Regulating the Cyberspace
Perspectives from Asia
Regulating the Cyberspace
Perspectives from Asia

EDITORS
Gisela Elsner
Aishwarya Natarajan

Rule of Law Programme Asia
Konrad Adenauer Stiftung
# Table of Contents

Preface vii

1 Asian Democracies and (European) Digital Constitutionalism: Recent Developments in Data Protection Legislation  
   *Fabian Duessel* 1

2 Cyber Norms and International Law in ASEAN  
   *Eugene Tan* 15

3 Regulating Privately Developed Public Technology in South and Southeast Asia: A Critical Analysis of Governance Through and Governance of Emerging Technology  
   *Vidushi Marda* 33

4 Digital Sovereignty: Data Governance in India  
   *Trisha Ray* 49

5 State Sovereignty in the Cyberspace and the Free Flow of Data  
   *Smitha Krishna Prasad* 65

6 From Self-Regulation to State Intervention: Shifting Modes of Social Media Regulation in Asia  
   *Cleve Arguelles* 79
On 22 May 2020, Estonia, the current president of the United Nations Security Council (UNSC), hosted an informal meeting of the UNSC to discuss “Cyber Stability, Conflict Prevention and Capacity Building”.¹ This is said to be the first-ever meeting of the UNSC that focused on “cyber” as a separate issue. Organised against the backdrop of increasing cyber-attacks against crucial healthcare-related services during the Covid-19 pandemic, most interventions spoke of the need to strengthen technological capabilities in this context.

The underlying issue that cut across states’ interventions, however, was the question of applying international law – and particularly international human rights and humanitarian laws – to the cyberspace.² This is not a new issue. While there is broad agreement that international law does indeed apply to the cyberspace³, multiple international processes have been put in place to discuss and define what this actually means. How does the concept of public international law, built around the idea of a sovereign


² “The Estonian Presidency of the UN Security Council Holds a Landmark Discussion on Cybersecurity” (n 1).

Regulating the Cyberspace

state, and its duties towards its people and its neighbours, translate to something as ubiquitous as the internet?

In the context of cyber-attacks against healthcare services, for example, the security of the digital infrastructure and the protection of vulnerable patients, whether in terms of maintaining the ability to provide medical care or to protect rights such as privacy, are paramount. Over the past decade, and more, there has been wide acceptance of the idea that civil and political rights, specifically freedom of speech and expression, and the right to privacy, are equally available both online and offline. The corollary to the exercise of human rights online is the right to access the internet in itself. These rights are based on universally accepted principles, recognised by most states that participate in the United Nations – under both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights⁴.

However, the manner in which states enable the exercise of these rights in the online context differs significantly.⁵ Domestically, this difference is certainly visible across Asia, where many states have a chequered history of recognising such rights offline as well. At the multilateral level, the broader question of how international humanitarian law applies to the cyberspace and state actions towards each other remains. With several states worried that they are losing control over their own security, or falling behind in the global race to benefit from the digital economy, different assertions of cyber-sovereignty have complicated efforts to govern the cyberspace at both domestic and international levels.

This article will explore some of the efforts made by countries in Asia to leverage their positions in the global digital economy, in the form of assertions of “data sovereignty” and attempts to control the flow of data out of their jurisdictions – for security and/or economic benefits.

---


Cross Border Data Flows – The Asian Perspective

Over the past few years, there has been a push for greater multilateral cooperation in the context of cybersecurity and the application of international humanitarian law to the cyberspace. However, the regulation of cross-border transfer of data⁶, and access to such data for security and law enforcement purposes, has been a question of bilateral cooperation at best. This has provided states with more room to explore policy options.

The United States (US) and the European Union (EU) have established themselves as proponents of the idea of an open internet, which calls for a free flow of data, responding to market needs rather than regulation.⁷ The US is home to many of the largest tech companies, and therefore more likely a “receiver” of such data than an exporter. The EU, while aiming to encourage a home-grown technology industry, has chosen the option of permitting the export of its data, so far as standards for protecting the data privacy of EU citizens and residents are met⁸. Russia and China are considered to be at the other end of this spectrum, with varying requirements for localised data storage and processing⁹.

Today, data privacy protections have increasingly become integral to trust in both government and the tech industry. As a result, many countries across the world have embarked on the process of legislating such protections. As Asian countries jump on this bandwagon – either updating or implementing new data protection laws – the region has also gained a reputation for promoting “data localisation” efforts, led by the Chinese model. A deeper study shows that only a few states in the region – including India, Indonesia and Vietnam – have considered or implemented data localisation in any significant manner. Recent developments suggest that even these states are now reconsidering comprehensive data localisation

---

⁶ For the purpose of this paper, “data” will mean personally identifiable information/data as commonly understood in the context of the right to privacy and data protection regulations.
measures. These countries now seem to be looking into more targeted solutions to the issues that led to the call for cross-cutting data localisation measures.

To understand the impact of both the global reputation as promoters of data localisation, and the many changes in domestic policy, a discussion on what localisation entails, and why different stakeholders push for it, is necessary.

**Data Localisation v. Conditional Cross Border Transfers**

Data localisation is one of the means by which governments control the outflow of data from the country by the private or public sector. It typically requires that certain types of data are processed and stored within the country, and restricts cross-border transfer of such data either as a whole, or in specific circumstances. For example, transfer may be permitted subject to storage of a copy locally. In the context of personal data, such control can be exercised by means of restrictions on cross-border transfers of data in comprehensive data protection laws. Sector specific regulations can also be used for this purpose – for instance, telecom, financial or healthcare service providers can be restricted from transferring any identifying information about their subscribers outside the country. The primary purpose of such data localisation is to ensure that “data generated locally on their citizens and residents be kept within their geographic boundaries and remain subject to local laws”.

Some of the more controversial models of data localisation prevalent in Asia are discussed below.

- **China**

  In 2017, China’s first comprehensive cyber security law made the news for its extensive data localisation requirements, among others. The law requires all critical information infrastructure operators to store personal information and other important data collected within China, locally. Critical information infrastructure was defined in a broad and

---


inclusive manner, as referring to public communication and information services, energy, transportation, water resources, finance, public services, and e-governance.12 While the law does not completely prohibit transfer of such information outside the country, it does require a security check to be completed, before transfer is permitted in many cases.13 Reports suggest that the draft guidelines that are intended to clarify implementation of this law provide for an extensive list of services that would fall within the ambit of the localisation requirements, in some cases creating more ambiguity about its application.14

The extensive localisation requirements under Chinese law are yet to come into force fully. However, it appears that a number of sectoral regulations and guidelines now require personal information to be stored locally15.

- India

In India, there has been much discussion about including data localisation requirements in the proposed comprehensive data protection law. Such measures were proposed in the draft Personal Data Protection Bill, 2018 that was recommended by a government-appointed committee of experts.16 Broad localisation requirements have also been recommended in proposed economic policies, such


14 “Chinese Data Localization Law: Comprehensive but Ambiguous” (n 12).


as the draft E-Commerce Policies of 2018 and 2019\(^\text{17}\). However, at the
time of writing, the most extensive data localisation requirements are
applicable only in the context of sensitive information in the financial
sector.\(^\text{18}\)

In December 2019, the Personal Data Protection Bill, 2019\(^\text{19}\), a revised
version of the draft from 2018, was introduced in Parliament. Among
others, one of the significant changes in this Bill was the minimisation
of data localisation requirements. The Bill does not restrict the trans-
fer of personal data outside of India, and places conditions based on
which sensitive personal data may be transferred and processed out-
side of India. Among other conditions, sensitive personal data must
also continue to be stored locally in India alongside such cross-border
transfers. Further, the transfer of sensitive personal data should not
negatively impact the enforcement of any other laws.

Critical personal data, which the government may define, cannot be
transferred outside India at all, except where required for health or
emergency services, or otherwise specifically permitted by the gov-
ernment.

- Indonesia

In Indonesia, data localisation requirements were applied in relation to
any personal information collected and processed for the provision of
public services.\(^\text{20}\) If the conditions laid down in this context were met,
the service provider would need to set up a data centre in Indonesia.
These requirements had wide import given that “public service” was
interpreted to include services such as banking, insurance, health, and
transport, even if they were provided by private companies.

A new regulation introduced in October 2019, now demarcates public
and private electronic system operators, and limits data localisation

---


\(^{19}\) “Personal Data Protection Bill, 2019”, https://www.prsindia.org/sites/default/files/bill_files/
Personal%20Data%20Protection%20Bill%2C%202019.pdf.

\(^{20}\) Dr. Clarisse Girot (n 11).
requirements to the public sector only.\[^{21}\] Reports suggest that these changes were made as a result of data localisation requirements being considered “inefficient”, and detrimental to the growth of the digital economy.\[^{22}\] The security concerns that typically counter such arguments are met by requiring companies that store data offshore to enable access to security and law enforcement agencies in specific circumstances.\[^{23}\]

- **Vietnam**

Vietnam’s cybersecurity law has broad data localisation requirements, applicable to almost all service providers in Vietnam’s cyberspace that collect, analyse or process private information or data relating to their users in Vietnam. Such service providers would need to establish a branch office in Vietnam, and store personal data of Vietnamese users locally for a specified period of time.\[^{24}\]

The government has since announced that this requirement would be relaxed, and published a draft guidance on its implementation.\[^{25}\] The new draft suggests that the data localisation requirements will be applicable only if a service provider meets certain additional criteria. The service provider must be notified that its services have been used to violate Vietnam’s laws, and then (a) fail to take measures to stop the violations, (b) resist, obstruct or fail to cooperate in the investigation


of such violations or (c) disable the effect of any protective measures taken by the authorities.26

These countries are not the only ones to restrict or consider restricting cross-border transfers of data. Many states impose conditions on the outflow of personal data, especially as it relates to their citizens. Typically, such conditions are either specific to “sensitive” sectors, or include requirements to ensure the recipient of the data maintains minimum data protection measures. The aim is to protect the privacy and personal information of citizens/residents, and limit access where information is particularly sensitive.

The distinction between such conditions for transfer and the more controversial localisation requirements implemented or proposed in the four Asian jurisdictions mentioned above lies in the scope of application. This is seen both in the reason behind such a policy, as well as its impact.

A look at the broader policy goals often shows that states are looking to control how the data generated domestically, or personal data of their citizens and residents, is used. Data localisation measures may be positioned as a sub-set of data protection regulation, and could indeed offer some of the protections that conditional transfer requirements offer. However, it may, in fact, be better described as a sub-set of efforts to ensure “data sovereignty”.27

The two policy aims that a data localisation requirement is typically meant to meet are: improvements in a state’s ability to enforce security and law enforcement measures domestically, and economic growth in the domestic markets.

1. Data Exports, National Security and Law Enforcement

Many developing countries offer large consumer bases and new markets to the tech companies emerging from the US (and now China) – the rapid expansion of these powerhouses has been both good and bad for such countries. As individuals across the world increase their use of


ubiquitous online services, whether social media or e-commerce, data about their online activities vests with the few companies that provide a majority of these services. In such a situation, whether these companies are based in the US, China or elsewhere, the host country where the service is provided faces similar problems – ensuring that these service providers are subject to domestic law for the protection of their citizens. The kind of protection that domestic law offers a citizen or resident of a country manifests in different ways, for instance, in the form of data protection laws that offer privacy protections, or laws that enable investigation of criminal activity. However, there has been increasing concern among governments regarding the fact that multi-national service providers are domiciled, or store and process data outside the country, limiting the reach of domestic regulators and law enforcement authorities.

Data localisation is often proposed as a solution to this problem in order to enable domestic security agencies and law enforcement authorities to undertake their functions without additional hurdles. There are at least three different concerns that a data localisation policy is said to address in this context: (a) security and law enforcement access to personal data held by foreign companies; (b) security and law enforcement access to personal data stored on servers outside the country; (c) protection from foreign surveillance; and (d) protection of critical information and personal data of citizens by means of compliance with local laws and security standards.

The first and second concern can be clubbed together to a certain extent, since the broader aims and issues behind the two are similar. Domestic laws in each country typically provide security and law enforcement agencies with powers and procedures to investigate illegal/criminal activity. Search and seizure as well as surveillance form an integral part of this process. When these activities need to be undertaken across borders, several conflict of laws questions come into play.

28 The term “conflict of laws” broadly refers to a situation where two jurisdictions have differing laws on the subject matter of a single case, and a decision has to be made regarding which jurisdiction’s laws are applicable. For more information, see “Conflict of Laws”, Encyclopedia Britannica, https://www.britannica.com/topic/conflict-of-laws; “Conflict of Laws”, LII/Legal Information Institute, https://www.law.cornell.edu/wex/conflict_of_laws.
What happens when a company incorporated in country X holds data about a citizen in country Y that could be helpful in the investigation of a crime in country Y? Are local police in country Y empowered to demand data and cooperation from a foreign company? What if country X has laws preventing its companies from sharing data with third parties? Would there be a significant difference if the company was incorporated in country Y but merely storing data in country X?

Bilateral agreements, known as mutual legal assistance treaties (MLAT), are meant to provide a solution to such problems. MLATs enable law enforcement authorities in one country to seek assistance from their counterparts in the other. However, these processes are dated and inefficient, with most authorities unable to keep up with growing demand for law enforcement access to electronic data across the world.29

Countries like India have proposed data localisation policies as a solution to this problem, arguing that if data is stored locally in India, local security and law enforcement agencies will have greater access to such data.30 However, the answer is unlikely to be as simple, given that other concerns such as the country of incorporation, and laws applicable to the company (and in the case of multi-national corporations, a subsidiary or affiliate company) that holds or controls the data must be taken into account as well.31 (New bilateral arrangements, for example, under the US CLOUD Act, which enables executive/government agencies from signatory countries to directly work with each other, have been pitched as a more likely solution.32)

The third and fourth concerns mentioned above speak more to trust in governments and their commitments to universal human rights, perhaps, than any technical measures such as localised storage of data.

30 Committee of Experts (n 16); Basu, Hickok and Singh Chawla (n 27).
32 Srikumar and others (n 29).
As the Snowden revelations show, it is imperative that states recognise the right to privacy, and commit towards protecting this right as it is available to their own citizens as well as citizens of other countries. Data protection laws and transparency and oversight of surveillance activities are important steps in this direction. However, it is unclear how data localisation requirements would contribute in this regard. In fact, many suggest that mandating local storage of data might in fact increase security risks.

The relaxations in the data localisation policies of both India and Indonesia indicate a shift from data localisation to the broader concept of data sovereignty. Provisions on cross-border data flow in Indonesia’s new regulation, and India’s proposed law, both provide that data can largely be transferred outside the country, as long as specified minimum standards of data protection are followed, and the Indonesian and Indian government, respectively, have access to such data for legitimate law enforcement purposes. While the requirement to ensure access for law enforcement purposes may still counter some of the conflict of laws issues discussed above, there seems to be a recognition that the local data storage requirements are merely additional complications.

2. Data Localisation and the Domestic Digital Economy

Although this paper focuses largely on data localisation as it relates to national security and law enforcement, no discussion on data localisation is complete without addressing the economic impact of such measures. As with security and law enforcement, the sheer size and reach of big tech companies from the US (and now China) have exacerbated the calls for data sovereignty and nationalism in many other countries.

---

34 Bhardwaj (n 33).
35 Agus Deradjat and Mahiswara Timur (n 21).
36 “Personal Data Protection Bill, 2019” (n 19).
Over the past 10-15 years, as these companies entered new markets across the world, they brought access to internet and new services to consumers. However, there is a growing fear that the dominance of big tech doesn't reflect in the kind of economic growth that a homegrown tech industry may offer.

Data sovereignty in the context of economic growth is quite different from the concept as we see it in the context of security and law enforcement. Measures such as localisation are proposed not to protect individuals, but to pave the way for their data to be shared with domestic industry and otherwise encourage innovation in emerging technology locally.\(^{37}\) This approach is limited in nature, and as many critics have pointed out, data centres do not automatically generate employment and data does not automatically generate AI-based products and services.\(^{38}\)

The arguments in favour of data localisation or sovereignty as necessary for the digital economy appear to be pushed by countries such as India which have a large number of internet users, generating massive amounts of data, as well as a growing local technology industry.\(^{39}\) It is not, however, a pan-Asian approach. New Zealand and Singapore, for instance, have taken a different route to usher in growth of the digital economy – leveraging the free flow of data and the capacity of their domestic businesses.\(^{40}\)

**Conclusion**

Data localisation measures have been seen as a potential “one-stop shop” solution to multiple state and economic interests. However, in effect these measures may at best act as temporary band-aids or negotiating tools, and do not by far solve underlying issues that harm these interests in the first place. It has been suggested that rather than have one loud but ineffective measure such as localisation in place, the state and economic

---

37 See for instance Committee of Experts (n 16).
38 Basu, Hickok and Singh Chawla (n 27).
interests that justify such a measure should be looked into in detail, and each addressed separately.\(^\text{41}\)

As states look to create policies for national security, law enforcement and economic growth in the context of data, they must not only ensure that the right to privacy and related rights of individuals are protected, but also look outward at multilateral engagement on these issues. In this paper alone at least three different avenues for the intersection of sovereignty, the internet and data, at an international level have been identified.

With security risks growing rapidly, discussions are taking place at the multilateral level, at the UNSC or other fora such as the United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security\(^\text{42}\) (OEWG), or Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security\(^\text{43}\). However, these discussions cannot take place in isolation. Geopolitical factors, such as the questions discussed in this paper, among others, will play into the positions states take at different international fora, and their discussions and negotiations in such contexts. India’s comments to the Pre-Draft of the OEWG Report\(^\text{44}\) (now removed from the OEWG webpage), which conflate mixed ideas of privacy, data ownership and sovereignty, in the context of a discussion on international humanitarian law are a concerning example.

Similarly, the back and forth on data localisation and data sovereignty policies at a domestic level in many jurisdictions show a lack of clarity and understanding of the consequences of such policies. In the absence of a broader regional approach in Asia, any data-related law or policymaking risks inevitably being viewed through the lens of US versus China versus EU policies. In these circumstances, it is important for states across the

\(^{41}\) Basu, Hickok and Singh Chawla (n 27).


\(^{44}\) In March 2020, the Chair of the OEWG published an initial pre-draft of the report of the deliberations of the OEWG, and requested participating delegations to provide feedback on the document.
region to develop clear and informed positions on these distinct aspects of sovereignty, as they relate to international and domestic laws and obligations.

Smitha Krishna Prasad is an Associate Director at the Centre for Communication Governance at National Law University Delhi.
Rule of Law Programme Asia
Konrad Adenauer Stiftung