishes a pre-sale certification mechanism for vaguely defined critical network equipment, and imposes protections for data collected during the operation of networks.<sup>63</sup>

Additionally, the law requires that any person or organization using networks must not engage in any behavior that undermines social morality and the national interest, or subverts national sovereignty.<sup>64</sup> The CSL is fairly limited in its applicability as the onus is placed on network operators. However, vague requirements outlined in the law contribute to compliance costs and regulatory risks for foreign firms seeking access to the Chinese market.

## The Data Security Law (DSL)

Soon coming into force, the DSL imposes specific restrictions on data, both within the geographic borders of China and beyond. Export controls are to be imposed on data related to national security, national interests, or the fulfilment of international obligations. The law also allows for reciprocal bans on countries that restrict data transfers to China.<sup>65</sup> Additionally, the DSL prohibits the transfer of any data stored in China to foreign authorities without the express consent of the Chinese government. Thus, authorities from countries that claim extraterritoriality in their data laws will need permission before they are granted access to their citizens' data stored in China.<sup>66</sup> Although they may claim extraterritorial rights to their citizens' data, the Chinese government is likely to resist other countries' efforts to do the same.



Recently Beijing had named and shamed the country's biggest tech giants, including Tencent, Baidu, and Alibaba for illegal access and excessive collection of user data.

### The Draft Personal Information Protection Law (PIPL)

Taking inspiration from the EU's GDPR, the PIPL will provide the overarching regulatory framework for personal data protection, currently governed by a patchwork of laws, regulations, and rules.

The second draft of the PIPL, released in April 2021, is undergoing a round of public consultations ahead of the third and final draft of the law.<sup>67</sup> Taking inspiration from the EU's GDPR, the PIPL will provide the overarching regulatory framework for personal data protection, currently governed by a patchwork of laws, regulations, and rules. The law will establish the need for informed consent when gathering, processing, and storing user data in China.<sup>68</sup> The law will also establish an independent regulatory body responsible for monitoring compliance.<sup>69</sup>

Though vaguely defined, the law appears to target companies with large numbers of users. This suggests that the law is a part of Beijing's efforts to rein in tech giants such as Alibaba, which was fined US\$2.82 billion in 2021 for alleged anti-monopoly activities.<sup>70</sup>

# Impacts of digital sovereignty

In a report published in July 2020, the Information Technology and Innovation Foundation found that with a one-point increase in a nation's data restrictiveness, gross trade output decreases 7%, productivity decreases 2.9%, and downstream prices increase 1.5% over five years.

Regulatory regimes that seek to localize and territorialize their data are enacting laws without evidence to support their claims. These efforts may prove counterintuitive, as restrictive data regimes are associated with a decrease in gross trade output and productivity. In a report published in July 2020, the Information Technology and Innovation Foundation found that with a one-point increase in a nation's data restrictiveness, gross trade output decreases 7%, productivity decreases 2.9%, and downstream prices increase 1.5% over five years.<sup>71</sup>

If more countries move toward digital sovereignty, the world may transition to a new era, one wherein the cross-border data transfers that enable digital connectivity become more difficult or even impossible.

Countries are justified in their concerns over the security and privacy of their data. Many governments have only recently realized the power of data – and the immense economic benefits of data innovation for businesses, governments, and individuals. But digital sovereignty is not only about ensuring citizens' rights are protected. Countries pursuing data sovereignty may see the regulatory approach as part of a multi-faceted effort to boost the domestic technology sector. In short, data sovereignty policies appear to be a form of protectionism. They appear to be enacted for the benefit of domestic firms and at the expense of the free flow of digital goods and services.

Many regulatory regimes pursuing digital sovereignty draw inspiration from the EU's GDPR. As the GDPR has been in force for several years and has been judged to be effective, other countries believe they are justified in enacting similar laws. When the GDPR was the only comprehensive data privacy law, businesses could easily comply; they simply applied EU standards globally to avoid increased compliance cost and risk.

As countries enact their own rules – different but equally strict – compliance becomes more difficult.

Soon, businesses may need to tailor their data policies to individual countries or to like-minded blocs, greatly increasing compliance costs and risks. Data may no longer flow freely across borders. International trade that relies on data becomes more difficult and expensive.

Soon, businesses may need to tailor their data policies to individual countries or to like-minded blocs, greatly increasing compliance costs and risks. With increased uncertainty, we may soon see a reversal of the digital trends of the past decades. Data may no longer flow freely across borders. International trade that relies on data becomes more difficult and expensive.

## Impacts for large markets in the Asia-Pacific region

Large markets in the Asia-Pacific region are likely to fare comparatively well in a world of data sovereignty. These countries, and the businesses seeking access to their markets, are likely able to adjust to the regulatory changes that come with the implementation of restrictive data management policies. Take, for example, localization requirements in China that bar sensitive data from leaving the country. To comply, a multinational company storing data would need to make use of an in-country data center, of which there are hundreds in China.<sup>72</sup>

Although China's data policies will disrupt existing business models, the digital infrastructure needed to comply with the new laws is widely available. Hence the risks, compliance costs, and financial burden of onshoring data is likely offset by the benefits of continued access to the Chinese market. After some short-term disruption, businesses will adjust their operations to maintain their presence in China.

Indeed, based on the EU's experience, large markets can expect to see a market concentrating effect for digital service providers. Larger firms with more resources and economies of scale facilitate compliance with new regulations. In India and China, where the overt pursuit of digital sovereignty has a decidedly protectionist tinge, domestic firms are poised to gain market share.

### Impacts for small countries in the Asia-Pacific region

Small countries in the region must carefully consider the trade-offs of pursuing digital sovereignty. On one hand, these countries must make significant efforts to instigate and facilitate economic digital transformation or risk being left behind. However, small countries without a domestic tech sector do not benefit from the growth in jobs, expertise, and knock-on effects experienced by those who do.

It is counterproductive to place restrictions on data flows and to enact localization requirements when the infrastructure and expert workforce necessary to maintain this infrastructure are not already present in the country.

Comparatively, small economies are generally less digitized and less developed. As such, the digital divide threatens to become larger and to exacerbate already apparent development gaps. Large economies – and some of the smaller ones too – seem to view digital sovereignty policies as a means to shoehorn a digital ecosystem into being. It is counterproductive, however, to place restrictions on data flows and to enact localization requirements when the infrastructure and expert workforce necessary to maintain this infrastructure are not already present in the country. Protectionist policies are particularly hazardous for small countries.<sup>73</sup>

As such, enacting severe restrictions on cross-border data flows, which necessarily make international trade more difficult, is counterintuitive when pursuing economic development.

The real danger of digital sovereignty will be revealed when a small country looks to enact regulations similar to those seen elsewhere in Asia. With little to no digital infrastructure already in place, companies present in these markets are unlikely to be prepared for localization requirements and transfer bans. Given the size of the markets in these countries, businesses may simply choose to cease operations rather than deal with the high compliance costs and risks. This could leave the least-developed countries in the region without access to digital services – the very thing digital sovereignty policies seek to boost.

# Conclusion

Policies seeking to achieve digital sovereignty are fraught with risks, both for large and small economies. Increasingly aware of the value of their data, countries are seeking to territorialize and localize data for national benefit. But digital sovereignty has not been evaluated with a critical eye. Economic analyses of the effects are missing from government decision-making processes. A careful understanding of the types of processes and business models that rely on information flows is also often missing.

The very concept of digital sovereignty runs counter to the founding principles of the internet and may negate the transformative power of next-generation digital technologies.

The impact of such policies is largely unknown, especially if states are covered by a patchwork of incompatible data transfer requirements. However, the very concept of digital sovereignty runs counter to the founding principles of the internet and may negate the transformative power of next-generation digital technologies. A world wherein data cannot cross borders is one where international trade is more difficult, cross-border communication is more inconvenient, and opportunities shrink.

Countries argue that they are simply looking to protect their interests. Yet the paucity of evidence to support policymaking oriented towards digital sovereignty is worrying. Large countries may be able to successfully erect digital borders. Small countries that attempt to do the same may face unintended and overwhelmingly negative consequences. Balancing privacy, security, and economic growth requires nuanced, careful data policies that accept the importance of cross-border data flows. Without such an approach, the pursuit of digital sovereignty risks negative consequences, with small countries bearing the brunt.



In the absence of a nuanced approach to balancing privacy, security, and economic growth, the pursuit of digital sovereignty risks negative consequences, with small economies and businesses bearing the brunt.

# Researcher bio: Asian Trade Centre and Dr. Deborah Elms



ASIAN TRADE CENTRE

**The Asian Trade Centre (ATC)** is the regional thought leader, advocate and educator for trade in the Asia Pacific region and serves as the resource for trade-related activities in Asia. They are a team of trade policy and supply chain subject matter experts positioned to meet the trade related needs of businesses — small and large — and governments — regional and foreign — operating in the Asia-Pacific.

ATC's primary activities include research, corporate advisory and capacity building services.

- They design and develop policy, macroeconomic and industry research analysis that incorporates qualitative and quantitative commercial, geo-strategic, economic and political analysis of the Asia-Pacific region.
- They assist companies with a regional supply chain footprint with the design and implementation of supply chain and duty optimization strategies that minimize tariffs, trade compliance and global trade management costs.
- They design and conduct training and capacity building programs for government officials and companies throughout Asia on key aspects of trade policy.

ATC is also the Secretariat to the Asia Business Trade Association (ABTA) and the Asia Pacific MSME Trade Coalition (AMTC).

This report was co-authored by **Nick Agnew**, Research Analyst of the Asian Trade Centre.



**Dr. Deborah Elms**

Founder and Executive Director  
Asian Trade Centre

**Dr. Deborah Elms** is the Founder and Executive Director of the Asian Trade Centre. The Asian Trade Centre works with governments and companies to design better trade policies for the region. Dr. Elms is also Vice Chair of the Asia Business Trade Association (ABTA) and sits on the International Technical Advisory Committee of the Global Trade Professionals Alliance and is Chair of the Working Group on Trade Policy and Law. She was also a senior fellow in the Singapore Ministry of Trade and Industry's Trade Academy.

Previously, Dr. Elms was head of the Temasek Foundation Centre for Trade & Negotiations (TFCTN) and Senior Fellow of International Political Economy at the S. Rajaratnam School of International Studies at Nanyang Technological University, Singapore. Her projects include the Trans-Pacific Partnership (TPP) negotiations, the Regional Comprehensive Economic Partnership (RCEP), the ASEAN Economic Community (AEC) and global value chains.

Dr. Elms received a PhD in political science from the University of Washington, a MA in international relations from the University of Southern California, and bachelor's degrees from Boston University. Dr Elms publishes the *Talking Trade* blog.

# Endnotes

1. [https://www.itu.int/dms\\_pub/itu-d/opb/ind/D-IND-DIG\\_TRENDS\\_ASP.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_ASP.01-2021-PDF-E.pdf)
2. <https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/>
3. <https://www.datanami.com/2018/11/27/global-datasphere-to-hit-175-zettabytes-by-2025-idc-says/>
4. <https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm>
5. [https://www.itu.int/dms\\_pub/itu-d/opb/ind/D-IND-DIG\\_TRENDS\\_ASP.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_ASP.01-2021-PDF-E.pdf)
6. <https://www.weforum.org/agenda/2018/01/google-ceo-ai-will-be-bigger-than-electricity-or-fire/>
7. <https://www.nature.com/articles/d41586-020-03157-9>
8. <https://www.forbes.com/sites/simonchandler/2019/11/05/how-the-internet-of-things-will-help-fight-climate-change/?sh=3b0e6d8758a3>
9. <https://policyreview.info/pdf/policyreview-2020-4-1532.pdf>
10. [https://aric.adb.org/pdf/aeir/AEIR2021\\_8\\_theme-chapter-making-digital-platforms-work-for-asia-and-the-pacific.pdf](https://aric.adb.org/pdf/aeir/AEIR2021_8_theme-chapter-making-digital-platforms-work-for-asia-and-the-pacific.pdf)
11. Ibid.
12. [https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ\\_1\\_Jan\\_2019.pdf](https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf)
13. [https://aric.adb.org/pdf/aeir/AEIR2021\\_8\\_theme-chapter-making-digital-platforms-work-for-asia-and-the-pacific.pdf](https://aric.adb.org/pdf/aeir/AEIR2021_8_theme-chapter-making-digital-platforms-work-for-asia-and-the-pacific.pdf)
14. Ibid.
15. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)
16. [https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT\\_20\\_1999](https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1999)
17. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)
18. <https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data>
19. <https://gdpr.eu/data-privacy/>
20. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
21. <https://gdpr.eu/companies-outside-of-europe/>
22. [https://www.bmw.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?\\_\\_blob=publicationFile&v=10](https://www.bmw.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10)
23. <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>
24. [https://www.bmw.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?\\_\\_blob=publicationFile&v=10](https://www.bmw.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10)
25. [https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1275&context=faculty\\_scholarship](https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1275&context=faculty_scholarship)
26. <https://voxeu.org/article/how-gdpr-affects-global-markets-data>
27. Ibid.
28. <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-extraterritorial-applicability.html>
29. [https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019\\_web.pdf](https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf)
30. <https://asean.org/storage/ASEAN-Digital-Masterplan-2025.pdf>
31. Ibid.
32. <https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf>
33. [https://www.aiti.gov.bn/SiteCollectionDocuments/Event/PCP\\_PersonalDataProtectionPrivateSector\\_20052021\\_final2.pdf](https://www.aiti.gov.bn/SiteCollectionDocuments/Event/PCP_PersonalDataProtectionPrivateSector_20052021_final2.pdf)
34. [https://www.aiti.gov.bn/SiteCollectionDocuments/Event/PCP\\_PersonalDataProtectionPrivateSector\\_20052021\\_final2.pdf](https://www.aiti.gov.bn/SiteCollectionDocuments/Event/PCP_PersonalDataProtectionPrivateSector_20052021_final2.pdf)
35. <https://www.pwc.com/id/en/services/assets/risk-assurance/newsflash/ra-newsflash-2019-01.pdf>

36. Ibid.
37. <https://www.pdp.gov.my/jpdpv2/assets/2020/01/Introduction-to-Personal-Data-Protection-in-Malaysia.pdf>
38. <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf>
39. Ibid.
40. <https://ecipe.org/blog/asia-data-regulation-gdp/>
41. <https://eitsc.com/wp-content/uploads/2018/05/Mapping-the-DPA-and-GDPR.pdf>
42. <https://pidswebs.pids.gov.ph/CDN/PUBLICATIONS/pidsdps2047.pdf>
43. <https://sso.agc.gov.sg/SL-Supp/S63-2021/Published/20210129?DocDate=20210129>
44. Ibid.
45. Ibid.
46. <https://www.pdpc.gov.sg/Commissions-Decisions>
47. <https://www.marsh.com/th/en/insights/research/personal-data-protection-act-in-thailand.html>
48. <https://home.kpmg/be/en/home/insights/2019/11/ta-thailand-personal-data-protection-act.html>
49. <https://www.forbes.com/sites/emmawoollacott/2019/01/09/days-after-introduction-of-cybersecurity-law-vietnam-has-facebook-in-its-sights/?sh=493d7ed526c5>
50. Ibid.
51. <https://www.cnn.com/2021/07/15/business/mastercard-india-rbi-intl-hnk/index.html>
52. <https://www.reuters.com/article/india-data-localisation/u-s-firms-face-off-with-indian-rival-paytm-in-lobbying-against-data-storage-rules-idINKBN1KE17L?edition-redirect=in>
53. <https://assets.kpmg/content/dam/kpmg/in/pdf/2020/08/impacting-digital-payments-in-india.pdf>
54. <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>
55. <https://digitalindia.gov.in/di-initiatives>
56. [https://iapp.org/media/pdf/resource\\_center/india\\_pdpb2019\\_vs\\_gdpr\\_iapp\\_chart.pdf](https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf)
57. Ibid.
58. Ibid.
59. [https://static.mygov.in/rest/s3fs-public/mygov\\_160922880751553221.pdf](https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf)
60. <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537>
61. <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537>
62. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>
63. Ibid.
64. Ibid.
65. <https://www.natlawreview.com/article/china-issues-data-security-law>
66. <https://www.jdsupra.com/legalnews/china-finalizes-data-security-law-to-4249871/>
67. <https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/>
68. <https://www.natlawreview.com/article/china-issues-second-version-draft-personal-information-protection-law-public>
69. <https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/>
70. Ibid.
71. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>
72. <https://www.ctamericas.com/global-data-center-map/>
73. <https://elibrary.worldbank.org/doi/pdf/10.1596/0-8213-2788-7>



---

The Hinrich Foundation is a unique Asia-based philanthropic organization that works to advance mutually beneficial and sustainable global trade.

We believe sustainable global trade strengthens relationships between nations and improves people's lives.

We support original research and education programs that build understanding and leadership in global trade. Our approach is independent, fact-based and objective.

---

#### MEDIA INQUIRIES





Ms. Theresa Fonseca,  
Head of Marketing and Communications  
T: +65 6982 6816  
[theresa.fonseca@hinrichfoundation.com](mailto:theresa.fonseca@hinrichfoundation.com)

There are many ways you can help advance sustainable global trade. Join our training programs, participate in our events, or partner with us in our programs. [inquiry@hinrichfoundation.com](mailto:inquiry@hinrichfoundation.com)

Receive our latest articles and updates about our programs by subscribing to our newsletter

[hinrichfoundation.com](http://hinrichfoundation.com)



 hinrichfdn  
 hinrichfoundation  
 hinrich foundation  
 hinrichfoundation

#### Disclaimer:

The Hinrich Foundation is a philanthropic organization that works to advance mutually beneficial and sustainable global trade through original research and education programs that build understanding and leadership in global trade. The Foundation does not accept external funding and operates a 501(c)(3) corporation in the US and a company in Singapore exclusively for charitable and educational purposes. © 2021 Hinrich Foundation Limited. See our website [Terms and Conditions](#) for our copyright and reprint policy. All statements of fact and the views, conclusions and recommendations expressed in the publications of the Foundation are the sole responsibility of the author(s).