KONRAD ADENAUER STIFTUNG

Regulating the Cyberspace
Perspectives from Asia

Gisela Elsner

Aishwarya Natarajan

www.kas.de

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

KONRAD
ADENAUER
STIFTUNG

Editors: Gisela Elsner, Aishwarya Natarajan

Konrad-Adenauer-Stiftung
Rule of Law Programme Asia
ARC 380, 380 Jalan Besar, #11-01
Singapore 209000
Tel: (65) 6603-6171
Fax: (65) 6603-6180
Email: law.singapore@kas.de
Website: http://www.kas.de/web/rspa/home

Cover design and typesetting by Select Books Pte Ltd.

National Library Board, Singapore Cataloguing in Publication Data

Name(s): Elsner, Gisela, editor. | Natarajan, Aishwarya, editor. | Konrad-Adenauer-Stiftung, publisher.
Title: Regulating the cyberspace : perspectives from Asia / editors, Gisela Elsner, Aishwarya Natarajan.
Description: Singapore : Konrad-Adenauer-Stiftung, Rule of Law Programme Asia, [2020]
Identifier(s): OCN 1178918480 | ISBN 978-981-14-7125-4 (paperback)
Subject(s): LCSH: Data protection--Law and legislation--Asia. | Computer networks--Law and legislation--Asia. | Social media--Law and legislation--Asia.
Classification: DDC 343.509944--dc23

Printed in Singapore.

Table of Contents

Preface

In 2018, the worldwide Rule of Law Programme of the Konrad Adenauer Stiftung (KAS) spearheaded an initiative to look at the impact of digitalisation on our society; more specifically, the initiative was desirous of exploring the linkages between law, policy and technology. In line with this goal, the Rule of Law Programme Asia took infant steps to set up the digitalisation programme for the Asian region.

Technology innovation and Asia are no strangers to each other. The success of the Far East Asian economies of Japan and South Korea have been backed by technology for decades. Now, South and Southeast Asia have also emerged as homes for technology start-up ecosystems. The emergence of tech start-ups has resulted in significant social and economic benefits for both sub-regions. China, India and Indonesia are the countries with the most number of internet users in the world. Young Asians are the avid users of social media as well. On the digital economy front, Asian states are in preparation to reap the benefits that Industry 4.0 has to offer to their societies. States are undertaking large-scale revamping of their society and governance models backed by technology by initiating smart city projects, and introducing e-governance platforms and issuing biometric identities to their citizens.

Simultaneously, Asian states are battling high levels of digital divide both within and between countries. A stable internet connection is the most basic requirement to access these digital services and Asia continues to suffer from a lack of internet connectivity, which contributes to the region's digital divide being one of the highest in the world. A 2016 UNESCAP report noted that 75 percent of fixed broadband subscriptions in Asia-Pacific were registered in North and Northeast Asia, mainly in the People's Republic of China, the Republic of Korea, and Japan. On a similar note, while there is increased awareness on digital rights and the need for

digital literacy, it remains limited to the urban centres in Asia. The region has a long way to go in achieving satisfactory levels of digital literacy and in securing a full range of digital rights for its citizens. Advanced information and communication technologies are a powerful tool to address developmental challenges and can facilitate states in fostering an equal and inclusive society. It can open up a world of opportunities for the marginalised and vulnerable groups in Asia. It has the potential to enable states in the region to achieve the UN Sustainable Development Goals (SDGs) in a timely manner.

It is in this context that Asian states are playing catch up by legislating on various aspects of technological advancement to minimise the harms arising out of it, including regulating social media, passing data protection laws and implementing intermediary liability rules. The international, regional and national regulatory frameworks relating to the digital space are in a state of constant flux and governance norms are continuously evolving. Asians, as the biggest users of the internet, should aim to contribute to the global debate on regulating the cyberspace. It is essential that Asian voices are heard and that their needs are met when the world is setting norms to regulate the digital space.

While many of us tend to believe that the multilateral world order has ended and the state is irrelevant in the age of the super platforms, legal policymaking powers continue to rest with the state. Governments play a critical role in allotting resources even in the digital space and defining the rules of the game via legal policy changes. Developing countries in Asia and beyond should secure their seat at the table along with the developed world and the private sector when rules regulating the digital economy are being formulated. While issues associated with the digital economy touch upon several areas of legal policy, including competition, taxation, intellectual property, trade and employment policies, the most critical element of this policy is data and cross-border flows of data. Data is the new oil for the digital economy and how Asia deals with its data will set the stage for the economic and social outcomes it achieves.

With this in mind, we bring forth this publication, which captures perspectives from South, Southeast and North Asia about data governance, regional cooperation in norm building, capacity building initiatives and the development of social media regulation in the region. We truly hope that the publication is a valuable contribution in making voices from Asia heard in the international policymaking arena.

1

Asian Democracies and (European) Digital Constitutionalism: Recent Developments in Data Protection Legislation

Fabian Duessel

1. Introduction

How to embed the ever-growing digital economy within the framework of constitutionalism is a key challenge for the 21st century. With good reason, the term "digital constitutionalism" can offer some solutions.[1] One of the most significant developments within this context is undoubtedly the General Data Protection Regulation (GDPR) of the European Union (EU), which was adopted in 2016 and took legal effect in 2018. EU market power and the GDPR's extraterritorial effect together compel public and private actors across the world to make choices on how to adapt to the requirements of the GDPR.[2]

The European Commission certainly considers the GDPR as the basis for further international cooperation on the issue of personal data protection. It has specifically mentioned the priority of holding discussions on possible adequacy decisions with key trading partners in East

[1] Edoardo Celeste, "Digital Constitutionalism: Mapping the constitutional response to digital technology's challenges," *HIIG Discussion Paper Series* 2018-02 (2018): 7.

[2] Paul M. Schwartz, "Global Data Privacy: The EU Way," *New York University Law Review* 94 (October 2019): 771-818.

and Southeast Asia.[3] In the absence of a comparable regional regulator that covers the whole of Asia or any of its sub-regions, the right to data protection in the Asian region can be expected to generally proceed along different paths.[4] However, signs of alignment between countries in Asia are emerging via their respective adaptation to the extraterritoriality of the EU's GDPR. Importantly, these adequacy decisions, which allow transfer of data between the EU and third countries, are subject to periodic review, thereby further generating the potential for evolving convergence and alignment.[5]

This chapter will provide a limited snapshot of recent developments in the field of data protection legislation in the following Asian democracies: Taiwan, Japan, South Korea and India.[6] Selected current discussion themes around revising Taiwan's Personal Data Protection Act (PDPA) are placed in comparison to Japan's 2016 Act on the Protection of Personal Information (APPI),[7] South Korea's 2020 Personal Information Protection Act (PIPA), and India's 2019 Personal Data Protection Bill (PDPB). Due to the complexity of these respective laws, it is impossible to make an exhaustive comparison within the limited scope of this chapter. Rather, the aim is to highlight some broad points of potential alignment, drawing on the experience of these Asian democracies in response to the global reach of the GDPR.

Taiwan has officially signalled interest in obtaining a GDPR adequacy decision from the EU, but at the time of writing has not yet revised its domestic privacy laws. However, preparations for revision are being made, and core issues for legislative change are being discussed by the

---

[3] European Commission, *Communication from the European Commission to the European Parliament and Council: Exchanging and Protecting Personal Data in a Globalised World* (Brussels: EUR-Lex, 10 January 2017), 8.

[4] Graham Greenleaf, "Asia's Data Privacy Dilemmas 2014-2019: National Divergences, Cross-Border Gridlock," *University of New South Wales Law Research Series* 103 (2019).

[5] See Article 45(3) and Recital 106 of the GDPR.

[6] These four Asian examples have been chosen for comparative analysis due to the overlap of four factors: their notable global economic power (especially in the IT sector), their relatively advanced democratic governance structures, the existence of specific laws or bills on personal data protection, and evident progress or plans to secure a GDPR adequacy decision in the near future.

[7] The APPI is currently due for amendment, see Personal Information Protection Commission, "Cabinet Decision on the Amendment Bill of the Act on the Protection of Personal Information, etc.," 24 March 2020, https://www.ppc.go.jp/en/news/archives/2020/20200324/.

government,[8] opposition parties,[9] as well as academia.[10] Japan has already obtained an adequacy decision from the EU, South Korea is in official GDPR adequacy negotiations,[11] and India has been reported to be potentially looking to apply for a GDPR adequacy decision once major domestic legislative changes are complete.[12]

According to a recent formulation of the role of digital constitutionalism, it is "intended as a declination of modern constitutionalism, imposes the necessity to generate normative counteractions to the alterations of the constitutional equilibrium produced by the advent of digital technology and, at the same time, provides the ideals, values and principles which guide such counteractions."[13] The GDPR certainly embodies such a type of constitutionalism: It clearly treats privacy and data protection as fundamental rights, aiming to increase the accountability of the data controller while at the same time introducing new data subjects' rights,[14] especially also using such an approach to tackle fundamental problems

---

[8] See 國家發展委員會 (National Development Council), "國發會推動個資法修法，力拼GDPR適足性認定" ("National Development Council pushing forward with amending the Personal Data Protection Act, striving to obtain GDPR adequacy decision"), Press Release on 29 December 2019, https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=632E56DC2B36CB76.

[9] Kuomintang (KMT) parliamentarians submitted two amendment proposals regarding the current PDPA in March 2020. Relevant official documents can be found in the database of the Legislative Yuan, available at: https://misq.ly.gov.tw/MISQ/IQuery/misq5000QueryBillDetail.action?billNo=1090317070201700 and https://misq.ly.gov.tw/MISQ/IQuery/misq5000QueryBillDetail.action?billNo=1090302070201400. For proposals by Taiwan People's Party (TPP) parliamentarians, see Radio Taiwan International, "後防疫時代 民眾黨提案修法避免個資外洩" ("After the era of epidemic prevention – Taiwan People's Party proposes legislative amendments to prevent personal data leaks"), 12 May 2020, https://www.rti.org.tw/news/view/id/2063658.

[10] For example, see 張陳弘 (Chang, Chen-Hung), "GDPR 關於蒐用一般個人資料之合法事由規範" ("GDPR provisions on the lawful processing of personal data"), 月旦法學雜誌 (No. 285) 2019.2, 174-190.

[11] See the EU official website on adequacy decisions: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[12] Megha Mandavia, "India to approach the EU seeking 'adequacy' status with the GDPR," *The Economic Times*, 30 July 2019, https://tech.economictimes.indiatimes.com/news/internet/india-to-approach-the-eu-seeking-adequacy-status-with-the-general-data-protection-regulation/70440103.

[13] Celeste, "Digital Constitutionalism", 6-7.

[14] Giovanni de Gregorio, "The Rise of Digital Constitutionalism in the European Union," *International Journal of Constitutional Law* (2020 forthcoming): 21-22, available at SSRN: https://ssrn.com/abstract=3506692.

which arise out of automated decision-making.[15] According to the current Data Protection Commissioner for Ireland, the GDPR regulates in order to liberate,[16] and the emerging body of GDPR-related case law will shape "the future of human autonomy and dignity."[17]

How growing (European) "digital constitutionalism" is received in the politically and economically rising Asian region is a worthy subject of future research in the years to come. It is hoped that this chapter provides one small contribution to this field of research. The following is structured around the broad themes of definitions, rights and obligations, and the necessity for an independent data protection authority.

2. Defining Personal Data

Advancing technology enables an unprecedented volume of collecting and processing of different types of data, making the need for regulation inevitable.[18] The question over what counts as "personal data" may have to be regularly revised in line with new technological possibilities. Unsurprisingly, the definition of "personal data" under the GDPR is broad,[19] since this is required to fulfil the purpose of data protection in the age of rapid technological change.[20] This trend towards broadening the definition of personal data is also visible in Asian democracies.

The current version of Article 2(1) of Taiwan's PDPA refers to a mixture of more traditional and obvious categories of personal data, some

---

15 de Gregorio, "Rise of Digital Constitutionalism", 22-23. See Article 22 and Recital 71 GDPR.

16 Helen Dixon, "Regulate to Liberate, Can Europe Save the Internet?" *Foreign Affairs* 97, no. 5, September/October 2018, 28-32.

17 Dixon, "Regulate to Liberate", 32.

18 Viktor Mayer-Schönberger and Yann Padova, "Regime Change? Enabling Big Data through Europe's new Data Protection Regulation," *The Columbia Science and Technology Law Review* XVII, (2016): 317.

19 Article 4(1) GDPR.

20 For a detailed discussion on the inevitability, associated problems and potential solutions related to an ever-broadening definition of "personal data", see Nadezhda Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law," *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.

examples of "sensitive data"[21] and some categories which could potentially cover an internet user's online data.[22] Nevertheless, there have been calls in Taiwan for explicit enumeration in Article 2(1) of further examples of sensitive data and online data. Examples of sensitive data that are currently not explicit in Article 2(1) PDPA are ethnicity, political opinion and religious belief.[23]

The importance of highlighting and naming a special category of sensitive data is clearly reflected in the relevant legal norms in Japan, South Korea and India. Article 2(3) of Japan's APPI speaks of "special care-required personal information", which includes race, creed, social status, medical history, criminal record, and the fact of having suffered damage by a crime. Article 23(1) of South Korea's PIPA states that "sensitive information" includes ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, and sex life. In India, Clause 3(26) of the PDPB provides examples of "sensitive data", which include financial data, health data, official identifier, sex life, sexual orientation, biometric data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation.

Apart from adding more examples of sensitive data, calls in Taiwan have also been made to add more examples of online data, such as online identifiers and an internet user's digital footprint.[24] It is therefore also instructive to look at the new legislation of other Asian democracies in terms of technology-driven expansion of the material scope of personal data. Clause 3(28) of India's PDPB explicitly speaks of "personal data" that is "online or offline". Recent legislative changes in South Korea have resulted in

---

[21] In GDPR terminology, sensitive data *are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. …* (GDPR Recital 51). In Taiwan, without stating a specific umbrella term in the relevant provision, such data are recognised in Article 6 PDPA: *Data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected, processed or used unless on any of the following bases: …*

[22] Article 2(1) PDPA: *"personal data" refers to a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person; …*

[23] Kuomintang, see note 9.

[24] Kuomintang and Taiwan People's Party, see note 9.

the PIPA being fully applicable to online service providers.[25] Article 39-3 of the revised PIPA imposes legal duties on any "information and communication service provider who intends to collect and use personal information of users". Article 2(1)(i) of Japan's APPI speaks of personal information in "electronic" form.

Article 2(1) of Taiwan's current PDPA concludes with the phrase "any other information that may be used to directly or indirectly identify a natural person". This arguably can include any type of personal data deemed as "sensitive data" as well as an internet user's online information. However, the key rationale for revising the definition of personal data as contained in the current PDPA seems to be the necessity for explicit enumeration. Even though catch-all phrases are in many situations useful to provide room for interpretation, in other situations they can be insufficient from the standpoint of legal certainty.

Beside the material scope, suggestions in Taiwan have also been made to expand the personal scope of data protection to explicitly include the personal data of children.[26] In contrast to the lack of references to children in the current PDPA, the equivalent laws in Japan, South Korea and India all make specific references to children, albeit to varying degrees. The most eye-catching is India's PDPB, since its Chapter IV (Clause 16) is entirely devoted to the "[p]ersonal data and sensitive personal data of children". Unlike India, South Korea's PIPA does not have a self-contained section on the personal data of children, but the interests of children are mentioned frequently throughout the law.[27] Japan's current APPI limits itself to mentioning the "fostering of healthy children" in Articles 16(3)(iii), 17(2)(iii) and 23(1)(iii).

3. Rights and Obligations

As demonstrated by the GDPR, data processing should only take place with the consent of data subjects and within the context of specified law-

---

[25] Kim and Chang, "Major Amendments to Three Data Privacy Laws: Implications," Privacy Legal Update, 10 January 2020, https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=20726.

[26] Kuomintang, see note 9.

[27] Articles 22(6), 38(2), 39-3(4) to (6), 39-15(1)2 and 71(4-6).

ful purposes.[28] Even if data processing takes place in a lawful manner, data subjects should also enjoy a specific set of rights that enable them to exercise control over their data.[29] In Article 3 of Taiwan's PDPA, a data subject has five rights over their personal data, which cannot be waived or limited contractually in advance: the rights to inquire or review; to request data copies; to supplement or correct; to demand cessation of collection, processing and use; and the right to erase. However, suggestions have been made to expand this list of rights in Taiwan's PDPA, especially when compared to the data subject rights contained in the GDPR.[30]

Two "new" rights of the GDPR that are often noted are the right to erasure (in some contexts more often known as the "right to be forgotten") and the right to data portability.[31] The former actually has already been subject to extensive debate and adjudication in Europe before the GDPR was adopted.[32] Also, wording such as the right to "erase" personal data already exists in laws not yet fully adapted to the global reach of the GDPR, such as in Taiwan's current Article 3 of the PDPA. International developments in recent years have demonstrated the growing complexity of the meaning of "erasure", raising difficult questions regarding its interpretation and effective application.[33] A full discussion and comparison of the provisions on the right to erasure and their respective nuances in the selected Asian democracies is beyond the scope of this chapter. Instead, this subsection will briefly point to the existence or absence of the other "new right", the right to data portability, in the selected legislative case studies.

---

[28] The GDPR provides a list of principles relating to processing of data (Article 5), specifies detailed criteria for the lawfulness of processing (Article 6), and defines conditions for consent (Article 7).

[29] Chapter III GDPR.

[30] 國家發展委員會 (National Development Council), 台灣經濟論衡 第16卷 / 第3期 (16(3) *Taiwan Economic Forum*, 2018/09), 88-89.

[31] The absence of the right to "data portability" (Article 20 GDPR) and the "right to be forgotten" (Article 17 GDPR) have been noted as a key reason for the narrower nature of data subject rights under the current PDPA when compared to the GDPR. See 簡毓寧 (Jian, Yu-Ning), 張馨云 (Chang, Hsin-Yun), 王世明 (Wang, Shih-Ming), "我國面對歐盟GDPR個資保護浪潮之因應與挑戰: 日本經驗之借鏡" ("Compliance and challenges in the face of the EU GDPR personal data protection wave: Lessons from Japan's experience"), 經濟前瞻186期 (12 November 2019): 56.

[32] See Judgment of the Court of Justice of the European Union (Grand Chamber): *Google Spain v AEPD and Mario Costeja González* (C-131/12).

[33] See Jure Globocnik, "The Right to Be Forgotten is Taking Shape: CJEU Judgments in *GC and Others* (C-136/17) *Google v CNIL* (C-507-17)," *GRUR International* 69, no. 4 (April 2020): 380-388.

In short, the right to data portability means that a data subject should be free to transfer his/her data from one data controller/processor to another. On the one hand, this right can be discussed from the perspective of competition law. On the other hand, portability reaffirms a deep-seated belief that individuals should be the ultimate sovereigns over their own data.[34] Taiwan's lack of a provision on the right to data portability in the current PDPA has been noted,[35] and calls have been made for its specific inclusion in the future revision of the PDPA.[36] It is therefore significant to note that Clause 19 of India's PDPB explicitly guarantees the right to data portability. Not only does the name of the Indian clause reflect the language of the GDPR, but also the content of this clause to some extent mirrors the language that is found in the equivalent GDPR provision. This includes its application to data processing through "automated means".[37]

In contrast, the new legislative framework in South Korea is less explicit when compared to the Indian example. This is because data portability in Korea's current laws is discussed in the context of credit data, which is regulated by the Credit Information Protection Act (CIPA) rather than the PIPA.[38] PIPA's provision on the "Rights of Data Subjects" (Article 4) makes no specific mention of the right to data portability. In Japan, even though there are plans to amend the APPI and expand the rights of data subjects, the right to data portability does not exist in the current APPI and has not been included in the relevant Revision Document.[39] In comparison, the explicit reference to the right to data portability in the Indian PDPB,

---

[34] Helena Ursic, "Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control," *SCRIPTed: Journal of Law, Technology and Society* 15, no. 1 (August 2018): 42-69.

[35] National Development Council (see note 30) and Jian et al. (see note 31).

[36] Taiwan People's Party, see note 9.

[37] See Article 20 GDPR.

[38] Bae, Kim and Lee LLC, "Data Protection & Privacy 2020 – South Korea – Trends and Developments," Chambers and Partners, last updated 9 March 2020, https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/south-korea/trends-and-developments/O5894.

[39] Keshawna Campbell, "Japan: APPI revision includes 'strengthening regulations of cross-border data transfers'," One Trust Data Guidance, December 2019, https://www.dataguidance.com/opinion/japan-appi-revision-includes-strengthening-regulations-cross-border-data-transfers. For a provisional English translation of the Amendment Bill of the APPI, see Personal Information Protection Commission, "Cabinet Decision on the Amendment Bill." See also Okada, Atsushi, "Japan: Impact of adopted APPI amendment bill," One Trust Data Guidance, June 2020, https://www.dataguidance.com/opinion/japan-impact-adopted-appi-amendment-bill.

a law which will determine the data protection of a very large proportion of the Asian population, signals a significant step in the evolution of data protection in the Asian region.

For rights to be effective, legal obligations must be specified. The complex and differentiated types and modes of obligations that are contained in the respective data protection laws in Japan, South Korea and India cannot be given adequate discussion within the scope of this chapter. However, some brief observations can be made as to the question of *who* should be the bearer of these obligations. How to classify entities which owe data protection obligations to data subjects is an issue which a future revision of Taiwan's PDPA may have to address. The distinction in the current PDPA between governmental and non-governmental organisations has been argued by some as being overly rigid.[40] Such calls for change reflect the fact that the protection of fundamental rights, including the right to data protection, often involves horizontal elements and strongly engages the obligations of private actors.[41] For example, rather than focusing on state/non-state distinctions, the GDPR's key distinction is between data controllers and data processors, which could be state or non-state entities, thereby focusing more on the nature of what is being done with data.[42]

In Japan's APPI, the obligations focus on the private sector. Obligations are imposed on the "personal information handling business operator"[43] and the government has the duty to regulate such operators.[44] In South Korea, the term "personal information controller" covers both public

---

[40] Chang (see note 10), 186. It has been reported that the National Development Council is considering to revise the current division between public and private bearers of data protection obligations, see 林于蘅 (Lin, Yu-Heng), "台歐27日三度協商GDPR認定 國發會：個資法勢必修法" ("Taiwan-EU to hold third round of GDPR adequacy negotiations on 27 November – National Development Council: Personal Data Protection Act should be amended"), *United Daily News*, 26 November 2019, https://udn.com/news/story/7238/4188419.

[41] The role of non-state rule makers is especially evident in cyberspace. See Chris Reed and Andrew Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham: Edward Elgar, 2018), 26-58. One key aim of "digital constitutionalism" is to limit both public and private power, see Celeste, "Digital Constitutionalism", 16.

[42] Article 6(1) GDPR lists six lawful grounds for data processing, without presenting a strict dichotomy between public and private entities. However, Article 6(1) notes that the sixth ground "shall not apply to processing carried out by public authorities in the performance of their tasks."

[43] Article 2(5) and Chapter IV APPI.

[44] Chapter II APPI.

and private sector entities.[45] India's PDPB uses the term "data fiduciary" to mean "…any person, including the State, a company, any juristic entity or any individual…"[46] However, even if public sector bodies are subject to data protection obligations, special exceptions may render the distinction to private actors once again visible: Clause 35 of India's PDPB grants the central government the power to exempt any government agency from the application of the PDPB for reasons such as national sovereignty or integrity, national security, friendly foreign relations, or public order. Of course, the GDPR also contains various restrictions to the scope of the rights and obligations contained in the GDPR. However, even before listing grounds for exceptions, the GDPR provision stipulates that such restrictions must respect the essence of fundamental rights and freedoms, and must be necessary and proportionate in a democratic society.[47] How restrictions such as those in Clause 35 of India's PDPB fare in any future adequacy decision negotiation remains to be seen.

It is noteworthy that India's PDPB makes a special distinction based on the impact that such an entity has on data processing: A "significant data fiduciary" is distinguished on the basis of the volume, sensitivity and turnover of the data it processes, as well as the risk of harm and the new technologies it uses in data processing.[48] Importantly, any social media intermediary is to be classified as a "significant data fiduciary" if the number of its users reaches above a certain threshold and the social media intermediary's actions "have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India."[49] This clearly reflects the recent global revelations regarding the power of social media platforms to sway political discourses and shape political outcomes, whether internet users are aware of this or not.[50]

---

45 Article 2(5) PIPA.

46 Clause 3(13) PDPB.

47 Article 23 GDPR.

48 Clause 26(1) PDPB.

49 Clause 26(4) PDPB.

50 See Cathy O'Neil, *Weapons of Math Destruction* (New York: Penguin Books, 2017), 179-197.

4. Data Protection Authorities

Data protection is a right which necessarily requires positive action on the part of those bearing legal obligations.[51] This can take the form of procedural safeguards or even the establishment of new institutions. Commentary on the potential revision of Taiwan's PDPA have included calls for the greater use of data impact assessments, the need to institute data protection officers, and the imperative to establish an independent data protection authority (DPA).[52]

The special significance of a DPA is highlighted by the fact that its existence counts as one of the most important criteria for successfully obtaining a positive GDPR adequacy decision by the EU.[53] Currently Taiwan lacks an independent DPA, but plans are being made to remedy this situation.[54] Legislation in Japan, South Korea and India all contain detailed provisions on their respective DPAs.[55]

In terms of composition, the members of the respective DPAs range from around seven to nine members in total.[56] Terms of office range from three to five years; reappointments are possible in Japan and South Korea, whereas in India reappointment is prohibited.[57] The methods of appointments vary. In Japan, appointment is by the Prime Minister with the consent of the legislature,[58] whereas in South Korea and India multiple bodies are involved. In South Korea, the power of appointment is allocated between different groups,[59] whereas in India the recommendation for

---

[51] For a discussion on data protection as a fundamental right, see Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Cheltenham: Edward Elgar, 2015), 186-213.

[52] 闕光威 (Que, Guang-Wei) and 陳婉茹 (Chen, Wan-Ru), "歐盟個人資料保護新規之衝擊與影響" ("Impact and influence of the new EU personal data protection regulation"), 22(1) 全國律師 (January 2018): 81-82; Jian et al. (see note 31), 56; Taiwan People's Party (see note 9).

[53] Recital 104 GDPR.

[54] National Development Council, see note 8.

[55] Chapter V APPI, Article 7 PIPA, Chapter IX PDPB.

[56] Article 63(1) APPI: nine members; Article 7-2(1) PIPA: nine members; Clause 42(1) PDPB: not more than seven members.

[57] Article 64 APPI: five years; Article 7-4 PIPA: three years, consecutive appointment once; Clause 43 PDPB: whichever is earlier, either the completion of a non-renewable term of five years or reaching the retirement age of 65.

[58] Article 63(3) APPI.

[59] Article 7-2 PIPA.

appointment is made by a selection committee.[60] Interestingly, the Indian PDPB stipulates that the selection committee shall include members from government departments that are in charge of legal affairs and affairs dealing with electronics and information technology.[61]

The most important aspect of a DPA is its independence. This depends on various factors, and in all the relevant laws one can find a combination of provisions which aim to secure independence. Some of the above-mentioned provisions also indirectly contribute to independence, but more direct requirements are also necessary. It can be an explicit prescription that they shall exercise their powers and authorities "independently",[62] and in all three countries the reasons for dismissal must be specifically enshrined in law.[63] The relevant Indian provisions also provide some procedural safeguards which apply in some situations of dismissal.[64] The provisions in all three countries also prohibit the commissioners from engaging in political campaigning, and also stipulate rules on profit-making activities.[65] The Indian provisions stand out for mandating a two-year prohibition on commissioners, once they leave their office, from accepting appointments to positions in government or at "significant data fiduciaries".[66]

5. Conclusion

This chapter's starting point is that Taiwan is currently in the process of seeking legislative change in order to secure a GDPR adequacy decision in the near future. A comparative overview of developments in other Asian democracies, especially those which are currently more advanced in terms of GDPR-relations with the EU or generally the revision of their relevant laws, can provide some orientation and inspiration.

---

60 Clause 42(2) PDPB.

61 Clause 42(2)(b) and (c) PDPB.

62 Article 62 APPI; Article 7-5(2) PIPA.

63 Article 65 APPI; Article 7-5(1) PIPA; Clause 44(1) PDPB.

64 Clause 44(2) PDPB.

65 Article 71 APPI; Article 7-6 PIPA; Article 43(3) PDPB.

66 Clause 43(3)(a) and (b) PDPB.

Developments in Japan, South Korea and India demonstrate the following: There is a trend of having a broad understanding of personal data; data subjects enjoy a broad set of rights, even though some of the newest rights such as data portability have not yet been consistently incorporated; usually there is no rigid distinction between public and private entities in terms of legal obligations, yet exceptions to the action of public authorities should not be underestimated; and different depths of institutional design exist to guarantee the independence of data protection authorities.

Due to the limited scope of this chapter, no exhaustive and comprehensive comparison was possible. However, the chosen issues focused on matters which are foundational for a discussion on data protection, and aimed to represent an overview of the different stages of data protection: definition of personal data, data subject rights, the bearer of legal obligations, and the institutional prerequisites of DPAs as the ultimate enforcer of data protection.

Further in-depth comparative studies of Asian democracies on these and other issues will be of instrumental value for future national and regional norm-setting endeavours. Examples of other issues for future research include the meaning of consent, criteria for the lawfulness of data processing, the tools for balancing different interests, and connections to nascent regional data protection systems such as the Cross-Border Privacy Rules of APEC. The GDPR's evolving global influence, including in Asia, will be especially worthy of continued research since GDPR adequacy decisions are subject to periodic review. The future of data protection determines the future of cyberspace governance.

Fabian Duessel is a Deputy Director of the AACC Affairs Division of the Constitutional Court of Korea, which also functions as the Secretariat for Research and Development (SRD) of the Association of Asian Constitutional Courts and Equivalent Institutions (AACC). The views expressed in this paper are solely the personal views of the author and do not necessarily represent the views of AACC SRD or the Constitutional Court of Korea.

2

Cyber Norms and International Law in ASEAN

Eugene EG Tan

The absence of a normative regime in cyberspace at the moment allows malicious actors to operate in a grey area where there is a low-risk, high-reward scenario to the attackers. In a sense, states operating today in cyberspace are bound in a situation akin to the Thucydidean scenario where the strong do what they want, and the weak suffer what they must.[1]

In 2015, the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications (ICT) in the context of International Security proposed eleven norms to ensure responsible state behaviour in cyberspace.[2] Having an agreed set of norms will benefit and affect all states in the international system, even those who have chosen not to adhere to the norms regime. There is a great reputational risk to states that choose to flagrantly ignore an internationally recommended norms regime.

ASEAN has done much to advance the creation of norms in the region under the chairmanship of Singapore in 2018. The 32nd ASEAN Summit in April 2018 brought forth a slew of statements from leaders recognising that norms and the rule of law are needed for cyberspace, and serve as a basis for using technology to advance economic growth in the region.[3]

---

[1] Thucydides, *The Peloponnesian War*, (trans. Steven Latimer), 5:89.

[2] United Nations General Assembly (2015) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[3] Prashanth Parameswaran (2018) "ASEAN Cybersecurity in the Spotlight Under Singapore's Chairmanship", *The Diplomat*, 2 May 2018, https://thediplomat.com/2018/05/asean-cybersecurity-in-the-spotlight-under-singapores-chairmanship/.

The ASEAN Leaders Statement on Cybersecurity made at the summit called for the identification of a concrete list of voluntary, practical norms of state behaviour in cyberspace that ASEAN can work towards adopting, taking reference from the eleven norms recommended by the 2015 UNGGE.[4] The ASEAN Ministerial Conference on Cybersecurity (AMCC) held in September 2018 also agreed that there is a need for a more formalised mechanism for ASEAN cyber coordination, and tasked Singapore to propose a mechanism for the AMCC to consider. The AMCC has also in-principle agreed to subscribe to the eleven voluntary, non-binding norms recommended by the 2015 UNGGE, as well as to focus on regional capacity building in implementing these norms.

Having and respecting a rules-based order is one of the 10 key principles underscoring the Leaders' Vision statement, which called upon ASEAN to promote the rule of law, anchored in respect for international law and norms.[5] This will in turn help with the development of the ASEAN Smart Cities network[6] and fulfil the leaders' pledge on cybersecurity cooperation.

Scholars have also tried to compare the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in hope that the processes to understand international law and conform to norms are similar.[7] This is unlikely to work, because unlike European Union leaders, ASEAN leaders place much importance on the principles of "mutual respect" and "non-interference", rather than desiring to move to a European-style integration on rules and law. ASEAN should be seen as a unique area where the formation of a regional grouping is based largely on mutual benefits and geography rather than a common cultural heritage, a common language or the need to face similar economic and security problems.

These structural impediments faced by ASEAN and the different member states in the physical space will translate to challenges of framing,

---

[4] ASEAN (2018) "ASEAN Leaders' Statement on Cybersecurity Cooperation", https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf; United Nations General Assembly (2015) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[5] ASEAN (2018) "ASEAN Leaders' Vision for a Resilient and Innovative ASEAN", https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Vision-for-a-Resilient-and-Innovative-ASEAN.pdf.

[6] ASEAN Smart Cities Network, https://asean.org/asean/asean-smart-cities-network/.

[7] Murray, Philomena (2010) "Comparative Regional Integration in the EU and East Asia: Moving beyond Integration Snobbery", *International Politics* Vol. 47 (2010), 308-323.

interpreting, and enforcing international law and norms in cyberspace. Understanding the governance of cyberspace in ASEAN therefore requires more than just recognising the political declaration made at the 32nd ASEAN Summit in 2018 by the leaders of the ASEAN member states.[8] The understanding and the level of implementation of cyber norms agreed at the 2015 UNGGE among the ASEAN member states are varied at best.

The revolving chairmanship of ASEAN also meant that the development in the governance of cyberspace has been superseded by other priorities of the incoming chairs. Progress in governance in cyberspace post-2018 has significantly slowed, with the only advancement in the governance process being the submission of a formal framework for regional cooperation by Singapore for consideration at the 2019 AMCC; it having been tasked the year before.[9]

This article thus seeks to first, elucidate the intricacies of ASEAN; second, explain how ASEAN views international law and norms; and third, establish how ASEAN can further strengthen the adoption and application of international law and norms in cyberspace. On this basis, the article argues that while ASEAN has on occasion stressed the need and its respect for a rules-based international order, it is not dogmatic on the framing of international law when it perceives that there is a deficit of order in the international system.

International Law and Southeast Asia

The ASEAN Charter[10] recognises that ASEAN has an international legal personality with a region-wide commitment to international law, the rules of an international public order, institutional and member-state accountabil-

---

[8] ASEAN (2018) "ASEAN Leaders' Statement on Cybersecurity Cooperation", https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf.

[9] "Singapore to draw up formal Asean mechanism for cyber security", *Straits Times*, 20 September 2018, https://www.straitstimes.com/singapore/singapore-to-draw-up-formal-asean-mechanism-for-cyber-security.

[10] Charter of the Association of Southeast Asian Nations, Singapore, 2007, https://asean.org/asean/asean-charter/charter-of-the-association-of-southeast-asian-nations/.

ity as a platform for compliance as well as respect for political pluralism under a common conception of shared values.[11]

It can be said that the establishment of ASEAN from the beginning is an expression of the member states' adherence to certain common values and principles, and commitment to internationally agreed principles and law. In addition to the ASEAN Charter of 2007[12], these common values and principles are set forth in the following documents:

- the ASEAN Declaration (Bangkok Declaration) of August 1967[13];
- the Declaration of ASEAN Concord of 1976[14];
- the Treaty of Amity and Cooperation in Southeast Asia of 1976[15];
- the ASEAN Vision 2020 of 1997[16];
- the Declaration of ASEAN Concord II (Bali Concord II) of 2003[17]; and,
- the Vientiane Action Programme of 2004[18].

The 1967 Bangkok Declaration Article 2(2) reaffirms the member states' commitment to "respect for justice and the rule of law in the relationship among countries of the region."[19] The 1976 ASEAN Concord mentioned "reliance on peaceful processes in the settlement of intra-

---

[11] Desierto, Diane A. (2008) "Postcolonial International Law Discourses on Regional Developments in South and Southeast Asia", *International Journal of Legal Information*, vol. 36, p. 387.

[12] ASEAN Charter (2007).

[13] The ASEAN Declaration (Bangkok Declaration), 8 August 1967, https://asean.org/the-asean-declaration-bangkok-declaration-bangkok-8-august-1967/.

[14] The Declaration of ASEAN Concord, Bali, Indonesia, 24 February 1976, https://asean.org/?static_post=declaration-of-asean-concord-indonesia-24-february-1976.

[15] Treaty of Amity and Cooperation in Southeast Asia Indonesia, 24 February 1976, https://asean.org/treaty-amity-cooperation-southeast-asia-indonesia-24-february-1976/.

[16] ASEAN VISION 2020, Kuala Lumpur, Malaysia, 15 December 1997, https://asean.org/?static_post=asean-vision-2020.

[17] Declaration of ASEAN Concord II (Bali Concord II), 7 October 2003, https://asean.org/?static_post=declaration-of-asean-concord-ii-bali-concord-ii.

[18] VIENTIANE ACTION PROGRAMME (VAP) 2004-2010, https://www.asean.org/storage/images/archive/VAP-10th%20ASEAN%20Summit.pdf.

[19] Bangkok Declaration (1967).

regional differences" and "mutual assistance in case of natural disasters".[20] Article 2 of The Treaty of Amity and Cooperation in Southeast Asia of 1976 committed states to be guided by a list of fundamental principles, which include the "settlement of differences or disputes by peaceful means".[21] The Treaty further defined its purpose by pledging "to promote perpetual peace, everlasting amity and cooperation among their peoples which would contribute to their strength, solidarity and closer relationship".[22] The Vientiane Action Programme in 2004 spoke about the need for norms of good conduct and described the ways to prevent conflict in the region.[23]

The current ASEAN agreements and declarations suggest, however, that ASEAN member states are not ready to move towards community law for deeper integration. ASEAN declarations, agreements and action plans are usually vague and too general to set practical rules of cooperation. ASEAN leaders typically fail to define clearly the meaning of its resolutions, making the implementation of the protocols signed at the summit by the ASEAN Secretariat difficult.[24] While ASEAN agreements appear to be legal achievements on some points, their substantial practice in fact is questionable because of the non-committal and neutral language used. These neutral words that yield little practical meaning include "promoting", "conducting", "encouraging" or "developing". It is also noted that ASEAN members often prioritise their respective self-interest instead of looking for collective benefits because of their individual political, economic, cultural, social and ethnic differences.[25]

Singapore, among others in Southeast Asia, does recognise the impact and the need for states to be part of the international law-making process, and that having well-developed international law that encompasses the interests of all states will order the international system to protect the interests and equality of smaller states.[26] The region is active in framing

---

[20] ASEAN Concord (1976).

[21] Treaty of Amity and Cooperation (1976).

[22] Ibid.

[23] Vientiane Action Programme (2004).

[24] Tan, Lay Hong (2004) "Will ASEAN Economic Integration Progress beyond a Free Trade Area?", ICLQ, Vol. 53, pp. 935-967.

[25] Ibid.

[26] Tan, Eugene EG (2020) "A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore", *Prism*, Vol. 8 No. 3 (January 2020).

international law and using international law as a dispute settlement mechanism among states, even in the physical realm.

Similarly, this general positive attitude towards international law is translatable to the efforts made by various states in the region towards the making of norms and the interpretations of international law in cyberspace.

Past Regional Experiences in International Law

Framing International Law

This flexibility in making fresh contributions to international law is an important feature in how the region approaches international law. The region's experience in framing international law is best encapsulated in its role in the development of the United Nations Convention on the Law of the Sea (UNCLOS).

As a background to UNCLOS, the international order post-Second World War was crumbling with the end of empires and the rise of new independent states. This situation was made worse with the uneven adoption of technology, where states with the wherewithal to own advanced fishing boats with radars could sail up to the territorial sea limit – then three nautical miles off the coast of any given state – to fish. States started to act unilaterally against the international order by setting their own limits to their territorial sea and fishing areas. The first two United Nations Conferences on the Law of the Sea in 1958 and 1960 mandated to discuss these issues of territoriality and sovereignty ended in failure.[27]

UNCLOS was born out of the third United Nations Conference on the Sea, which convened in December 1973.[28] The UNCLOS process took almost nine years to complete, with adoption of UNCLOS taking place on 30 April 1982. The process that made UNCLOS possible also means that international law concepts can be tweaked and are not concepts made *in and for perpetuity,* although it must be done so in a manner that all states can agree with while respecting the interests and stability of all states.

---

[27] United Nations Conference on the Law of the Sea, https://legal.un.org/diplomaticconferences/1958_los/.

[28] United Nations Convention on the Law of the Sea of 10 December 1982, https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm.

The provisions made in UNCLOS were, in the words of Professor Tommy Koh, the president of the final year of the Conference, "revolutionary" as UNCLOS invented new concepts of international law that were modern and equitable.[29]

This revolutionary tilt towards international law can be seen in how the concept of "archipelagic states" came to be accepted as an international law concept. The novel concept redefined how the territory of an archipelagic state is measured, and, with the Southeast Asian region being a partly archipelagic region, had an immense impact on how the region is ordered. Indonesia and the Philippines had sought recognition as archipelagic states in the first two United Nations Conferences on the Sea, but were turned away. UNCLOS changed this by allowing archipelagic states to draw its baseline from the outermost points of the outermost islands rather than from each individual island. The waters inside the baseline will be thus considered archipelagic waters.[30]

The region has also shown itself to be slow in adopting international treaties that it did not have a hand in framing, despite ASEAN's general principle of cooperation for peace and security. An example of this in cyberspace is the lone signatory of the Philippines to the Convention on Cybercrime, otherwise known as the Budapest Convention, in its almost twenty years of existence.[31] Signed in November 2001 and coming into force three years later, the Convention was a treaty process initiated by the Council of Europe, seeking to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation".[32]

---

[29] Koh, Tommy (2019), "The UN Convention on the Law of the Sea: A Revolutionary Treaty", *Straits Times*, 30 April 2019, https://cil.nus.edu.sg/publication/the-un-convention-on-the-law-of-the-sea-a-revolutionary-treaty/.

[30] Ibid.

[31] NATO CCDCOE (2019) ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone, https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/.

[32] Council of Europe (2001), Convention on Cybercrime (ETS 185), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Application of International Law

Scholars have described Southeast Asia as more of a geographical than a political, economic or cultural region, making it more difficult for ASEAN members to engender mutual trust to move quickly on effective regional integration and on strengthening common standards and values.[33] This can be seen in the different border disputes that have arisen in the region post-Second World War, when most of the states, bar Thailand, gained independence. Southeast Asian states are, however, respectful of the application of and submission to international law.

Cases that were submitted to international law adjudication include:

- ASEAN's opposition to Vietnam's invasion of Cambodia in 1979[34];
- the settlement between Singapore and Malaysia over Pedra Branca in 2008[35];
- the dispute between Thailand and Cambodia over the Temple of Preah Vihear in 1962[36]; and,
- the Philippines seeking adjudication by the Permanent Court of Arbitration (PCA) over certain issues in the South China Sea in 2013 under UNCLOS.

The verdicts passed down by international law courts have largely been respected by the claimant states, with the exception of the PCA ruling on the South China Sea. The dispute between Cambodia and Thailand over the Temple of Preah Vihear also descended into skirmishes between the

---

[33] Lin, Chun Hung (2010) "ASEAN Charter: Deeper Regional Integration under International Law?", *Chinese Journal of International Law*, Vol. 9, p. 827.

[34] "Sovereignty principle was at stake in Vietnam's invasion of Cambodia in 1978", *Straits Times*, 8 June 2019, https://www.straitstimes.com/singapore/sovereignty-principle-was-at-stake-in-vietnams-invasion-of-cambodia-in-1978.

[35] Government of Singapore (n.d.), *Pedra Branca*, Ministry of Foreign Affairs, https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/Key-Issues/Pedra-Branca; "Malaysia accepts ruling on Pedra Branca, says Mahathir", *Straits Times*, 25 June 2019, https://www.straitstimes.com/politics/malaysia-accepts-ruling-on-pedra-branca-says-pm-mahathir.

[36] Updates on the Case Temple of Preah Vihear (Cambodia v. Thailand), https://www.icj-cij.org/en/case/45.

claimant states as recently as 2008, and a second ruling by the International Court of Justice (ICJ) was required to restore order.[37]

Cyber Norms and ASEAN

As previously observed, ASEAN member states are generally welcoming of having behavioural norms for states, having previously agreed to a set of normative behaviour standards for states to ensure security and stability in the region as part of the Vientiane Action Programme in 2004.[38] Having done this previously, it is therefore not surprising that the ASEAN member states agreed to be guided by the eleven norms recommended by the 2015 UNGGE, albeit only three years after the recommendations were made.[39]

The subsequent UNGGE in 2017 ended without a consensus agreement, casting doubt over the ability of states to make further progress on behavioural norms in cyberspace. This doubt led to the birth of more initiatives to create norms, both by non-government organisations, such as Global Commission on the Stability of Cyberspace (GCSC)[40] and the Global Forum of Cyber Expertise (GFCE)[41], and states, like France, which launched calls to action.[42] These moves were meant to inject impetus into what was seen as a moribund norms process.

Some ASEAN member states have occasionally shown support and participated in these multi-stakeholder efforts at establishing norms of behaviour in cyberspace. The governments of Cambodia, Philippines, and Singapore have expressed support for the nine principles in the Paris Call, and Singapore was recognised as one of the partners of the GCSC, having hosted one of the meetings during Singapore International Cyber

---

[37] REQUEST FOR INTERPRETATION OF THE JUDGMENT OF 15 JUNE 1962 IN THE CASE CONCERNING THE TEMPLE OF PREAH VIHEAR (CAMBODIA v. THAILAND), 11 November 2013, https://web.archive.org/web/20131111173337/http://www.icj-cij.org/docket/files/151/17704.pdf.

[38] VIENTIANE ACTION PROGRAMME (VAP) 2004-2010.

[39] United Nations General Assembly (2015), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[40] Global Commission on the Stability in Cyberspace, https://cyberstability.org/.

[41] The Global Forum on Cyber Expertise, https://thegfce.org/.

[42] Paris Call For Trust and Security in Cyberspace, 12 November 2018, https://pariscall.international/en/.

Week 2018.[43] It will, however, take time for all ASEAN member states to accept the recommendations on norms by these initiatives, because of the varied capacity in understanding and implementing these additional norms of behaviour among the ASEAN member states.

These new initiatives have caused concern to a few scholars, such as Eneken Tikk. The main complaint is that the norms process has become mired in a discussion to encompass wider applications of norms in all scenarios, rather than solely focusing on international security or peace. To them, this catch-all, solve-all approach seeks to address everything that is wrong with cyberspace. This in turn dilutes the quality of the discussion and the purpose of cyber norms. Adding to the frustration of these scholars is the fact that the norms being developed are being promoted as being voluntary and non-binding.[44]

That said, multilateral processes setting rules for responsible behaviour in cyberspace for states are set to continue for the foreseeable future. There are currently two ongoing processes at the United Nations discussing international security with regard to the use of cyberspace – the Open-ended Working Group (OEWG) and the Group of Governmental Experts (UNGGE).[45] Both these processes seek to "develop the rules, norms and principles of responsible behaviour of States", albeit with differences in how information security is dealt with vis-à-vis information and communication technologies (ICT) and in the composition of group membership.[46]

Regionally, there is recognition that there is an urgent need to address cybersecurity issues irrespective of political views held by the OEWG process "led" by Russia and China or the West-sponsored UNGGE process. Indonesia and Singapore, the two regional representatives to the UNGGE process, together with the Philippines, voted to advance both processes in spite of ideological differences between the processes. Additionally, Singapore was of the view that the two processes to be established by

---

[43] GLOBAL COMMISSION INTRODUCES SIX CRITICAL NORMS TOWARDS CYBER STABILITY, https://cyberstability.org/research/singapore_norm_package/.

[44] Tikk, Eneken (2019) "2018: The year that cyber peace became non-binding", *ICT4Peace*, https://ict4peace.org/wp-content/uploads/2018/12/ICT4PeaceFoundation_The_year_that_cyber-peace_became_non-binding2018-12-31-1.pdf.

[45] United Nations, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct", GA/DIS/3619, 8 November 2018, https://www.un.org/press/en/2018/gadis3619.doc.htm.

[46] Ibid.

both drafts are not incompatible to each other, and both drafts had been amended in the negotiation process to embrace different views.[47]

Similarities between the ASEAN Charter and the 2015 UNGGE Cyber Norms

Another key reason for the relatively swift adoption of the 2015 UNGGE norms[48] by ASEAN member states is the similarity between all eleven of the recommended norms and the obligations that the ASEAN member states have agreed to in the ASEAN Charter agreed in 2007.

For instance, the norm calling on states to "not knowingly allow their territory to be used for internationally wrongful acts using ICTs" can be mapped onto Article 2.2 (k) of the ASEAN Charter, calling on ASEAN member states to "abstain from participation in any policy or activity, including the use of its territory, pursued by any ASEAN Member State or non-ASEAN State or any non-State actor, which threatens the sovereignty, territorial integrity or political and economic stability of ASEAN Member States".[49]

Further, the willingness to be guided by *all* the eleven norms is surprising because of the inherent tensions over human rights in ASEAN. One of the 2015 UNGGE norms calls for the "promotion, protection and enjoyment of human rights on the Internet",[50] which runs contrary to the scepticism that international observers have over some ASEAN member states' adherence to the current human rights regimes and their obligations.[51] Human rights are protected in ASEAN as one of the principles in the ASEAN Charter, Article 2.2(i).[52] ASEAN member states have further committed to

---

47 Ibid.

48 United Nations General Assembly (2015) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015 https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

49 ASEAN Charter, 2007.

50 UNGA (2015), Report of the UNGGE.

51 Gerber, Paula (2012), "ASEAN Human Rights Declaration: a step forward or a slide backwards?", *The Conversation*, 21 November 2012, https://theconversation.com/asean-human-rights-declaration-a-step-forward-or-a-slide-backwards-10895.

52 ASEAN Charter, 2007.

the ASEAN Human Rights Declaration in November 2012, including the freedom of expression and opinion.[53]

The norms recommended by the UNGGE also places much importance on cooperation to tackle cybercrime and terrorism, which is an important issue to ASEAN member states. The ASEAN Charter places much emphasis on cooperation against transnational crime through its expressed purpose in "responding effectively … to all forms of threats, transnational crime and transboundary challenges" and "to strengthen cooperation in building a safe, secure, and drug-free ASEAN", and its principle in having a "shared commitment and collective responsibility in enhancing regional peace, security and prosperity".[54]

Integration of Laws vis-à-vis Cyberspace among ASEAN Member States

Having agreed regionally on the goals, principles and purposes of ASEAN with regard to the use of cyberspace, the challenge now for ASEAN is to develop a set of domestic legislation that is translatable among ASEAN member states. Unlike the European Union, where its legal system has binding legal force throughout every member state, ASEAN has no such legal standing. Current ASEAN agreements and declarations usually allow the member states to enact laws that enable them to fulfil their individual obligations towards ASEAN, which may take significantly more effort and time.[55]

The legal systems of the ASEAN member states also differ greatly, ranging from common law as in the case of Singapore to civil law systems such as that in Indonesia, and hybrids of both, such as in Thailand, which makes it difficult to build a community law. ASEAN member states have also been reluctant to encourage the formation of a binding uniform legal system, stemming from a fear of impinging on ASEAN's long-held principles of non-interference and consensus.[56] To this, some scholars have argued

---

[53] ASEAN Human Rights Declaration, November 2012, https://asean.org/asean-human-rights-declaration/.

[54] ASEAN Charter, 2007.

[55] Lin (2010), ASEAN Charter.

[56] Sim, Edmund W. (2008) "The ASEAN Charter: One of Many Steps towards an ASEAN Economic Community", *International Trade LR*, Vol. 14, pp. 109-116.

that ASEAN may be relying on "consultation" and "consensus" principles to tactically reach agreements on how the domestic laws of the different ASEAN member states can be integrated into a regional legal system that respects cultural sensitivities and national sovereignty.[57]

There is also value in developing legislation that can be translated across all ASEAN member states and by extension, a common language related to cyberspace. Singapore and Vietnam both passed cybersecurity legislations in 2018, but these deal with totally different areas of cybersecurity, with Singapore focussing on the protection of critical infrastructure[58], and Vietnam on the localisation of data and control of content.[59] Thailand updated and strengthened the Thai Computer Related Crime Act of 2017 in 2019 to include information and content restrictions.[60] The timing of the Thai update has been criticised for being too close to the elections in 2019, and the law has been used to charge political rivals.[61]

This does not mean that Singapore has no concerns over security risks stemming from the content and information available in cyberspace, and has chosen to eschew regulation on information in cyberspace to focus solely on critical infrastructure protection. Singapore passed in June 2019 a separate law governing the proliferation of deliberate online falsehoods, the Protection from Online Falsehoods and Misinformation Act.[62] The Act

---

[57] The legal systems of ASEAN member states are legacies from their colonial past. The Philippines' legal system is rooted in strong influences from United States laws; common law forms the basis for the legal systems of Brunei, Malaysia and Singapore; while Indonesian laws follow the Dutch legal system. Thailand, having not been colonised before, has elements of both civil and common law systems. See Haas, Deborah A. (1994) "Out of Others' Shadows: ASEAN Moves toward Greater Regional Cooperation in the Face of the EC and NAFTA", *American University JILP*, Vol. 9 (1994), 809.

[58] Government of Singapore (2018) Cybersecurity Act 2018, https://www.csa.gov.sg/legislation/cybersecurity-act.

[59] Wen, Ruiqiao (2019) "Vietnam's New Cybersecurity Law: A Headache for US Service Providers?", *Georgetown Law Tech Review*, https://georgetownlawtechreview.org/vietnams-new-cybersecurity-law-a-headache-for-us-service-providers/GLTR-02-2019/.

[60] Government of Thailand (2019) Cybersecurity Act, B.E. 2562 (2019), https://www.mdes.go.th/law/detail/1904-Cybersecurity-Act--B-E--2562--2019-.

[61] "Future Forward's Thanathorn charged with computer crime", *Bangkok Post*, 24 August 2018, https://www.bangkokpost.com/thailand/politics/1527190/future-forwards-thanathorn-charged-with-computer-crime.

[62] Government of Singapore (2019), PROTECTION FROM ONLINE FALSEHOODS AND MANIPULATION ACT 2019, https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625.

seeks to protect the society from deliberate online falsehoods created by malicious actors by targeting falsehoods, not opinions and criticisms, nor satire or parody. It defines a falsehood as a "statement of fact that is false or misleading."[63] This clarity between the concepts of cybersecurity and information security may enable states to discuss these issues and strengthen normative behaviour on each concept globally at the OEWG and UNGGE.

Capacity Building Measures in ASEAN

To enable states to better discuss these issues, the 2015 UNGGE report also endorsed the capacity building measures proposed by the 2010 and 2013 iterations of the UNGGE. The 2013 report had "called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use".[64] The 2015 UNGGE also stressed that "capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats".[65]

According to the 2017 ASPI Cyber Maturity Report, the Asia-Pacific region has so far escaped a major state-led cyber incident more because of the peaceful macro environment than because of strong defences and resiliency. At the individual level, more than 55% of people in the Asia-Pacific are still not connected to the internet. While this represents a massive growth opportunity, it also points towards large-scale early user vulnerability as this population comes online.[66]

---

[63] Ministry of Law, Singapore (2019) *New Bill to Protect Society from Online Falsehoods and Malicious Actors*, https://www.mlaw.gov.sg/news/press-releases/new-bill-to-protect-society-from-online-falsehoods-and-malicious-actors.

[64] United Nations General Assembly (2013) "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/68/98, https://undocs.org/A/68/98.

[65] UNGA (2015), Report of the UNGGE.

[66] Australian Strategic Policy Institute (2018) *Cyber Maturity in the Asia-Pacific Region 2017*, Canberra, Australia: ASPI, https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017.

The report also notes that some states in the ASEAN region lack the capacity to make policies and to protect their critical infrastructure.[67] For example, although Myanmar set up its Computer Emergency Response Team (mmCERT) in 2004, membership of the group remains a small group of eight people in 2018. This team is responsible for "incident handling, research on cybersecurity, providing technical advisories, conducting trainings, seminars and workshops to constituencies, Computer and Technological Universities' Students, as well as providing effective Capacity Building to Technical Team members, enhancing public awareness, and promoting International and National Co-operations for CERT Activities and doing Research on Log Data Analysis". [68]

ASEAN is willing to work with states from within and outside the region to address this deficit in capacity. Different ASEAN member states have stood up initiatives to provide capacity building programmes in collaboration with others.

The ASEAN-Japan Cybersecurity Cooperation Hub was started in December 2017, with funding from the Japan-ASEAN Integration Fund (JAIF). A physical cybersecurity training centre was set up in Bangkok, with the view to train at least 280 ASEAN cybersecurity experts and specialists on CYDER (Cyber Defence Exercise with Recurrence), forensics, and malware analysis, and raise cybersecurity awareness among youth in the region.[69]

Singapore has pledged 30 million SGD to set up the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) to help "build a more secure and resilient cyberspace through capacity building programmes for ASEAN senior policy and technical officials with decision-making responsibilities". This represents an upgrade on the 10 million SGD ASEAN Cyber Capacity Programme (ACCP) that Singapore started in 2016. Singapore is not the only contributor to the centre, with collaboration efforts from other ASEAN member states, ASEAN dialogue partners, and international partners including Australia, Canada, European Union, Japan, New Zealand, Republic

---

[67] Ibid.

[68] APCERT (2019) APCERT Annual Report 2018, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2018.pdf.

[69] Japan-ASEAN Integration Fund (2018) ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2), https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html.

of Korea, United Kingdom and United States. The centre intends to run virtual cyber defence training and exercises, provide CERT-related technical training, and conduct research and provide training in international law, cyber strategy, legislation, norms, and other policy issues.[70]

Cyber Norms and International law for ASEAN: The Way Forward

These capacity building measures can help ASEAN understand threats better and may lead ASEAN member states to reach a common understanding on what cyber norms and international law mean to ASEAN, especially once these threats become more apparent to their own domestic security. As seen above, the understanding of what cyber norms mean and why they are important are very disparate among ASEAN member states. It is important to note that norms are not rules, but a set of commonly accepted behaviour that can be practised by states, society, and individuals.

ASEAN member states need to develop a common language related to cyberspace, and by extension, a common understanding of how the obligations placed by the 2015 UNGGE norms translate to domestic legislation in the individual states. This will help the ongoing processes at the UN to assess behavioural norms (short of a treaty) and demonstrate how having a robust, well-implemented set of behavioural norms can contribute to international security and stability in cyberspace. The success in implementation of the 2015 UNGGE norms can in turn give rise to another set of norms that are stronger and binding on all states.

ASEAN is a body created for cooperation, and should do more on its framework for cooperation among ASEAN member states and external parties in order to build cyber capacity in ASEAN – be it in policy, norms, or technical capabilities. Perhaps CERT-to-CERT cooperation among ASEAN member states can serve as a template for cooperation among ASEAN member states and Track II partners. The non-political nature of CERT-to-CERT cooperation allows states to deal with cyber issues to instil confidence in each other's capability to deal with cyberattacks. This, in turn, engenders the trust among states that partner states have the

---

[70] Cybersecurity Agency Singapore (2019) Factsheet: ASEAN-SINGAPORE CYBERSECURITY CENTRE OF EXCELLENCE (ASCCE), https://www.csa.gov.sg/-/media/csa/documents/sicw_2019/amcc/factsheet-ascce-2019.pdf.

capability to not let its territory be used for committing internationally wrongful acts against another state.

Cyber maturity among ASEAN member states is improving, but there is still much work to be done to be able to fulfil the eleven norms agreed.[71] As stated in the ASEAN ICT Masterplan 2020, ASEAN wishes to use ICT to enable "an innovative, inclusive, and integrated ASEAN" that is safe and secure.[72] To do this, ASEAN will build on its own terms a stable and prosperous cyberspace governed by rules and norms in a trust-based environment based on the collective interests and political nature of its member states, rather than one that is moulded by states outside the region. ASEAN has followed this instinct of creating an internationally agreed, rules-based order based on its own interests in other arenas where international law is absent; it would be foolish to expect a different outcome for governance in cyberspace.

Eugene EG Tan is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

[71] Hanson, Fergus et al. (2017) *Cyber Maturity in the Asia-Pacific Region 2017*, Australian Strategic Policy Institute, 2017.

[72] ASEAN (2015) ASEAN ICT Masterplan 2020, https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf.

3

Regulating Privately Developed Public Technology in South and Southeast Asia: A Critical Analysis of Governance Through and Governance of Emerging Technology

Vidushi Marda

Introduction

In the last few years, states in South and Southeast Asia have grappled with the intersection of technology and governance more than ever before. The allure of technical solutions for states can be attributed to a few reasons – applications of biometrics, for instance, offer identification and authentication at an unprecedented scale; emerging technologies like artificial intelligence (AI) hold the promise of uncovering patterns and analysis with extraordinary speed; "smart cities" promise to herald a cost effective and data-driven era of governance.

In 2020, real-world examples of these deployments abound. Singapore's "Smart Nation" plans are well underway, with AI-powered governance solutions already in operation.[1] Smart cities are increas-

[1] Housing & Development Board, *Success Story HDB: Optimizing Customer Service Through Intelligent Virtual Assistants*, Taiger, July 2018, http://old.taiger.aikenstaging.com/wp-content/uploads/2018/07/HDB-Success-Story-iConverse-Taiger.pdf.

ingly popular in other countries too, notably Malaysia,[2] India,[3] Indonesia,[4] Vietnam,[5] and the Philippines,[6] among others. India is home to the largest biometric database in the world, Aadhaar.[7] It is also building the Automated Facial Recognition System (AFRS) to centralise crime and criminal tracking between police stations all over the country.[8] Myanmar's Ministry of Labour, Immigration and Population (MoLIP) plans to roll out a national biometric identity system in 2020.[9]

The vehicles for this era of governance are privately developed technology, which significantly impact constitutional rights and economic growth. This essentially makes private entities arbiters of governance in some cases, giving rise to questions of accountability, transparency and redressal. At the same time, there has been a marked increase in conversations around policies and regulations concerning data protection, data localisation, AI, etc. For instance, data protection bills are currently pending in India, Thailand, Indonesia and Vietnam; smart cities missions have emerged from most countries in the region as well.

These developments occurring in parallel bring to the fore an important question: what is the regulatory landscape in a constantly evolving, textured field? How should regulators respond, and who has been influencing the forms and extents of regulations? What are the larger goals, assumptions and incentives that are guiding regulations?

---

[2] Alita Sharon, "*Malaysia Pushing Smart City Initiatives*", OpenGov, 28 November 2019, https://www.opengovasia.com/malaysia-pushing-smart-city-initiatives/.

[3] Government of India, Ministry of Housing and Urban Affairs, "*Smart Cities Mission*", http://smartcities.gov.in/content/.

[4] Jonathan Davy, "What lies ahead of Indonesia's 100 Smart Cities movement?", *The Jakarta Post*, 5 December 2019, Science and Tech, https://www.thejakartapost.com/life/2019/12/05/what-lies-ahead-of-indonesias-100-smart-cities-movement.html.

[5] Samaya Dharmaraj, "Vietnam's Plans for Smart City Projects", OpenGov, 18 October 2019, https://www.opengovasia.com/vietnams-plans-for-smart-city-projects/.

[6] Muir, Paul, "In Philippines, Smart Cities are on the horizon", *Asia Times*, 25 November 2019, Finance, https://asiatimes.com/2019/11/philippines-firm-aims-to-develop-smart-cities/.

[7] Government of India, Unique Identification Authority of India, "What is Aadhaar", https://uidai.gov.in/what-is-aadhaar.html.

[8] Marda, Vidushi, "Facial recognition is an invasive and inefficient tool", *The Hindu*, 27 July 2019, Opinion, https://www.thehindu.com/opinion/op-ed/facial-recognition-is-an-invasive-and-inefficient-tool/article28629051.ece.

[9] The third Myanmar Digital Rights Forum 2019, "*Summary Report*", https://www.myanmar-responsiblebusiness.org/pdf/2019-11-22-MDRF-Summary-Report.pdf.

In this essay, I will explore these questions in the context of South and Southeast Asia. In section II, I will provide an overview of the current landscape of technological adoption and regulatory developments in the region, with a focus on three prominent technical trends: smart cities, biometrics and AI. In section III, I will offer an analysis and reflect on promises and pitfalls emerging from the current landscape. Section IV will conclude with recommendations.

Landscape

Applications

The areas of focus for this essay, i.e., smart cities, biometrics and AI, were chosen due to enhanced government attention and funding in the last five years. Technically speaking, these are not three types of technology, but rather three areas of policy focus that technically overlap in significant ways. For instance, smart cities contemplate the use of biometrics and AI to function. Machine learning (the most popular subset of AI techniques) is used for applications like facial recognition which enable biometric authentication and identification.

Smart Cities

Broadly defined, smart cities contemplate the use of technology for government service delivery and functions. Singapore is considered a world leader in smart cities through its Smart Nation initiative. It envisions a nation where "[p]eople will be more empowered to live meaningful and fulfilling lives, enabled seamlessly by technology, offering exciting opportunities for all. It is where businesses can be more productive and seize new opportunities in the digital economy. It is a nation which collaborates with [its] international partners to deliver digital solutions and benefit people and business across boundaries."[10]

The assumption here is that the use of digital technologies will introduce efficiency and speed into traditional forms of governance, and this

[10] Government of Singapore, Smart Nation and Digital Government Office, "*Smart Nation: The Way Forward*", 18 November, Singapore, https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2.

is a narrative that is spoken widely in the region. ASEAN member states launched the ASEAN Smart Cities Network (ASCN) to identify digital solutions for organisations to deliver integrated public services and maximise job opportunities in 26 cities.[11] In Cambodia, Phnom Penh, Battambang and Siem Reap are working towards becoming smart cities under this network through cooperation on city planning and development between the private sectors and governments.[12] Malaysian states like Johor, Sabah and Sarawak are also a part of this initiative.[13]

Smart cities are essentially a suite of technologies that are meant to work in an integrated fashion. Take, for instance, India's Smart Cities Mission (SCM). The SCM is a flagship project of the government of India that looks to improve the quality of life in India through smart solutions while optimising economic growth.[14] The range of services under this includes e-governance solutions, crime monitoring, management solutions for energy, smart meters and waste management. Similarly, in Indonesia, an urban digitisation programme called "Gerakan Menuju 100 Smart Cities" is intended to be phased in over the course of a few years, and has three overarching goals: smart connectivity (infrastructure), smart solution (environment, governance, citizen, security, education, transport, healthcare); and smart users (community).[15]

Even though smart cities are largely conceptualised as being the next step towards modernisation of governance solutions, it is interesting to take into account the spaces and frameworks within which these solutions are pitched. In 2019, Thailand introduced the Eastern Economic Corridor to transform three Thai provinces into smart cities. This, and the concurrent plan to reach 100 smart cities by 2022 are in accordance with Thailand 4.0 – an *economic* model that is geared towards making Thailand a high-income

---

[11] Association of Southeast Asian Nations, *"Asean Health Sector Efforts On Covid-19"*, Asean.org, https://asean.org/asean/asean-smart-cities-network/.

[12] Kevin Livingston, "Smart Cities, a future in the making for Cambodia", CapitalCambodia, https://capitalcambodia.com/smart-cities-a-future-in-the-making-for-cambodia/.

[13] Tech Wire Asia, "Malaysia lays out plan for next state-level smart city projects", TECHWIREASIA, 24 February 2020, https://techwireasia.com/2020/02/malaysia-lays-out-plans-for-next-state-level-smart-city-project/.

[14] Government of India, Ministry of Housing and Urban Affairs, *"SMART CITIES MISSION"*, India.

[15] Anisa Herdiyanti, "Modelling the Smart Governance Performance to Support Smart City Program in Indonesia", 2019, https://www.sciencedirect.com/science/article/pii/S1877050919318459.

nation.[16] It would appear that while the substance of smart cities is generally aimed at improving the quality of life and governance, the form is determined by economic incentives. In Vietnam, the Industry 4.0 narrative has been persuasive as well, with Ho Chi Minh and Hanoi geared towards smart city development with the hope that "industry 4.0 will solve city-specific problems".[17]

Biometric identification

The use of biometric data for identification has also been on the rise across jurisdictions in the region. India is home to the largest biometric database in the world, Aadhaar. It was initially rolled out in 2010 as a voluntary system to introduce efficiency and reduce corruption in India's welfare system (although the stated intention behind the project has been altered and wordsmithed through the years).[18] In 2020, Aadhaar is a mandatory requirement for the receipt of government services and subsidies, for filing of income tax, etc[19]; even after its constitutionality was challenged – and upheld – in the Supreme Court of India in 2018.[20]

Thailand's Digital ID Bill was passed by the National Legislative Assembly in 2019, and envisions the use of biometrics along with Thailand's existing Smart ID Card.[21] The Thai government has also recently mandated the use of DERMALOG's Biometric Border Control Solutions to improve

---

16 Louis, Jillian, "Thailand Leading the way for Smart Cities in ASEAN", *The Asean Post*, 30 January 2020, Spotlight, https://theaseanpost.com/article/thailand-leading-way-smart-cities-asean.

17 Samaya Dharmaraj, "Vietnam's Plans For Smart City Projects", OpenGov, 18 October 2019, https://www.opengovasia.com/vietnams-plans-for-smart-city-projects/.

18 Ramakumar, R., "What The UID Conceals", *The Hindu*, 17 December 2016, Opinion, https://www.thehindu.com/opinion/lead/What-the-UID-conceals/article15786909.ece.

19 PTI, "Pan to become inoperative after March 31 if not linked with Aadhaar: Income Tax Department", *The Economic Times*, 15 February 2020, Wealth, https://economictimes.indiatimes.com/wealth/personal-finance-news/pan-to-become-inoperative-after-march-31-if-not-linked-with-aadhaar-i-t-dept/articleshow/74140366.cms?from=mdr.

20 Prasad, Malavika, "Aadhaar Verdict: SC's Majority judgment lacks consistency in logic and reasoning, turns constitutional analysis on its head", FirstPost, 29 September 2018, TECH2 INNOVATE, https://www.firstpost.com/india/aadhaar-verdict-scs-majority-judgment-lacks-consistency-in-logic-and-reasoning-turns-constitutional-analysis-on-its-head-5284941.html.

21 Alita Sharon, "Six digital bills passed in Thailand by NLA", OpenGov, 12 February 2019, https://www.opengovasia.com/six-digital-bills-passed-in-thailand-by-nla/.

border security[22], and in 2017, announced new methods for registration of SIM cards through biometrics to enhance safety and security.[23] Similar to the Thailand model, Myanmar is currently developing a national level plan that will require all individuals to submit their biometrics at the time of purchasing mobile phone services.[24] In Indonesia, trials of facial biometric authentication for social assistance subsidies recently concluded.[25]

In Singapore, the National Digital Identity (NDI) Programme (under the Smart Nation initiative) will take Singapore's current ID system, SingPass, one step forward by omitting the need for passwords and two-factor authentication for digital transactions involving sensitive data. The first step towards creating a centralised biometric scheme as part of NDI will start with facial recognition, where citizens will only register the biometric information under one centralised system.[26] According to Singapore's government technology agency, GovTech, the NDI will bring about a "seamless digital experience to citizens, and the efficiencies of digitalisation to businesses."[27] In Malaysia, the National Registration Department has announced plans to require biometric data to be integrated within marriage certificates and all identification documents; this is meant to improve security features.[28] The government of Bangladesh, on the other hand, has taken an unconventional approach. In partnership with Gavi, it has formed a public-private alliance that involves testing multiple biometric identification technologies for infants with the aim of ultimately building a biometric

---

[22] Karnjanatawe, Karnjana, "Immigration Biometrics", *Bangkok Post*, 16 May 2019, LIFE, https://www.bangkokpost.com/life/social-and-lifestyle/1678696/immigration-biometrics.

[23] Toomgum, Sirvish, "New SIM registration to require biometric ID starting Dec 15", *The Nation Thailand*, 6 November 2017, Corporate, https://www.nationthailand.com/Corporate/30330973.

[24] Chau, Thompson, "Myanmar wants mobile user biometrics", *Myanmar Times*, 5 December 2017, Business, https://www.mmtimes.com/news/myanmar-wants-mobile-user-biometrics.html.

[25] Tony Bitzionis, "Indonesia Government Assesses Facial Recognition System for Social Assistance Distribution", FIND BIOMETRICS, 25 May 2020, https://findbiometrics.com/indonesian-government-assesses-facial-recognition-system-social-assistance-distribution-052509/.

[26] Lago, Christina, "Singapore to use Facial Recognition in National Digital Identity System", CIO, 11 October 2018, Government IT, https://www.cio.com/article/3313337/singapore-to-use-facial-recognition-in-national-digital-identity-system.html.

[27] Lago, Christina, "Inside Singapore's National Digital Identity Programme", CIO, 16 August 2019, Vertical Industries, https://www.cio.com/article/3432144/inside-singapore-s-national-digital-identity-programme.html.

[28] Bernama, "Birth and Marriage certs to contain biometric data soon", FMT News, 9 February 2020, News, https://www.freemalaysiatoday.com/category/nation/2020/02/09/birth-and-marriage-certs-to-contain-biometric-data-soon/.

ID programme based on the success rates of these approaches.[29] In the Philippines, in a narrative strikingly similar to India, the rollout of a national biometric ID system is planned for the efficient delivery of social benefits and government services.[30] The central bank of the Philippines, BSP, plans to produce 23 million IDs in 2020.[31] In Pakistan, the narrative of national security and counter-terrorism has pushed the National Database and Registration Authority (NADRA) to build a centralised citizen database, including biometrics.[32]

Artificial Intelligence

Although AI has existed as a field of study in the realm of computer science for over six decades, it has gained prominence in the context of policy and governance in the last five years due to greater availability of data, more computing power and more cost-effective ways of scaling this technology. As countries around the world grapple with how to best use AI for economic growth and governance, significant investments and strategic plans surrounding this technology have emerged. AI is one of the most prominent technologies that will undergird applications within flagship projects such as smart cities, making the role of such systems more pervasive and also more important to fully understand.

In Singapore, the National AI Strategy Document focuses on deployment with the aim of using AI to transform Singapore's economy and "going beyond just adopting technology, to fundamentally re-thinking business models and making deep changes to reap productivity gains and create now areas of growth."[33] In addition to the overarching strategy, and state

---

[29] Alex Perala, "New ID2020 Project to Build Biometric ID Program Around Infant Immunization", FINDBIOMETRICS, 19 September 2019, https://findbiometrics.com/new-id2020-project-to-build-biometric-id-program-around-infant-immunization/.

[30] Mehedi Hassan, "Philippines Biometric National ID - What can we expect?", M2sys Blog, https://www.m2sys.com/blog/biometric-hardware/philippines-biometric-national-id/.

[31] Chipongian, Lee C., "BSP to print 23 million IDs next year", Manila Bulletin, 4 August 2019, Business News, https://business.mb.com.ph/2019/08/04/bsp-to-print-23-million-ids-next-year/.

[32] Malkani, Anum, "Identity Issues", Dawn, 6 January 2019, Archive, https://www.dawn.com/news/1455825.

[33] Singapore Government, Smart Nation and Digital Government Office, "National AI Strategy: The new key frontier of Singapore's Smart Nation Journey", Singapore, 20 April 2020, https://www.smartnation.gov.sg/why-Smart-Nation/NationalAIStrategy.

applications in public housing[34] and law enforcement,[35] Singapore has also seen sectoral approaches to AI, for instance, from the financial sector.[36] An industry-lead Advisory Council on the Ethical Use of AI and Data is meant to advise the government on issues that arise from the commercial deployment of AI.[37]

The Indian government has consistently allocated significant funding towards emerging technologies, with the focus on AI in the last few years,[38] and with parallel initiatives emerging in the last three years.[39] Notably, the National Institution for Transforming India (NITI Aayog), a government-run think tank, in its National Artificial Intelligence strategy states India's AI Vision to be one that will "leverage AI for economic growth, social developments and inclusive growth and finally as a 'garage' for emerging and developing economies."[40] In September 2019, NITI Aayog received approval for a Rs 7,500 crore project to set up an AI framework.

The Indonesian government, as part of its preparation towards Industrial Revolution 4.0, has indicated plans to develop an Artificial

---

[34] Housing & Development Board, *Success Story HDB: Optimizing Customer Service Through Intelligent Virtual Assistants*, Taiger, July 2018, http://old.taiger.aikenstaging.com/wp-content/uploads/2018/07/HDB-Success-Story-iConverse-Taiger.pdf.

[35] Them, Irene, "Using Artificial Intelligence to fight crime and terror", *The Strait Times*, 3 June 2017, Technology, https://www.straitstimes.com/singapore/using-artificial-intelligence-to-fight-crime-and-terror.

[36] JD Alios, "Monetary Authority of Singapore works with Financial sector on Framework for AI and Big Data", Crowdfund Insider, 13 November 2019, https://www.crowdfundinsider.com/2019/11/154061-monetary-authority-of-singapore-works-with-financial-sector-on-framework-for-ai-and-big-data/.

[37] Government of Singapore, Infocomm Media Development Authority, "Inaugural meeting of the Advisory Council on the Ethical use of Artificial Intelligence and Data", 6 May 2019, Singapore, https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2019/inaugural-meeting-of-the-advisory-council-on-the-ethical-use-of-artificial-intelligence-and-data.

[38] Thiagarajan, Sreeraman, "Budget 2020: India takes a leap of faith; makes a move towards adopting AI, ML and tech", Financial Express, 2 February 2020, Brandwagon, https://www.financialexpress.com/brandwagon/budget-2020-india-takes-a-leap-of-faith-makes-a-move-towards-adopting-ai-ml-and-tech/1852525/.

[39] Vidushi Marda, "Artificial Intelligence Policy in India: A Framework for Engaging the Limits for Data-Driven Decision Making", Philosophical Transactions A: Mathematical, Physical and Engineering Sciences (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240384.

[40] Government of India, NITI Aayog, "National Strategy For Artificial Intelligence #AIFORALL", June 2018, India, https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf.

Intelligence strategy in 2020.[41] Pakistan's approach to AI was likened to Industry 2.0 until recently, when the government allocated a substantial seed fund of 1.1 billion to propel AI skilling and research.[42] The need for an integrated national AI strategy remains.[43] The government of Thailand has been working closely with Microsoft and The Digital Economy and Society Ministry to establish an AI lab that will focus on Smart City projects, particularly looking at the farming sector.[44] The Bangladesh government has perhaps the widest departure from mainstream narratives around AI, with the IT Minister in 2018 explicitly stating concerns surrounding the use of Artificial Intelligence in the context of humanity and employment.[45] Elsewhere, a draft policy framework for the promotion of AI was published by the Sri Lanka Association of Software and Services Companies, and is intended to drive debate on and discuss the opportunities and challenges of AI in the Sri Lanka context.[46]

Regulation

The regulatory landscape of emerging technologies is a textured field, as there are a number of approaches to regulation that are advocated for. On one hand, the pitch for permissionless innovation is made in order to fully tap into the economic potential of emerging technologies and avoid the traps of overregulation. Another approach advocates for self-regulation

---

41 Nugraha, Ricky Mohammad, "Govt Eyes Artificial Intelligence Strategy Completion in 2020", Tempo.Co, 21 November 2019, Economy & Business, https://en.tempo.co/read/1274783/govt-eyes-artificial-intelligence-strategy-completion-in-2020.

42 Durrani Fakhar, "Govt Allocate Rs. 1.1 Billion for Artificial Intelligence Projects", *The News*, 19 April 2018, National, https://www.thenews.com.pk/print/306187-govt-allocates-rs1-1-billion-for-artificial-intellige.

43 Khaqan Ahmad, "Need for National Artificial Intelligence Strategy for Pakistan", Centre for Strategic and Contemporary Research, Issue No. 4 (2020), https://cscr.pk/pdf/perspectives/Need-for-National-AI-Strategy.pdf.

44 Alita Sharon, "Thailand Drafts Ethics Guidelines For AI", OpenGov, 4 November 2019, Augmented Intelligence, https://www.opengovasia.com/thailand-drafts-ethics-guidelines-for-ai/.

45 PTI, "Call to Regulate AI before it becomes a danger to humanity", *The Week*, 10 December 2018, Sci/Tech, https://www.theweek.in/news/sci-tech/2018/12/08/Call-to-regulate-AI-before-it-becomes-a-danger-to-humanity.html.

46 Biyagamage, Hiyal, "SLASSCOM launches Sri Lanka's first AI Policy framework", DailyFT, 27 June 2019, http://www.ft.lk/front-page/SLASSCOM-launches-Sri-Lanka-s-first-AI-policy-framework/44-680805.

by developers of technology to publicly indicate ethical standards and incentives. A third approach has been to advocate for state regulation.

Data protection forms the backbone of all the technologies discussed so far. Smart cities are built with technologies that include machine learning, biometrics, sensors and large-scale data analysis. Machine learning is the most popular subset of AI techniques that depend on the availability of data to train and learn from. Biometric technologies contemplate matching individual biometrics to large (often centralised) datasets for the purposes of authentication and identification.

Data is, thus, a fundamental, crucial and irreplaceable building block of the future of governance. Currently, data protection bills are pending in both India[47] and Indonesia.[48] In fact, data protection efforts in India, Indonesia and Thailand were activated after years of inaction, which was more than a coincidence. With the General Data Protection Regulation (GDPR) coming into effect in May 2018,[49] pressure had mounted on states in South and Southeast Asia to keep up with global trends and position themselves as jurisdictions for external investment and ease of business. Thailand's Personal Data Protection Act came into existence in May 2019,[50] and is strongly modelled along the lines of the GDPR. Singapore's approach to data protection has been articulated in terms of strengthening regional trade flows and digital businesses.[51] Its AI Strategy contemplates establishing frameworks for public-private data collaboration with the aim of free

---

[47] Phartiyal, Sankalp, "India's cabinet clears data protection bill for tabling in Parliament", *Reuters*, 4 December 2019, Technology, https://in.reuters.com/article/india-dataprotection/indias-cabinet-clears-data-protection-bill-for-tabling-in-parliament-idINKBN1Y8123.

[48] Damiana, Jessica, "Indonesia to step up Data Protection with new bill amid booming digital economy", *Reuters*, 28 January 2020, Asia, https://www.reuters.com/article/us-indonesia-data/indonesia-to-step-up-data-protection-with-new-bill-amid-booming-digital-economy-idUSKBN1ZR1NL.

[49] Matt Burgess, "What is GDPR? The summary guide to GDPR compliance in the UK", *Wired*, 24 March 2020, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[50] Graham Greenleaf and Arthit Suiryawongkul, "Thailand – Asia's Strong New Data Protection Law", 160 Privacy Laws and Business International Report (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3502671.

[51] Ying, Wong Siew, "Singapore must deepen global links, press on with open trade", *The Strait Times*, 10 February 2017, Business https://www.straitstimes.com/business/economy/singapore-must-deepen-global-links-press-on-with-open-trade.

sharing and use of data to spur innovation.[52] This sentiment is echoed in other jurisdictions as well. For instance, in the Philippines, the Data Privacy Act of 2012 was brought into force to "boost the country's competitiveness in the international information economy by providing a legal framework by which personal information shall be handled and transferred."[53]

Regional initiatives have mentioned data protection, including the SAARC Agreement on Trades and Services[54] and the ASEAN Economic Community Blueprint of 2025,[55] and also framed data protection as a trade and economic concern. While these can be positive developments for businesses that are looking for ease of data flows and data sharing, from a governance perspective, this creates unique challenges in terms of meaningfully accounting for context and the use of emerging technologies at the localised level. Regional data protection standards, thus, have a decidedly horizontal characteristic, i.e., they are predicated on ease of business instead of being rooted in a system of rights and individual benefits. Integrated data protection regulations do not exist in many jurisdictions like Indonesia, India, Cambodia, Vietnam, etc; many of which have taken enthusiastic steps towards the adoption of emerging technologies and smart city missions.

Current inconsistencies between data sharing and data localisation requirements in the region have also fractured integrated approaches to data protection. While cross-border data flows are a prominent driving force behind data protection reform, some countries like India, Vietnam and Indonesia have explicitly considered or enacted data localisation requirements. The tension between cross-border data flows and conceptions of digital sovereignty were perhaps most pronounced during recent negotiations of the Regional Comprehensive Economic Partnership (RCEP),

---

[52] Government of Singapore, Smart Nation and Digital Government Office, "National Artificial Intelligence Strategy", Singapore, November 2019, https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy-summary.pdf?sfvrsn=55179e0f_4.

[53] DR. Clarisse Girot, "Convergence of the Rules and Standards for cross border data transfers in Asia", Asian Business Law Institute, https://abli.asia/Projects/Data-Privacy-Project.

[54] SAARC Agreement on Trade in Services (SATIS), https://commerce.gov.in/writereaddata/trade/SAARC%20Agreement%20on%20Trade%20in%20Services%20SATS.pdf.

[55] Association of Southeast Asian Nations, "Asean Health Sector Efforts on COVID-19", https://asean.org/?static_post=asean-economic-community-blueprint-2025.

where India exited the trade agreement following disagreements surrounding cross-border data flows.[56]

Analysis

In this section, I will draw on the varied applications and regulatory frameworks discussed above to outline five important trends in the context of technology and governance.

1. **Prioritising the business case for governance:** The initiatives discussed in this essay are by and large intended for more efficient forms of governance, for the eradication of corruption, to reduce inefficiency, etc. The form and substance of how these initiatives will come to be deployed, however, are often decided in commercial contexts – either through the lens of Industry 4.0 or economic progress or commercial viability. For instance, in the Pune Smart City project, research has found that smart sanitation initiatives are driven by commercial bottom lines and not the purported aims of smart governance. The smart sanitation initiative within the Pune Smart City focuses on the business-use case and commercial viability of sanitation facilities, and does not reckon with the human rights baselines and constitutional considerations that states are traditionally required to take into account in the context of sanitation.[57] The prioritisation of economic progress and industrial growth is important – however, when this prioritisation is at the cost of government responsibilities, it must be re-examined. In many ways, it seems like the introduction of new technology involves outsourcing accountability for perceived efficiency and modernity.

2. **Structural dilution of state accountability:** The technologies described in this essay do not readily lend themselves to scrutability or

---

[56] Singh, Mallika, "RCEP pull-out: India stands by reduced trade deficits, data localisation, and enhancing domestic markets", Wion, 5 November 2019, https://www.wionews.com/india-news/rcep-pull-out-in-the-face-of-chinese-products-potentially-flooding-the-market-india-wants-to-reduce-deficits-and-keep-data-localisation-intact-260125.

[57] Malvika Prasad and Vidushi Marda, "Interrogating 'Smartness': A Case Study on the Caste and Gender Blind Spots of the Smart Sanitation Project in Pune, India", Association for Progressive Communications, Article 19, and Swedish International Development Cooperation Agency (SIDA), (2019), https://giswatch.org/sites/default/files/gisw2019_web_india_mal.pdf?fbclid=IwAR2yW6idX3KSkyIefaCLXINtPmDbv3B8LydsBval0cR5GdsaJ2pG6UDuuzI.

transparency.[58] This is either because the system itself is opaque, like complicated neural nets, or because the system's functioning is not made available for scrutiny, such as the various ways in which biometric databases are used and analysed in the absence of data protection safeguards. For instance, Myanmar's plans for biometric enrolment for SIM cards raise serious questions in respect of privacy and liberty as there is little visibility on how the database will be used and what purpose it is meant to serve.[59] The use of opaque technology for consequential decision making is made even more concerning when the entities deploying it, i.e., states in this case, are not equipped to understand or explain the systems themselves.

3. **Regulation by private actors:** While public-private partnerships for the provision of infrastructure is not a radical concept, in the case of emerging technologies, they present crucial challenges. Most of the deployments discussed in this essay are introduced on a pilot or trial basis, and eventually becoming cemented in the daily functioning of societies. At the stage of pilot testing, traditional forms of regulation, governance and deliberation are foregone to make way for innovation and modernisation. This essentially means that industry leads the conceptualisation, design, development and finally deployment of technologies that have a profound impact on governance, transparency, accountability and redressal. Here, it is also important to consider the ways in which deployments come to exist. Emerging technologies for smart cities, for instance, are sold to governments by companies who offer a suite of integrated products that are claimed to be helpful in governance. For instance, in Vietnam, the Smart Cities Project currently underway in Ho Chi Minh has been built in consultation with the Vietnam Posts and Telecommunications Group (VNPT) and Viettel Group.[60] Public-private partnerships also transcend jurisdictions. Limestone Network, a

---

[58] Vidushi Marda, "Machine Learning and Transparency: A Scoping Exercise", Article 19 Global Campaign for Free Expression, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3236837.

[59] "Myanmar: Dangerous Plans for Biometric SIM Card Registration Must Be Scrapped", Privacy International, 9 December 2019, ,https://privacyinternational.org/news-analysis/3303/myanmar-dangerous-plans-biometric-sim-card-registration-must-be-scrapped.

[60] Socialist Republic of Vietnam, Ministry of Information and Communications, "Smart city challenges Vietnam Gov't and localities", Vietnam, 18 October 2019, https://english.mic.gov.vn/Pages/TinTuc/139821/Smart-city-challenges-Vietnamese-Gov-t-and-localities.html.

Singaporean start-up, is planning to build a smart city in Phnom Penh, where the company will not only plan and build the smart city but also help in the day-to-day functioning of it through a Limestone app which will integrate government services for quick and efficient delivery.[61] The regulatory impact and extent of industry is therefore more complex and implicit than one may be led to believe at first glance.

4. **Priming for mission creep**: Many initiatives surrounding emerging technologies come into existence without a clear legal basis. In addition to the legal basis being unclear and/or non-existent, the surrounding regulatory framework in most jurisdictions does not address the fundamental issues presented by technologies. Aadhaar was introduced in 2010 without a legislative framework, and has demonstrated the perils and unfettered mission creep that follow hasty deployment.[62] In the absence of robust regulatory tools that necessitate narrowly defined use cases, the guardrails are heavily influenced by industrial action; either at the stage of selling particular products to governments, or while developing these technologies and determining capabilities, or at the time of deploying these technologies for various use cases.

5. **Visibility at the deployment stage**: Use cases for emerging technologies are usually made publicly known when governments unveil plans, budgets, priorities, pilots, or results from pilots. In other words, the use, form and extent of technology are usually made known to the public at the stage of deployment, or, at best, between the stages of conceptualisation and deployment. This means that actors like civil society are invited to the room much later than industry, severely jeopardising the opportunity for meaningful dialogue and pushback. This procedural opacity facilitates entrenchment of industry interests at

---

[61] Senase, Jose Rodriguez T., "Singaporean company plans to build smart city in Cambodia", *Khmer Times*, 19 August 2019, Business, https://www.khmertimeskh.com/634713/singaporean-company-plans-to-build-smart-city-in-cambodia/.

[62] Kritikaccg, "The Mission Creep behind the Aadhaar Project", The Centre for Communication Governance, 12 September 2016, https://ccgnludelhi.wordpress.com/2016/09/12/the-mission-creep-behind-the-aadhaar-project/.

the cost of constitutional rights and fundamental freedoms, as has been evidenced from experiences in India[63] and Myanmar,[64] among others.

Conclusion

The incremental value of technology in governance is immense, but current applications sidestep deliberation and nuance for speed and modernity. The analysis offered thus far has painted an intentionally critical picture of current deployments in order to take stock of crucial questions to ask in the future. To conclude this essay, I leave the reader with three recommendations for state deployment of privately developed technology going forward:

1. Converse often, early, and across stakeholder groups: Technology cannot be advocated for by a single stakeholder or discipline, if deployment is intended to be truly beneficial and impactful in society. Current trends point to overwhelming industry influence at the cost of civil society perspectives, often leading to a myopic view of governance and progress. A deliberative, iterative process of conceptualising and using technologies can have far reaching benefits for governance and governments.

2. Embrace the socio-technical nature of emerging technologies: It is crucial to remember that in matters of governance, technical systems have a decidedly socio-technical role to play, and actors deploying them must deeply reckon with the ways in which societies, individuals, and power structures are impacted by their use. Technology is not a silver bullet for complex social and human problems. Much of the narrative around technology is predicated on the massive potential and transformative impact these systems offer. There is little, if any, acknowledgement of the very real and demonstrated limitations of emerging technologies.

---

[63] Mandavia, Megha, "Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna", *The Economic Times*, 12 December 2019, Business, https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms.

[64] Nam Lwin, "Amid Int'l Espionage Concerns, Mandalay to Embrace Huawei for 'Safe City' Project", *The Irrawaddy*, 19 June 2019, https://www.irrawaddy.com/opinion/analysis/amid-intl-espionage-concerns-mandalay-embrace-huawei-safe-city-project.html.

3. Combine deployment with training: Technical systems need to be met with competence for meaningful deployment. While sophisticated technologies can introduce efficiency into governance processes, their use and procurement must be matched with individual and institutional capacity building and training in order to understand the role and extent of technologies.

Vidushi Marda is a lawyer and Senior Programme Officer at ARTICLE 19. She is also a non-resident research analyst at Carnegie India, Bangalore.

4

Digital Sovereignty: Data Governance in India

Trisha Ray

Introduction

"Let data roam free" is a common refrain heard the world over in response to governments putting up safeguards that address the powerlessness of users vis-à-vis data behemoths like Alphabet, Facebook and Tencent. This user-platform asymmetry is further complicated by global asymmetries, whereby developing countries' governments do not have access to their own citizens' data. Only a handful of countries are able to leverage their market size and/or robust institutions to offset these dynamics.

India's draft Personal Data Protection Bill (PDP Bill) is a bold piece of legislation animated by a clear theme: data sovereignty. Through the concept of "data fiduciary", the PDP Bill attempts to level a playing field that has till now seen the incommensurate influence of a handful of powerful technology giants. The PDP Bill also established and empowers a new agency to oversee compliance with the provisions of the Bill. However, the state itself is also a direct market player and a consumer of data; therefore, there is a clear conflict of interest when it comes to data regulation.

This essay will include three major components. The first is an outline of existing drivers, institutions, and regulations in India. The second component will explore the feasibility of "co-regulation" in the Indian context. The final portion will lay out recommendations applicable to states in South and Southeast Asia. The core question animating this essay is: can we strengthen state capacity on data governance in a way that empowers users and leverages the strengths of the private sector?

Drivers of Data Governance

Digital technologies are framed in Indian policymaking in terms of access, inclusion, and empowerment. They are a means for the government to provide essential services to its nearly 1.4 billion people, enabling them to participate in the country's economic growth. A Ministry of Electronics and Information Technology (MeitY) report dubbed this "India's Trillion Dollar Opportunity".[1] At the core of *Digital India* is the generation of value from data, whether this be in the form of better healthcare delivery or through the creation of open data portals, which enterprising individuals and homegrown firms can use to create digital applications.

The creation of digital governance tools like Aadhaar is one of the antecedents of the data protection debate in India. The groundwork for Aadhaar, a 12-digit unique ID, was laid by the Unique Identification Authority of India (UIDAI), a statutory body first chaired by prominent technocrat Nandan Nilekani. The objective of Aadhaar, according to the UIDAI website, is to "provide for good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services." Aadhaar is virtually compulsory for any individual wanting to access welfare schemes and a host of other government services.[2] From its inception, the Aadhaar project has sparked privacy and other fundamental rights concerns. Some cite its origin in the post-Kargil War proposition to create a "National Population Register" to stem the flow of "aliens and unauthorised people".[3] Others have pointed to the absence of informed consent and clear opt-out pathways, as well as the potential for mass-surveillance and the risk of data leakages.[4]

---

[1] "India's Trillion Dollar Opportunity", *Ministry of Electronics and Information Technology* (2018), https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

[2] Ibid. Aadhaar was also, in effect, mandatory for accessing private services like banking and mobile services until a September 2018 Supreme Court judgment struck down the relevant provision of the Aadhaar Act (Section 57). Ananya Bhattacharya and Nupur Anand, "Aadhaar is voluntary – but millions of Indians are already trapped", *Quartz*, 26 September 2019, https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/.

[3] R. Ramakumar, "What the UID Conceals", *The Hindu*, 21 October 2010, https://www.thehindu.com/opinion/lead/What-the-UID-conceals/article15786909.ece.

[4] Staff, "'Aadhaar Act is Unconstitutional': The Fiery Dissent of Justice D.Y. Chandrachud", *The Wire*, 26 September 2018, https://thewire.in/law/aadhaar-supreme-court-verdict-justice-chandrachud; Gautam Bhatia, "India's Growing Surveillance State", *Foreign Affairs*, 19 February 2020, https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state.

A second set of antecedents come from an election security standpoint. The *Cambridge Analytica* scandal in the US as well as allegations that Chinese apps like TikTok and Helo were being used to spread misinformation and harmful content during the 2019 Lok Sabha elections have generated distrust in technology giants' handling of personal data.[5] A 2019 survey by Youth Ki Awaaz identified misinformation and election manipulation as key concerns of young internet users in India.[6] The unchecked growth of social media platforms, facilitated by the wholesale exploitation of personal data, therefore animates the data protection discourse.

Finally, data governance is increasingly viewed as integral to national security. India's National Cybersecurity Strategy (NCSS) 2013 briefly stated that robust data protections will reduce economic costs incurred due to cybercrime and data theft.[7] The call for comments for the 2020 iteration of the Cybersecurity Strategy indicates that data governance will be a more prominent component of the new strategy:

> New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime, cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged. Further, existing structures may need to be revamped or revitalised. Thus, a need exists for the formulation of a National Cyber Security Strategy 2020.[8]

This broadened focus for NCSS 2020 also highlights how the national security case for data localisation is built on the argument that localisation requirements help bring the data of Indians under the aegis of Indian law. This can be viewed as an empowering measure, holding technology companies that are based overseas legally accountable for the misuse of personal data, and for the misuse of their platforms. The spread of fake

---

[5] Shreya Ganguly, "After TikTok, BJP Asks For A Ban On Chinese Social Media App Helo", *Inc42*, 5 April 2019, https://inc42.com/buzz/after-tiktok-bjp-asks-for-a-ban-on-chinese-app-helo/.

[6] "Youth Attitudes on the Future of the Internet", *Observer Research Foundation*, https://www.orfonline.org/youth-bytes/.

[7] National Cybersecurity Policy 2013, *Ministry of Electronic and Information Technology*, https://meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

[8] "NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020) Call for Comments", https://ncss2020.nic.in/.

news about kidnappings through WhatsApp, for instance, led to a series of lynchings which claimed over 30 lives, an incident with clear law enforcement implications.[9]

Data Protection Landscape: Key Institutions and Rules

The primary law governing cyberspace in India is the Information Technology Act (IT Act) 2008. The Act contains provisions that create penalties for unauthorised access to data [Section 43(a)], damage or alteration of data [Section 43(i)], failure to adequately protect personal data (Section 43A), and privacy violations (Section 66E).

In July 2017, the Government of India (GoI) set up a Committee of Experts on data protection, headed by Justice B.N. Srikrishna. Many of the recommendations of the Srikrishna Committee Report – including data localisation, the right to be forgotten and the concept of the "data fiduciary" – are reflected in the 2018 and 2019 drafts of the PDP Bill. Localisation provisions under Chapter VII of the Bill impose certain restrictions on the transfer of critical and sensitive personal data. The Bill also outlines obligations of privately owned data fiduciaries (Chapter II), including "specific, clear and lawful" purposes for processing personal data (Section 4), informed consent (Section 5a), limits on the retention of personal data (Section 9) and remedies to the data principal in case of a data breach (Section 25).

The PDP Bill proposes the establishment of the Data Protection Authority (DPA) to ensure compliance with the provisions of the Bill. The tools the Bill proposes are:

- Database of data fiduciaries: The DPA will create and maintain a database of data fiduciaries on its website.
- Data audits: The DPA will train and appoint data auditors who will evaluate a data fiduciary's compliance with the Bill.
- Data trust score: Maintain a database of data fiduciaries along with a "data trust score" that indicates compliance with the Bill.

---

[9] Mayank Mohanti, "WhatsApp Messages and the Mad Mob Lynching: A Timeline", *News18*, 11 March 2019, https://www.news18.com/news/india/whatsapp-messages-and-the-mad-mob-lynching-a-timeline-1798135.html.

- Monitoring: The DPA shall monitor cross-border flows of personal data, relevant technological developments and practices in this area.
- Guidelines: The DPA will issue codes of practice in keeping with the PDP Bill and promote general awareness regarding the protection of personal data.
- Advising: The DPA will advise central and state governments as well as other state authorities on enforcement and monitoring implementation.

The DPA joins a veritable cornucopia of existing government institutions in this ecosystem, with little clarity on how these bodies will interact. A brief overview of some of the relevant bodies is below:

1. National Critical Information Infrastructure Protection Centre (NCIIPC)

The NCIIPC was proposed under Section 70A in the IT Act and formally created via a Gazette of India notification in 2014.[10] The mission of the NCIIPC is "to facilitate protection of Critical Information Infrastructure (CII), from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction." The Centre recommends a number of "critical controls", which include guidelines on data storage, data loss prevention and data recovery. CII entities are not legally bound to follow the NCIIPC's recommendations on critical controls.

NCIIPC falls under the National Technical Research Organisation (NTRO), an agency under the National Security Council (NSC). The NSC is an executive body that advises the Prime Minister's Office on all matters of national security, and consists of relevant cabinet ministers, the vice-chair of NITI Aayog, the National Security Advisor (NSA) and the Deputy NSA. In 2014, the NSC floated an internal proposal that would mandate that all email service providers host their servers in India. The NSC also reportedly asked the Department of Telecom to explore the feasibility of asking all telecom and internet companies to route local data through the National

[10] Department of Electronics and Information Technology, Notification No. 9(16)/2004-EC, http://meity.gov.in/sites/upload_files/dit/files/S_O_18(E).pdf.

Internet Exchange of India.[11] As stated earlier, the NSC is also looking to update the National Cybersecurity Strategy, likely with a stronger focus on data governance. The NCIIPC primarily serves a national security function and is non-transparent by design.

2. Computer Emergency Response Team (CERT-In)

CERT-In was introduced in Section 70B of the IT Act and became operational in 2004. It is the national agency responsible for emergency response and crisis management, analysis, forecast and alerts on cyber security breaches. CERT-In, while growing, is severely understaffed, with less than 100 personnel.

3. Data Security Council of India (DSCI)

The DSCI is an industry body and policy advocacy group comprising over 500 companies across the banking, energy, IT, security, telecom and other sectors.[12] The DSCI organises consultations with parliamentarians, ministers and other key regulators on data protection, privacy and cybersecurity.

4. Telecom Disputes Settlement and Appellate Tribunal (TDSAT)

The IT Act (Section 48) created the Cyber Appellate Tribunal (CyAT), envisioned as the primary appellate body for disputes arising under the Act. In 2017, the CyAT was merged with the TDSAT, where it continues to be housed. The TDSAT has, however, not adjudicated on any cyber appeal or petition since the merger.[13]

---

[11] "National Security Council proposed 3-pringed plan to protect internet users", *The Hindu*, https://www.thehindubusinessline.com/info-tech/National-Security-Council-proposes-3-pronged-plan-to-protect-Internet-users/article20727012.ece#.

[12] Data Security Council of India, Member Directory (accessed 16 April 2020), https://www.dsci.in/member-directory/.

[13] Data from "Record of Proceedings", *Telecom Disputes Settlement and Appellate Tribunal* (accessed 20 April 2020), http://www.tdsat.gov.in/Delhi/services/record_of_proceeding.php.

Table 1: Overview of existing bodies in the data governance space.

Agency	Parent Body	Function	Budget 2019-2020 (INR)	Personnel
CERT-In	MeitY	Protect and monitor non-critical information infrastructure	420 million	95
NCIIPC	NSC	Protect and monitor critical information infrastructure	Classified	Unknown
TDSAT	Department of Telecommunications (DoT), Ministry of Communications	Adjudicate on legal conflicts arising out of IT Act	180.6 million	21 (Incl. administrative staff)

Enforcing Data Protection Regulations

I. The Paradox of Market Regulation Paradigms in Data Protection

India's data protection regulations are framed using traditional market regulation paradigms that view the state as an intermediary in the relationship between businesses and consumers. In this paradigm, governments create bodies and devise policies that grant privileges or curtail freedoms of businesses, thereby fostering economic growth while maximising social benefit.[14]

In the realm of data, this intermediary role, however, has an added dimension: the state itself is also a direct market player, albeit one that is playing catch-up. With businesses, consumers trade personal information in exchange for "better delivery" of goods and services. With governments, citizens forego their data in exchange for social protections and security. The PDP Bill reflects this inherent contradiction of data governance: the regulator is also the regulated.

Section 35 of the 2019 draft allows the Central Government to exempt any government agency from the provisions of the PDP Bill. In effect, all personal and critical data can be accessed by government agencies using

[14] Richard A. Posner, "Theories of Economic Regulation", NBER Working Paper No. 41 (May 1974); Nancy Rose and Paul Joskow, "The effects of economic regulation", Chapter 25 in Handbook of Industrial Organization, 1989, vol. 2, pp. 1449-1506.

a wide gamut of justifications, including "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, and public order". Furthermore, while many state agencies are data fiduciaries per the definitions in the PDP Bill, they are not legally accountable for any violations of data principal rights nor failures to adequately secure personal data. Many of the most critical breaches in the past couple of years have affected government agencies: in the first half of 2018, for instance, nearly a billion Aadhaar records were compromised, and in 2017, the data of 130 million Aadhaar card holders was publicly available on the internet.[15]

II. Emerging Narratives on Co-regulation

In light of the inherent issues with market regulation in the realm of data, namely that the state itself is a data fiduciary but will not be held to the same standards of transparency and accountability as private fiduciaries, there are growing calls amongst certain political leaders, industry and civil society organisations in India for a "co-regulation" model for data governance.

Co-regulation refers to a paradigm whereby the state and private actors collaborate in the implementation of regulations:

> Co-regulation entails explicit government involvement in the regulatory framework. It is generally considered that co-regulation involves government giving explicit legislative backing in some form for the regulatory arrangements. The specific types of instruments or mechanisms, such as codes of practices, voluntary agreements, dispute resolution procedures that may be created under a self-regulatory regime are similar under a co-regulatory framework. It is the degree of government involvement and legislative backing that determines the difference between the two.[16]

---

[15] Correspondent, "1 bn records compromised in Aadhaar breach since January: Gemalto", *The Hindu*, 15 October 2018, https://www.thehindubusinessline.com/news/1-bn-records-compromised-in-aadhaar-breach-since-january-gemalto/article25224758.ece; Amber Sinha and Srinivas Kodali, "Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information", *Centre for Internet and Society*, 1 May 2017, https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1.

[16] Glen Hepburn, "Alternatives to Traditional Regulation", *OECD* (2013), https://www.oecd.org/gov/regulatory-policy/42245468.pdf.

The rationale for co-regulation in data governance is two-fold: first, it addresses issues of government resource overstretch; second, it accommodates much-needed pushback against regulatory echo-chambers within the governance mechanism itself. Consultations held in the process of providing feedback to the Joint Parliamentary Committee on the 2019 PDP Bill have repeatedly produced recommendations along these lines. The Observer Research Foundation's submission highlights the steep operational, technical and human costs of data audits and analysis.[17] Stakeholders at digital news portal Medianama's closed session underlined that the DPA as it stands is functionally under the Central Government's "shadow", and suggested instead that the DPA would stand to benefit from a co-regulation model and was "ripe for setting the practice that regulators can come from the private sector".[18]

At the same time, the success of co-regulation is predicated on a number of conditions: transparency, the clear definition of objectives and benchmarks of success, as well as robust dispute resolutions mechanisms.[19] Effective co-regulation also requires a degree of alignment between government, private sector and the community. When such alignment is weak, a co-regulation mechanism would need to accommodate stakeholders from government, industry and civil society.

---

[17] ORF Technology and Media Initiative, "The Personal Data Protection Bill 2019: Recommendations to the Joint Parliamentary Committee," ORF Special Report No. 102, March 2020, Observer Research Foundation, https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/.

[18] "#NAMA INDIA'S DATA PROTECTION LAW – JANUARY 2020", *Medianama*, https://www.medianama.com/tag/nama-indias-data-protection-law-january-2020/.

[19] Glen Hepburn, "Alternatives to Traditional Regulation", *OECD* (2013).

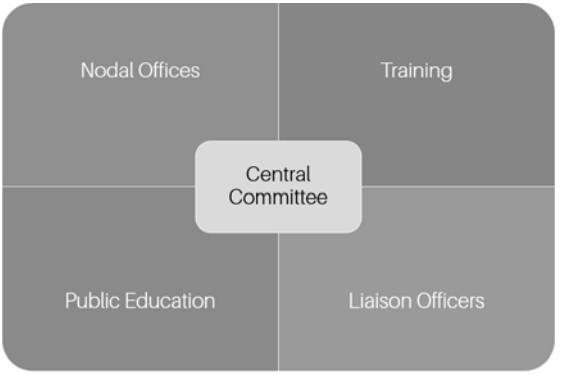
III. Envisioning a Co-Regulation Model for Data Governance

The proposed DPA, according to the 2019 draft of the PDP Bill, will consist of experts appointed by representatives from MeitY, the Department of Legal Affairs and the Cabinet Secretary; hence the above-mentioned critique of it being functionally a government agency even though the Bill states it is a body corporate.

A co-regulatory DPA (DPA 2.0) would help bridge a critical gap in the existing data regulation landscape: the need for a responsive, flexible, well-resourced agency to handle the full breadth of data protection enforcement. DPA 2.0 would consist of one central committee and a grid of offices that would supervise auditing, training, and public-facing functions.

The Central Committee would consist of experts – technical, legal, civil society and industry – with members nominated through relevant ministries and departments (MeitY, Legal Affairs, Cabinet Secretary), industry bodies like the DSCI, as well as academia or think tanks. The Chairman of the Committee will be elected through a vote by the Committee. As mentioned in the previous section, the success of co-regulation is predicated on transparency, clear objectives and parameters for success. The Committee would therefore need to set clear guidelines for data audits, data trust scores and other recommended data practices. Data auditors in the current version of the DPA would be public servants; however, DPA 2.0 could benefit from partnering with private sector auditing firms.

Fig 1: DPA 2.0 Structure



The Training wing would combine online and offline resources, providing flexible training options for DPA officers and partnering auditors on specific processes relating to the guidelines set by the Committee. The Public Education wing would deploy online means such as social media platforms and mobile applications as well as offline ones such as seminars, providing data principals with an accessible compendium of knowledge on their rights under the PDP Bill. Nodal officers trained under the DPA would collate reports from data auditors. Finally, DPA liaison officers would be placed with CERT-In, NCIIPC and other relevant agencies, facilitating inter-agency cooperation when necessary.

DPA 2.0 would be an ambitious project and would create an enforcement structure that is a lot more dynamic, responsive, and accountable than the purely government-led version laid out in the PDP Bill (2019). By incorporating private stakeholders into the data governance process, DPA 2.0 would leverage both civil society and private sector resources on the one hand, including a body of professionals who understand the legal and technical aspects of compliance, as well as government regulations that can be legally enforced.

However, DPA 2.0, and by extension any co-regulatory body modelled after it, will have to contend with several challenges, born out of overlapping functions, a legacy of exceptionalism on nebulous national security grounds and geopolitical asymmetries. The final section of this paper will lay out some of these challenges, many of which are in common with countries in South and Southeast Asia.

Challenges and Recommendations

Clarity on Overlaps in Data Governance Structures

The Indian data governance ecosystem at present consists of multiple state agencies, as well as potentially two sets of rules under the IT Act and the PDP Bill, with very little clarity on how they would interact. Sectoral regulations such as the Draft National E-Commerce Policy could further complicate this landscape.

Bureaucratic glut would be the death of any data protection body. The CyAT's fate is one such cautionary tale. CyAT was intended to create a quick pathway for adjudication on civil disputes under the IT Act. However, between 2006 and 2017, prior to its merger with TDSAT, CyAT received 87 appeals, of which it only cleared 17.[20] The merger with TDSAT, as mentioned in this paper, has not resulted in any significant improvement. Will the PDP Bill supersede all other existing data regulation rules? What would the pathways of cooperation between the DPA, CERT-In, NCIIPC and other relevant agencies look like? These are key questions that must be addressed in the next draft of the PDP Bill.

In Singapore, for instance, the interactions between various regulatory instruments have been laid out. The Personal Data Protection Act (PDPA) (2012) does not supersede existing sector-specific regulations.[21] Public agencies are governed by a separate set of regulations, including the Public Sector (Governance) Act, which cover data security, anonymisation and unauthorised disclosure.[22] The PDPA complements consumer data protections contained under the Banking Act (2008), the Telecommunications Act (2000), etc.

---

[20] Kundan Jha, "Body meant to resolve cases of cyber fraud near defunct", *Sunday Guardian Live*, 16 December 2017, https://www.sundayguardianlive.com/news/12014-body-meant-resolve-cases-cyber-fraud-near-defunct.

[21] Section 62, Personal Data Protection Act 2012, https://sso.agc.gov.sg/Act/PDPA2012.

[22] Lester Wong, "Parliament: Laws exist to hold public agencies accountable for data breaches", *Straits Times*, 6 May 2019, https://www.straitstimes.com/politics/parliament-laws-exist-to-hold-public-agencies-accountable-for-data-breaches.

Data Governance is Geopolitical

India's bid to fulfil the "trillion-dollar opportunity" of going digital, underpinned by robust data governance and a deep distrust of technology giants, is one shared by several nations in its extended neighbourhood. Sri Lanka, for instance, has drafted data protection regulations with this rationale.

> WHEREAS it has become necessary to facilitate the growth and innovation in the digital economy in Sri Lanka whilst safeguarding the rights of the individuals and ensuring the consumer trust.
>
> - Personal Data Protection Legislation, Sri Lanka (2020)

The trust deficit between governments and global technology giants like Google, Facebook or Tencent, which are primarily based in the US and China, means that data governance is as much a geopolitical issue as it is an economic one. For instance, global data protection regulations and the resultant threat to US dominance of the data economy led to US President Trump's statement at the 2019 G20 Summit, which emphasised the free flow of data.[23]

Co-regulatory data governance would have to contend with these geopolitical headwinds. Chinese tech giants, such as Alibaba Cloud and Tencent Cloud, have opened data centers in India, and others like ByteDance have announced that they will be doing so as well.[24] IBM, Microsoft, Google, AWS and Oracle are similarly vying for the Indian cloud services market by setting up data centres in the country.[25] The lucrative Indian market has served as a strong pull factor for technology giants' continued engage-

---

[23] "On Data Localisation, US President Donald Trump's Signal to India, China", *NDTV*, 28 June 2019, "https://www.ndtv.com/india-news/g20-summit-us-president-donald-trumps-signal-to-india-china-on-data-localisation-2060607.

[24] "Alibaba Cloud to Open Data Centers in India and Indonesia", *Alibaba Cloud*, 10 June 2017, https://www.alibabacloud.com/press-room/alibaba-cloud-to-open-data-centers-in-india-and-indonesia; "Tencent Cloud Global Infrastructure", *Tencent Cloud* (accessed 20 May 2020), https://intl.cloud.tencent.com/global-infrastructure; "Bytedance announces plans to establish India data centre", *TikTok India*, https://newsroom.tiktok.com/en-in/bytedance-announces-plans-to-establish-india-data-centre.

[25] Sanjay Gupta, "Why Google wants to set up a data centre in India", LiveMint, 14 October 2017, https://www.livemint.com/Technology/sUrnGVik4HYP0rGOtb6VuO/Why-Google-wants-to-set-up-a-data-centre-in-India.html.

ment with data governance, despite these companies' qualms about these regulations.

Table 2: Data Governance Legislation, Economic and Governance Indicators for Select Countries in SA and SEA (Source: World Bank).

Country Data	Protection Act/Bill	Signatory to a Regional Instrument	Internet Penetration % 2015	Internet Penetration % 2017-2018	GDP Rank (PPP)	Regulatory Quality SCORE[26]
BHUTAN	N[27]	N	39.8	48	155	-0.33
India	Y	N	17	51	3	-0.18
Indonesia	Y	Y	22	40	7	-0.07
Bangladesh	N[28]	N	14.4	15	33	-0.82
Malaysia	Y	Y	71	81	25	0.68
NEPAL	Y	N	17.58	34	92	-0.74
Philippines	Y	Y	36	60	27	0.04
Singapore	Y	Y	79	88	38	2.13
PAKISTAN	Y	N	14	15.51	23	-0.64
Sri Lanka	Y	N	12	34	58	-0.15
Thailand	Y	Y	39	57	19	0.11
Vietnam	N[29]	Y	45	70	32	-0.38

Where a country's market size is insufficient to drive engagement and compliance, it may pool together with other similar countries to create regional frameworks. The African Union's Convention of Cyber Security and Personal Data Protection and the ASEAN Framework on Personal Data Protection both aim to harmonise data governance in their respec-

[26] The World Bank's Regulatory Quality index "captures perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development". A higher score corresponds with more enabling regulations.

[27] Bhutan does not have a comprehensive data protection legislation; however, the Information Communication and Media Bill (2016) includes sections on user data protection.

[28] Bangladesh's Digital Security Act (2018) and ICT Act (2006) include elements of data security and privacy.

[29] Vietnam's Cybersecurity and Consumer Protection Acts include elements of privacy, localisation and data security.

tive regions. Both are voluntary but lay out useful guidelines for countries legislating on this issue.

In South Asia, where regional institutions are weak and often fractured, no such framework exists. Furthermore, aside from India, Nepal and Pakistan are the only two countries with draft or existing legislations expressly focused on data governance. In smaller countries with weaker regional institutions, the feasibility of co-regulation and strong data governance itself will need to be studied.

Conclusion

While India's ambitious PDP Bill elicited backlash from advocates of the free flow of data, it is a prudent piece of legislation that accounts for the global asymmetry of user data access and empowers the government and ordinary users vis-à-vis private technology giants. This paper proposed DPA 2.0, a co-regulatory body that leverages private sector capacities to build a robust, well-resourced body that can best carry out this ambitious set of regulations while also keeping in check an overstepping government. DPA 2.0 should learn from similar experiences in the region, including novel ways to manage the privacy and security question regarding government-collected data. It may also serve as a model for data governance that engaged with the private sector, civil society and a range of other stakeholders.

DPA 2.0 as a model will, however, need to be modified according to the unique contexts of countries in the region. Data governance lies at the intersection of economic growth, geopolitics and individual rights, with each country possessing differing strengths, regulatory capacities and engagement with key stakeholders in each area. In India, for instance, market size, regulatory capacity and active engagement with the domestic private sector in India (MeitY's data panel, for instance, is headed by the co-founder of one of India's biggest IT companies) have shaped its approach to governance.[30] Similarly, the drivers for data governance differ in each country as well, which in turn will shape the scope of legislation and the

[30] Neha Alawadhi, "Infosys co-founder Kris Gopalakrishnan to head govt's data panel", *Business Standard*, 14 September 2019, https://www.business-standard.com/article/companies/infosys-co-founder-kris-gopalakrishnan-to-head-govt-s-data-panel-119091400060_1.html.

kinds of instruments needed. However, clear objectives and milestones of success as well as transparency in functioning should remain as the driving principles across geographies.

Trisha Ray is a Junior Fellow with the Cyber Initiative at the Observer Research Foundation in India.

5

State Sovereignty in the Cyberspace and the Free Flow of Data

Smitha Krishna Prasad

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 cyberspace[3], 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

[1] "The Estonian Presidency of the UN Security Council Holds a Landmark Discussion on Cybersecurity", *Estonia in UN*, 21 May 2020, https://un.mfa.ee/the-estonian-presidency-of-the-un-security-council-holds-a-landmark-discussion-on-cybersecurity/.

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

[3] Resolution of the United Nations General Assembly, Right to Privacy in the Digital Age [A/RES/68/167]; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015 [A/70/174].

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 Rights[4].

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.

---

[4] "Universal Declaration of Human Rights", 10 December 1948, https://www.un.org/en/universal-declaration-human-rights/index.html; "International Covenant on Civil and Political Rights" (1976), https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

[5] "The Crisis of Social Media" (*Freedom House*), https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

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 data[6], 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 met[8]. Russia and China are considered to be at the other end of this spectrum, with varying requirements for localised data storage and processing[9].

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.

[7] William Alan Reinsch, "A Data Localization Free-for-All?", https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all.

[8] Article 45, General Data Protection Regulation (Regulation 2016/679) 2016 (OJ L).

[9] Dennis Broeders, Liisi Adamson and Rogier Creemers, "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace" [2019] The Hague Program For Cyber Norms Policy Brief, https://papers.ssrn.com/abstract=3493600.

measures.[10] 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"[11].

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

---

[10] Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam", https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/.

[11] Dr. Clarisse Girot, *Regulation of Cross-Border Transfers of Personal Data in Asia*, Asian Business Law Institute 2018.

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 locally[15].

- 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

---

[12] "Chinese Data Localization Law: Comprehensive but Ambiguous", *The Henry M. Jackson School of International Studies*, 7 February 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

[13] Sui-Lee Wee, "China's New Cybersecurity Law Leaves Foreign Firms Guessing", *The New York Times*, 31 May 2017, https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html.

[14] "Chinese Data Localization Law: Comprehensive but Ambiguous" (n 12).

[15] "Episode 10: Stricter Data Localisation and Security Rules for Financial and Insurance Data in China | Insights | DLA Piper Global Law Firm", *DLA Piper*, https://www.dlapiper.com/en/europe/insights/publications/2020/03/navigating-china-episode-10/; Samuel Yang, "China: Data Localisation", *Global Data Review*, https://globaldatareview.com/insight/handbook/2020/article/china-data-localisation.

[16] Draft Personal Data Protection Bill, 2018; Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, accessed 28 May 2019.

as the draft E-Commerce Policies of 2018 and 2019[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.[18]

In December 2019, the Personal Data Protection Bill, 2019[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 transfer of personal data outside of India, and places conditions based on which sensitive personal data may be transferred and processed outside 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 government.

- Indonesia

In Indonesia, data localisation requirements were applied in relation to any personal information collected and processed for the provision of public services.[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

---

[17] "Draft National E-Commerce Policy 2019", https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

[18] "Reserve Bank of India Directive on Storage of Payment System Data", 6 April 2018, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.

[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

---

[21] Agus Deradjat and Mahiswara Timur, "Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems", https://www.abnrlaw.com/news_detail.php?send_news_id=366&year=2019.

[22] Nadine Freischlad, "Indonesian IT Minister Says to Rethink Strict Data Localization Laws", *KrASIA*, https://kr-asia.com/indonesian-it-minister-says-to-rethink-strict-data-localization-laws.

[23] The Jakarta Post, "Government Does About-Face on Onshore Data Storage Plan", *The Jakarta Post*, https://www.thejakartapost.com/news/2019/09/16/government-does-about-face-on-onshore-data-storage-plan.html.

[24] "Vietnam to Enforce Cybersecurity Law despite Google, Facebook Pleas", *South China Morning Post*, 11 October 2018, https://www.scmp.com/news/asia/southeast-asia/article/2167999/vietnam-enforce-tough-new-cybersecurity-law-would-require.

[25] "Vietnam: Draft Decree on Cybersecurity Law 'Reduces Burden' of Localisation Requirements", *DataGuidance*, 8 November 2018, https://corporate.dataguidance.com/vietnam-draft-decree-on-cybersecurity-law-considerably-reduces-the-burden-on-companies/.

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

---

[26] "Data Localisation Requirements Narrowed in Vietnam's Cybersecurity Law", *The Business Times*, 15 October 2019, https://www.businesstimes.com.sg/asean-business/data-localisation-requirements-narrowed-in-vietnams-cybersecurity-law.

[27] Arindrajit Basu, Elonnai Hickok and Aditya Singh Chawla, "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India", 19 March 2019, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

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[28] 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.

---

[29] Madhulika Srikumar and others, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms", *Observer Research Foundation*, https://www.orfonline.org/research/india-us-data-sharing-for-law-enforcement-blueprint-for-reforms-47425/.

[30] Committee of Experts (n 16); Basu, Hickok and Singh Chawla (n 27).

[31] Smitha Krishna Prasad, Yesha Paul and Aditya Singh Chawla, "Centre for Communication Governance at National Law University Delhi, Comments-on the Draft Personal Data Protection Bill, 2018", https://ccgdelhi.org/wp-content/uploads/2018/10/CCG-NLU-Comments-on-the-PDP-Bill-2018-along-with-Comments-to-the-Srikrishna-Whitepaper.pdf.

[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.[33] In fact, many suggest that mandating local storage of data might in fact increase security risks.[34]

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[35], and India's proposed law[36], 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.

---

[33] Kritika Bhardwaj, "Data Localisation Must Go, It Damages the Global Internet", *Hindustan Times*, 3 August 2018, https://www.hindustantimes.com/analysis/data-localisation-must-go-it-damages-the-global-internet/story-Aah1052ExFq6Ylcb9BQ4jJ.html; Rishab Bailey and Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends", https://nipfp.org.in/publications/working-papers/1837/.

[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).

[39] See "Economic Survey of India" (2019).

[40] "Unpacking the Digital Economy Partnership Agreement (DEPA)", *Asian Trade Centre*, http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa.

interests that justify such a measure should be looked into in detail, and each addressed separately.[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[42] (OEWG), or Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security[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[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).

42 "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", https://www.un.org/disarmament/open-ended-working-group/.

43 "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", https://www.un.org/disarmament/group-of-governmental-experts/.

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.

6

From Self-Regulation to State Intervention: Shifting Modes of Social Media Regulation in Asia

Cleve V. Arguelles

Introduction

Social media is one of the most significant forces that are shaping contemporary Asia. Social media is a platform for the quick exchange of information among its users with contents ranging from photos and videos to files and texts. A community with more than two billion members and still growing, the centre of the world's social media activity is in Asia. Countries such as India, Indonesia, the Philippines, and Thailand continue to dominate the number of users of giant global social media communities, including Facebook, YouTube, and Instagram. Asians are at the forefront of innovating how social media is creatively used in different areas of everyday life: in communication, commerce, and even in politics. These innovations also include lessons on the potentials and drawbacks of emerging models of state-dominated regulation of social media.

As social media becomes indispensable to many Asian societies, the region is also rapidly forced to respond to its dark side. Philippines, a global social media capital, was famously the "patient zero" for how disinformation campaigns on Facebook and YouTube can be used to manipulate elections[1]. In India, the world's most populous democracy, religious extremists have discovered that WhatsApp can be used to coordinate successful violent

[1] Jonathan Corpus Ong and Jason Vincent A. Cabañes, "When Disinformation Studies Meets Production Studies: Social Identities and Moral Justifications in the Political Trolling Industry," *International Journal of Communication* 13 (2019): 5771-5790.

mob attacks against minority communities, especially in information-poor rural areas[2]. The list of the pernicious effects of social media's dark side is long. In response, governments have shifted their gaze to strengthening regulatory mechanisms around the use of social media. However, its ill effects on internet freedom is a cause to rethink this direction.

This chapter maps shifting modes of social media regulation in Asia. Asian societies are witnessing a worrying convergence towards a model of active state control of social media, its increasingly similar contours mirroring tightening government control of the entire internet architecture. Despite diverse socio-political contexts, many Asian states are turning away from models of platform self-regulation to active state policing of social media activity. This shift has grievously undermined internet freedom and human rights in the region. Three significant developments characterise the new regulation model. First, government capacities to censor, manipulate, and restrict social media activity have become increasingly sophisticated in recent years. Second, governments are also centralising material and organisational resources for social media monitoring through creation of top-level organisations with dedicated social media regulation responsibilities. And third, governments are also rapidly adopting punitive and criminal law sanctions to keep social media companies and users in their best behaviours. This chapter pays attention to how these regional developments are distinctly manifested on the ground especially in countries in South and Southeast Asia. The changing trends in social media regulation are most prominent in these two regions, where the world's highest concentration of social media activity coincides with the most state-dominated internet regimes in Asia.

The discussions in this chapter are organised in three sections. The first section traces the evolution of regulation models that have come to emerge since the success of internet penetration and first introduction of social media in many societies. From a field of open experimentation, the social media community proceeded to develop a culture of self-regulation. In the second section, this chapter discuss in detail the crisis confronting the self-regulation model. Disinformation campaigns and data privacy leaks are only some of the biggest challenges that have tested the limits of old approaches to social media regulation. The last section critically

---

[2] Rahul Mukherjee, "Mobile witnessing on WhatsApp: Vigilante virality and the anatomy of mob lynching," *South Asian Popular Culture* 18, no. 1 (2020): 79-101.

interrogates Asia's shift to active state policing of social media. The new model enabled state authorities in the region to impose significant constraints on the free and responsible use of social media. This worrying trend in social media regulation in Asia, coupled with the spectacular decline of internet freedom in the region, demonstrates an urgent need to develop alternative ways to govern social media that will ensure that platforms remain as open spaces for communication and innovation.

Beyond the Wild West: From Open Commons to Self-Regulation

Governments and social media communities have been playing cat and mouse for decades, as authorities try to regulate the use of social media in the region. Social media regulation shifted, over time, from an "open commons" approach in its early period to a multi-stakeholder "self-policing" model during its mainstreaming phase and then to an active "state intervention" approach at its present stage. This section briefly traces the shift from the first phase of "open commons" approach to the second phase of "self-policing" model.

As social media platforms were introduced to the region from the late 1990s to early 2000s, they were run and used by many as unregulated spaces for communication and creativity. Early social networking sites like Friendster and MySpace functioned as "open commons" with users and platforms free to experiment and test the boundaries of social media activity. For example, although Friendster was created as a dating site, it evolved into an entirely different virtual community. Its users found the space useful for a variety of purposes, including networking for personal and business purposes. This period is an exploration stage for both users and platforms, both simultaneously discovering new unintended uses of the sites and ways to run the community. State authorities paid little attention to social media platforms, many of them often guided by the idea that the "online world" is different and less significant than the "real world". At this stage, there is an extensive consensus among users, platforms, and governments that traditional means of regulation would not work when applied to internet activity[3].

---

[3] Ronald Deibert et al., eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge and London: MIT Press, 2011).

As social media became domesticated, from around the early 2000s until the end of the decade, problems have begun to mushroom left and right. Troubling social behaviours like bullying and trolling as well as criminal activities in the form of scams and identity theft have also taken root in social media spaces. Shifting from the laissez-faire approach of the previous years, the response from many governments is a partial involvement – an "arms-length relationship" with platforms and users – in regulating social media activities[4]. Popular social media platforms like Facebook and Twitter have introduced and enforced "community standards", set to guide its users to observe prevailing community norms and values in engaging others online. Users are warned that platforms may take down contents, and even profiles, that violate the set standards covering issues such as illegal drugs, pornography, sex work, violence, and other contents deemed to be hateful, harmful, and abusive. At this point, state authorities trust that platforms have an effective way of limiting prohibited contents and activities in their social media sites.

These developments reflect a model of self-policing, similar to how a free press operates in democracies, in which shared standards on what is harmful and dangerous are enforced by those who provide the social media service as a means of regulating community behaviour. Such rules usually draw upon prevailing broader social values and cultural norms about acceptable and unacceptable activities rather than, or only to a lesser extent, state-sponsored legal prohibitions and sanctions. Non-state third party actors, most notably civil society groups, also play occasionally decisive roles in shaping social media community standards. For instance, many social networking sites deem sexually obscene contents as inappropriate more as a result of being sensitive to both community norms and civil society campaigns to restrict access of minors and other vulnerable groups to pornographic materials rather than due to the dictates of formal state laws. The state, instead of being the only regulating authority, is considered one among many different stakeholders setting the parameters of appropriate social media contents and behaviours.

---

[4] Majid Yar, "A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media," *International Journal of Cybersecurity Intelligence and Cybercrime* 1, no. 1 (2018): 5-20.

Around the same time, a few countries like China and Saudi Arabia had already started exploring the active regulation of internet activity[5]. These states had introduced filters to restrict the access of their citizens to certain prohibited sites deemed offensive for political or religious reasons. The filtering technology, however, was still crude and sloppy at that time. Until governments invested extensive resources to develop the filtering regime much later, it was still an unreliable way of regulating the internet. For most states, the multi-stakeholder-led self-policing model has been adopted in one form or another in the hope that it will ensure a safe and thriving social media landscape.

The Social Media Party is Over: Self-Regulation Model in Crisis?

The success of the self-policing model, however, appeared to be short-lived. Due to the increasing number of societal challenges generally rooted to the misuse of social media, platforms faced extensive criticisms for their alleged failure to effectively police harmful actors and activities on their sites. This has led states and societies to reconsider the value of the model and to search for new approaches to regulating social media activity. This section features a concise discussion of the issues confronting the self-regulation model.

One of the biggest scandals to have dented the public's trust in the self-policing model is the rapid spread of disinformation in social media. For instance, elections in some of the biggest Asian democracies are under siege by disinformation in social media[6]. India's ruling Bharatiya Janata Party (BJP) has been revealed to have used WhatsApp to spread malicious rumours and false news against its political opponents to as many as 230 million Indian users of the platform[7]. WhatsApp has responded by limiting some of its features in India, but it has yet to meaningfully restrict the activities of partisan "cyberarmies" that have infiltrated many chat

---

[5] Ronald Deibart et al., "Access Contested."

[6] Allie Funk, "Asia's Elections Are Plagued by Online Disinformation," *Freedom House*, 2 May 2019, https://freedomhouse.org/article/asias-elections-are-plagued-online-disinformation.

[7] Snigdha Poonam and Samarth Bansal, "Misinformation Is Endangering India's Election," *The Atlantic*, 1 April 2019, https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/.

groups[8]. Aside from electoral interference, disinformation in social media has also facilitated violent attacks against many minority communities in the region[9]. For years, Facebook has failed to take down accounts and contents supporting the genocide of the Rohingya community in Myanmar, describing them as "dogs", "maggots", or "rapists" who "should be fed to pigs", "shot", or "exterminated"[10]. This, even months after a United Nations report had already identified the significant role played by hate speech on Facebook in the continuing violence against the Rohingyas[11]. Most recently too, we see how the thriving of medical misinformation in social media have also endangered the lives of many during the coronavirus pandemic[12]. In Indonesia, messages carrying a mixture of anti-Chinese sentiments and false medical claims went viral in Facebook[13]. Some of the falsehoods range from claims that garlic is a cure for the coronavirus disease to warnings that the virus is coming from mobile phones made in China. In response, Facebook and even Instagram have attempted to take down false contents regarding the virus in many countries but Facebook's algorithm has also removed thousands of news from mainstream sources[14]. The end result is that millions of site users could not access even trustworthy information regarding the pandemic for several days.

---

[8] Ibid.

[9] Brandon Paladino, "Democracy disconnected: Social media's caustic influence on Southeast Asia's fragile republics," *Brookings*, July 2018, https://www.brookings.edu/research/democracy-disconnected-social-medias-caustic-influence-on-southeast-asias-fragile-republics/.

[10] Steve Stecklow, "Why Facebook is losing the war on hate speech in Myanmar," *Reuters*, 15 August 2018, https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

[11] United Nations Human Rights Council, "Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar," 17 September 2018.

[12] Nuurianti Jalli, "Combating medical misinformation and disinformation amid coronavirus outbreak in Southeast Asia," *The Conversation*, 8 April 2020, https://theconversation.com/combating-medical-misinformation-and-disinformation-amid-coronavirus-outbreak-in-southeast-asia-131046.

[13] The Jakarta Post, "Coronavirus: Govt finds hoaxes on social media, amplified by news media for clickbait," *The Jakarta Post*, 4 February 2020, https://www.thejakartapost.com/news/2020/02/04/coronavirus-govt-finds-hoaxes-on-social-media-amplified-by-news-media-for-clickbait.html.

[14] Katie Paul, "Facebook bug causes legitimate coronavirus posts to be marked as spam: executive," *Reuters*, 18 March 2020, https://www.reuters.com/article/us-health-coronavirus-facebook/facebook-bug-causes-legitimate-coronavirus-posts-to-be-marked-as-spam-executive-idUSKBN21508L.

Social media manipulation through the use of disinformation campaigns is a global problem. But its effects are even more pernicious in many Asian societies where, for many people, one or two social media platforms is the internet. In many South and Southeast Asian countries like India, Pakistan, Myanmar, and the Philippines, Facebook is the internet as the platform offers free mobile internet in exchange for restrictions on access to sites other than Facebook. This service, called the "Free Basics", has been heavily criticised by civil society groups, especially because a user's inability to check other sites, including trusted news sources, heightens a user's exposure to the risks of misinformation on the platform[15].

This disinformation crisis raises significant questions on the long-term effectiveness and sustainability of the self-regulation model. Especially for those who argue for more government regulation, they have continuously criticised the model for its shortcomings on limiting harmful activities in social media. Many are doubtful whether the model can effectively handle proliferation of online crime and harassment and data privacy breaches, alongside the disinformation plague. It also does not help that platforms have been less transparent than needed in how they are effectively enforcing their community standards[16]. In the meantime, while the social media community are still exposed to unnecessary risks on their platforms on a daily basis, these platforms continue to earn billions and billions from the personal data generated by their community of users.

The model of voluntary content control, along with the state's "arms-length" relationship with platforms, is in crisis. The response from governments is a shift towards mandatory content restrictions, active state oversight of social media activities, and the use of punitive sanctions.

A Cure Far Worse than the Disease? From Self-Regulation to State Intervention

As a consequence of the social media crisis, Asian societies are witnessing governments shake off the self-regulation approach in exchange for a

---

[15] Global Voices, "Free Basics in Real Life," 27 July 2017, https://advox.globalvoices.org/wp-content/uploads/2017/08/FreeBasicsinRealLife_FINALJuly27.pdf.

[16] Ryan Baudish, "What Transparency Reports Don't Tell Us," *The Atlantic,* 19 December 2013, https://www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529/.

more assertive role for the state. The question is not whether social media should be regulated and to what extent, but rather what the most effective way for states to tighten control of social media is. This section discusses in detail the varied features that primarily characterise the shift to active state policing of social media in Asia. These developments, as this section also demonstrates, are moving in a direction that threatens internet freedom and human rights in the region.

Among the most important features of the shift is the increasing sophistication of state capacity to censor, manipulate, and restrict social media activity. In the past, technological options for governments were generally limited to crude website filters or blockers that were extremely prone to errors and comparably easier to circumvent. Now, states increasingly rely on a range of tools, including disinformation operations, computer network attacks and nuanced filtering technology, and even large-scale surveillance of platforms. The efforts of human regulators too are fast becoming complemented, if not replaced, by automated machine regulators that rely on programmed algorithms in removing content and accounts[17]. Governments are actively investing in cutting-edge technologies to regulate social media.

India and Pakistan, for instance, use a combination of filtering technology and disinformation campaigns to shape social media content accessible to their citizens. Both countries actively block thousands of websites that are deemed to be pornographic, religiously offensive, and threats to national security. However, contents that are critical of the ruling parties as well as those related to internet freedom are also occasionally subjected to filtering. Moreover, those accessing blocked websites are given an error page instead of a declaration that the government has blocked these sites[18]. This particular filtering strategy gives users the false impression that the sites are temporarily inaccessible because of irregular network problems instead of government filtering.

State authorities in India and Pakistan also extend these content filters to social media sites including Facebook and Instagram. The latest

---

[17] Adrian Shahbaz and Allie Funk, "Social Media Surveillance," *Freedom House*, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

[18] OpenNet Initiative, "India," 9 August 2012, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf; OpenNet Initiative, "Pakistan," 9 August 2012, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-pakistan.pdf.

Facebook Transparency Report indicates that both countries are among the world's most notorious in terms of content restrictions on Facebook and Instagram[19]. Although Pakistan's Telecommunication Authority restricts several thousand more contents than India's Ministry of Electronics and Information Technology, both countries restrict blasphemous, extremist, and separatist contents alongside critical commentaries on the judiciary, the parliament, and the rest of the government[20]. Aside from these tools, both governments have also been found to employ hundreds of human bots to manipulate social media conversations[21]. These bots are usually engaged to harass the media and civil society groups, influence foreign governments and international organisations, and even interfere in the politics of other countries.

Bangladesh too is a good example of this development. In the run-up to the 2019 national elections, hundreds of police teams were formed across the country to conduct active surveillance of social media[22]. A year before, the Bangladesh government had previously made public its Cyber Threat Detection and Response Project, which modernised the country's capacity to conduct mass surveillance of social media platforms through the installation of the latest monitoring equipment at the country's internet network[23]. With this technology, all social media traffic is monitored round-the-clock, which gives state authorities unlimited access to people's social media activities. The notorious Rapid Action Battalion, a paramilitary force accused of grave human rights violations, has also been

---

[19] Facebook, "Content Restrictions Based on Local Law," 2020, https://transparency.facebook.com/content-restrictions.

[20] Ibid.

[21] Saad Sayad, "Facebook removes accounts linked to Pakistani military employees", 1 April 2019, *Reuters*, https://uk.reuters.com/article/uk-facebook-accounts-pakistan/facebook-removes-accounts-linked-to-pakistani-military-employees-idUKKCN1RD1RM; Digital Rights Monitor, "DRM Investigates: Twitter Accounts Behind the Hashtag #ArrestsAntiPakJournalists," 5 July 2019, https://digitalrightsmonitor.pk/drm-investigates-twitter-accounts-behind-the-hashtag-arrestantipakjournalists/; EU Disinfo Lab, "Influencing policymakers with fake media outlets: An investigation into a pro-Indian influence network", December 2019, https://www.disinfo.eu/wp-content/uploads/2020/01/20191213_InfluencingPolicymakers-with-Fake-media-outlets.pdf.

[22] The Daily Star, "100 police teams active nationwide," 7 October 2018, *The Daily Star*, https://www.thedailystar.net/city/two-people-arrested-spreading-anti-state-rumours-on-youtube-channel-1643338.

[23] Rejaul Karim Bayron and Muhammad Zahidul Islam, "Cyber Threat Detection, Response: Govt installs tools for constant watch," 29 March 2017, *The Daily Star*, https://www.thedailystar.net/frontpage/govt-monitor-online-activities-1382893.

actively acquiring training and equipment for internet surveillance in the past years. Among others, this includes training for the "Location Based Social Network Monitoring System Software" in the US, another training programme for the "Backpack IMSI Catcher (2G, 3G, 4G)" in Russia, and the procurement of the "Wi-Fi Interceptor" from the Netherlands[24].

Aside from enhanced state capacity to regulate social media, another significant feature is the intensive efforts by governments to centralise material and organisational resources in controlling social media activity. Governments are rapidly setting up top-level national command centres solely focused on real-time regulation of social media. These institutions are sometimes under the jurisdiction of defence or military officials while at other times are led by executive authorities. Aside from being technologically enabled, these offices are similarly also given the power to impose registration, licensing, or identity requirements on internet service providers, internet cafes, and even social media users for the use of the internet. This allows the government to restrict social media activity even at just the initial point of accessing the internet network.

These developments are strongly reflected in Thailand. For years now, internet in the country has been consistently rated by Freedom House as "unfree"[25]. Thousands and thousands of websites are blocked in the country, the majority of which carry contents critical of the monarchy, the military, and the government[26]. Until recently, filtering decisions are made on an ad hoc basis, mostly through government requests to internet service providers. The centralisation efforts started with the setting up of a Ministry of Digital Economy and Society in 2016. Since then, the ministry has publicly unveiled a national "Anti-Fake News Centre". Although the official name suggests that they are focused on combating false news,

---

[24] Privacy International, "Updated – Amid Crackdown in Bangladesh, Government Forces Continue Spytech Shopping Spree," 14 August 2018, https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree.

[25] Freedom House, "Freedom on the Net 2019: Thailand", 2019, https://freedomhouse.org/country/thailand/freedom-net/2019.

[26] Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, "Situational Report on Control and Censorship of Online Media, through the Use of Laws and Imposition of Thai State Policies," *iLAW*, 9 December 2010.

their powers and responsibilities are actually broader[27]. Set up like a war room with its own dedicated staff, the centre is tasked to monitor trending conversations in social media, especially those that refer to government policies and contents that broadly touch on "peace and order, good morals, and national security"[28]. The centre pursues legal actions, including jail time, against individuals or groups they have identified to be behind the production or dissemination of prohibited contents in the country[29]. The ministry has also ordered internet cafes and even coffee shops with Wi-Fi services to keep a record of their customers' browsing activities and have them submitted regularly to the centre[30]. Prior to this, Thailand's Election Commission had also set up a "war room" with its own staff, tasked to monitor social media platforms for violations of campaign rules by parties and candidates[31]. In the 2019 general election, candidates and parties were also required by the commission to first register their social media profiles and contents with them prior to their use and dissemination[32]. In the near future, Thailand's government also aspires to establish a Cyber Defense Command Centre and a National Cybersecurity Agency and Hacking Training Centre, a new set of offices reflecting the country's quick move towards organisationally centralising regulation of social media contents[33].

In other historically closed societies like Myanmar and Vietnam, governments have also started establishing dedicated social media moni-

---

[27] Cristina Tardáguila, "'Obscene content' is 'fake news' in Thailand – and you can get arrested for spreading it", *Poynter*, 20 November 2019, https://www.poynter.org/fact-checking/2019/obscene-content-is-fake-news-in-thailand-and-you-can-get-arrested-for-spreading-it/.

[28] Patpicha Tanasempipat, "Thailand unveils 'anti-fake news' center to police the internet," *Reuters*, 1 November 2019, https://www.reuters.com/article/us-thailand-fakenews/thailand-unveils-anti-fake-news-center-to-police-the-internet-idUSKBN1XB48O.

[29] Tardáguila, "'Obscene content' is 'fake news' in Thailand".

[30] Bangkok Post, "Digital minister wants café customers' search histories," *Bangkok Post*, 8 October 2019, https://www.bangkokpost.com/tech/1767604/digital-minister-wants-cafe-customers-search-histories.

[31] Patpicha Tanakasempipat, "In Thai election, new 'war room' polices social media," *Reuters*, 18 March 2019, https://uk.reuters.com/article/uk-thailand-election-socialmedia/in-thai-election-new-war-room-polices-social-media-idUKKCN1QZ1DJ.

[32] Cleve Arguelles, et al., "The 2019 Thai General Election: A Missed Opportunity for Democracy," *Asian Network for Free Elections*, 2019, https://anfrel.org/anfrel-2019-thai-general-election-mission-report/.

[33] United Nations Institute for Disarmament Research, "Cyber Policy Portal: Thailand," April 2020, https://cyberpolicyportal.org/en/.

toring offices and teams[34]. However, due to the absence of transparency, these new programmes and their details are likely to be less known to the public. Nevertheless, there is evidence to show that a substantial part of the government budget is being redirected for social media regulation. For instance, Myanmar's Ministry of Transport and Communications has recently revealed that it spent almost five million US dollars in setting up a national government-led "social media monitoring team"[35]. Whether done in public or hidden from them, there is an outpouring of government resources to institutionalise state-led social media regulation.

The most significant and widely shared feature of the model shift is the rapid adoption by many states of punitive and criminal sanctions to compel the best behaviour from social media companies and users. Laws have been introduced to penalise the production and dissemination of certain contents in social media, including false, blasphemous, or obscene posts. Sanctions range from censorship and huge fines to several years behind bars, targeting users, platforms, and even internet service providers. While these legislations were often adopted under the guise of promoting public interest, they have also been frequently used to curb public dissent. The combination of advanced technological and organisational surveillance capacity and legal controls ensures that those using and operating social media are aware that the state is ever-present even in social media spaces: it is watching them, can shut them down, and is legally allowed to jail them – producing a chilling effect on speech online.

Singapore's recently adopted "Protection from Online Falsehoods and Manipulation Act" (POFMA) shows this particular direction. Under this law, government ministers can order social media platforms to remove contents or accounts deemed to be spreading falsehoods or require them to put a notice of correction alongside it[36]. Criminal sanctions, ranging from a fine of up to 700,000 USD for companies and up to 70,000 USD for users

---

[34] Freedom House, "Freedom on the Net 2019: Myanmar", 2019, https://freedomhouse.org/country/myanmar/freedom-net/2019; Freedom House, "Freedom on the Net 2019: Vietnam", 2019, https://freedomhouse.org/country/vietnam/freedom-net/2019.

[35] Zaw Zaw Htwe and Aung Kyaw Nyunt, "Critics rail against govt budget for monitoring of Facebook," *Myanmar Times*, 22 March 2018, https://www.mmtimes.com/news/critics-rail-against-govt-budget-monitoring-facebook.html.

[36] Tham Yuen-C, "Singapore's fake news law to come into effect Oct 2," *The Straits Times*, 1 October 2019, https://www.straitstimes.com/politics/fake-news-law-to-come-into-effect-oct-2.

to jail terms of 10 years for both, have also been imposed on violators[37]. POFMA's first use came weeks after, when the POFMA office directed an opposition politician to correct a Facebook post after he made critical comments about the government's relationship with the state investment firm Temasek[38]. In a subsequent case involving a foreign citizen outside the reach of Singapore's laws, the government instead ordered Facebook to add the label "it is legally required to tell you that the Singapore government says this post has false information" at the bottom of the post critical of the ruling People's Action Party[39]. In both cases, POFMA has been used against government critics. For many experts, the country seems to be moving in a direction in which state supervision in broadcast and print media is being extended to the realm of social media[40].

Even in countries like the Philippines where internet freedom is relatively better, similar legislations have also been used to target government critics amidst the global coronavirus pandemic[41]. Philippine President Rodrigo Duterte was given broad emergency powers to contain the virus, including the authority to impose a fine on and to jail individuals spreading "false information" related to the outbreak[42]. This is on top of the existing Anti Cybercrime Prevention Act which also penalises "unlawful" online contents. As the country was placed under one of the world's longest lockdown in early 2020, citizens flocked to social media to express their frustrations on the government's inadequate response to the outbreak

---

37 Ibid.

38 Channel News Asia, "POFMA Office directs Brad Bowyer to correct Facebook post in first use of 'fake news' law," 25 November 2019, https://www.channelnewsasia.com/news/singapore/brad-bowyer-facebook-post-falsehood-pofma-fake-news-12122952.

39 BBC, "Facebook bows to Singapore's 'fake news' law with post 'correction'," 30 November 2019, https://www.bbc.com/news/world-asia-50613341.

40 Cleve V. Arguelles and Jose Mari H. Lanuza, *Linking media systems and disinformation vulnerability: The case of Southeast Asia* (Manila: Consortium on Democracy and Disinformation, 2020), manuscript in preparation.

41 Carlos Conde, "Philippine Authorities Go After Media, Online Critics," *Human Rights Watch*, 6 April 2020, https://www.hrw.org/news/2020/04/06/philippine-authorities-go-after-media-online-critics.

42 Lian Buan, "Duterte's special powers bill punishes fake news by jail time, up to P1-M fine," *Rappler*, 24 March 2020, https://www.rappler.com/nation/255753-duterte-special-powers-bill-coronavirus-fines-fake-news.

as well as the selective enforcement of lockdown rules[43]. Using both laws, dozens have been arrested, including journalists, teachers, and volunteers, for Facebook posts that raised questions on the effectiveness of the government's strategies to curb the spread of the virus[44]. The same legislations were also used by the government to request the deportation of an overseas Filipino worker based in Taiwan for videos critical of Duterte that were posted on Facebook, but Taiwan's Ministry of Foreign Affairs rejected the deportation order[45]. Far from targeting groups responsible for disinformation campaigns, the laws are being used to silence government critics.

The developments we have discussed are classic examples of "mission creep"[46]. Governments usually justify enhancing state capacity and resources to monitor and manipulate social media activity through the need to modernise cyberwarfare capabilities. But this is a most dangerous slippery slope. Once this capacity is adopted for reasons of national security, or for whatever reasons of public interest, it is used easily for other politicised and partisan purposes[47].

Conclusion

The shift from platform self-regulation to an active state intervention model raises urgent concerns on internet freedom and human rights for citizens of Asia. The new mode of social media regulation that has emerged in the region will have far-reaching consequences for the free and responsible use of social media over many years to come. Once limited to states

---

[43] Sofia Tomacruz and Don Kevin Hapal, "Online outrage drowns out Duterte propaganda machine," *Rappler*, 24 April 2020, https://www.rappler.com/newsbreak/in-depth/258827-coronavirus-response-online-outrage-drowns-duterte-propaganda-machine.

[44] Reporters Without Borders, "Two Philippine journalists face two months in prison for coronavirus reporting," 2 April 2020, https://rsf.org/en/news/two-philippine-journalists-face-two-months-prison-coronavirus-reporting; Emmanuel Tupas and Edith Regalado, "Cyber cops arrest 32 for 'fake news'," *Philippine Star*, 7 April 2020, https://www.philstar.com/headlines/2020/04/07/2005988/cyber-cops-arrest-32-fake-news.

[45] Christia Marie Ramos, "Taiwan nixes PH bid to deport OFW over 'nasty' anti-Duterte remarks," *Philippine Daily Inquirer*, 28 April 2020, https://globalnation.inquirer.net/187296/taiwan-nixes-ph-bid-to-deport-ofw-over-nasty-anti-duterte-remarks.

[46] Majid Yar, "A Failure to Regulate?"

[47] Jonathan Corpus Ong and Ross Tapsell, "Mitigating Disinformation in Southeast Asia Elections: Lessons from Indonesia, Philippines and Thailand," *NATO StratCom Centre of Excellence*, 2020, https://www.stratcomcoe.org/mitigating-disinformation-southeast-asian-elections.

like China and North Korea, tight state control of social media and the rest of the internet has made its way to many countries in Asia. Most governments in the region are now legally, organisationally, and technologically empowered to monitor, censor, disrupt, and even criminalise social media activity in their countries. And with all these being done on a massive and centralised scale as a matter of course. Not surprisingly, the new model has been used to persecute opposition groups, independent press, government critics, and minority communities. Abandoning the self-regulation model due to its shortcomings, societies are in turn now confronting the limitations of the state intervention approach. As this chapter demonstrated, Asia's developing experiences with state-dominated social media spaces call for renewed caution and rethinking. An alternative means of social media regulation, one that successfully combines the benefits of previous models and avoids their risky consequences, is an urgent need in the region.

This need is most reflected in how more and more Asian citizens, especially the young, are discovering new ways to use social media to challenge state omnipotence in their everyday social media lives[48]. Young users are seeking messaging platforms that can ensure privacy and refuse government backdoor access through guaranteed encryption. Practices of ringfencing, or the use of closed groups or channels, as well as "Voldemorting", or deliberately misspelling keywords to confuse monitoring algorithms, are also becoming popular. Most importantly, a wave of new citizen groups in the region have been most active in demanding public transparency and civil society oversight on how both states and platforms are governing social media sites. It is these creative citizen responses that are keeping social media a vibrant and thriving space despite a restrictive regulatory environment.

At its heart, social media regulation is expected to involve restrictions on freedoms. However, in many democratic societies, the task of state actors is to find the right balance between keeping social media as spaces for freedom and creativity while also ensuring that the public is protected from unnecessary harm. Governments will necessarily play a crucial role here but its power to intervene and police social media must be coupled

---

[48] Cleve V. Arguelles, "青年是否正在虚度青春 ——作为菲律宾干禧一代新兴政治的数字公民 <Is youth really wasted on the young? Digital citizenship as an emerging politics of Filipino millennials>," *Refeng Xueshu* <热风学术网刊> 14 (2019): 47-62.

with democratic oversight of its use. One of the ways in which this can be done is to divide the enormous regulatory powers among independent and co-equal government agencies to minimise threats of abuse of power as well as political opportunism. For instance, regulatory responsibilities may be shared by security authorities, media and communication regulation bodies, and justice departments. Tech platforms will also play an equally crucial role to develop alternative ways of social media regulation. The more transparent, effective, and accountable social media companies are, the less justified reasons there will be for states to intervene. Involving a multi-stakeholder committee in developing company-level rules on content regulation in social media, composed of journalists, scholars, authorities, tech experts, human rights advocates, and other interested parties, is a step in this direction. If the challenge for governments is to resist the temptation of monopolising control over social media, the test for tech platforms is to control their tendencies to seek profit even at times when it is harmful to public interests. And both governments and tech platforms should take seriously the inputs of the community of social media users: they ultimately enjoy the benefits and suffer from the harms of models that over/under-regulate social media. The key to reconciling regulatory needs with principles of human rights and democracy is to pluralise formal sources of regulatory powers while mainstreaming shared informal norms of responsible use of social media.

Cleve Arguelles is a PhD Scholar at the Australian National University in Australia.

Rule of Law Programme Asia
Konrad Adenauer Stiftung

KONRAD
ADENAUER
STIFTUNG

ISBN 978-981-14-7125-4