KONRAD ADENAUER STIFTUNG

Regulating Data in India and Indonesia

A Comparative Study

Institute of South Asian Studies, National University of Singapore
Center for Digital Society, Universitas Gadjah Mada
Konrad Adenauer Stiftung, Rule of Law Programme Asia, Singapore

www.kas.de

Regulating Data in India and Indonesia

Regulating Data in India and Indonesia

A Comparative Study

Prepared by the Institute of South Asian Studies, National University of Singapore and Center for Digital Society, Universitas Gadjah Mada

for the Konrad Adenauer Stiftung, Rule of Law Programme Asia, Singapore.

March 2021

KONRAD ADENAUER STIFTUNG

CfDS CENTER FOR DIGITAL SOCIETY

NUS National University of Singapore | ISAS Institute of South Asian Studies

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

ISBN 978-981-18-0630-8

Image credits

Cover: binary image designed by starline / Freepik
Page 7: bank icon and money bag icon designed by Kreativkolors / Freepik
Page 7, 11, 33: internet icon and phone icon designed by rawpixel.com / Freepik
Page 35: click icon designed by rawpixel.com / Freepik
Page 36: shopping image designed by Katemangostar / Freepik
Page 79: multiple server image by Cskiran on Wikipedia

About Konrad Adenauer Stiftung (KAS)

The Konrad Adenauer Stiftung (KAS) is a political foundation of the Federal Republic of Germany, which has, for over 50 years, committed itself to the promotion of democracy and international cooperation. Founded in 1964, it was named after the first Chancellor of the Federal Republic of Germany, Konrad Adenauer. KAS offers political and social training activities, conducts research, grants scholarships to students, and supports and encourages international understanding and economic development. The Rule of Law Programme is a worldwide programme of KAS with regional offices in Asia, Europe, Latin America, Sub-Saharan Africa and Middle East/Northern Africa. The Rule of Law Programme Asia, based in Singapore, is dedicated to working with its Asian partners towards the development of rule of law in the region. It initiated its digitalisation programme to take stock of the regional developments regarding the emergence of new media and advanced technologies. One of the particular areas of focus is to explore the interplay between technology, society and the role of law.

Project Leads from KAS:

- Stefan Samse, Director, Rule of Law Programme Asia
- Aishwarya Natarajan, Programme Manager, Rule of Law Programme Asia

About Institute of South Asian Studies, National University of Singapore

The Institute of South Asian Studies (ISAS) was established in July 2004 as an autonomous research institute at the National University of Singapore (NUS). ISAS is dedicated to research on contemporary South Asia. The Institute seeks to promote understanding of this vital region of the world, and to communicate knowledge and insights about it to policy makers, the business community, academia and civil society, in Singapore and beyond.

Contributors from ISAS:

- Karthik Nachiappan
- Ronojoy Sen

About Center for Digital Society (CfDS), Universitas Gadjah Mada

Center for Digital Society (CfDS) is a research centre under the Faculty of Social and Political Sciences, University of Gadjah Mada. The institution was founded by the development and dynamics of contemporary socio-political life in the world, marked by the influence of the technological information. Thus, it requires a new approach to managing and understanding the phenomenon of digital society. Our research and activities are mainly supported by the leading mottos of productive, innovative, and influential.

Contributors from CfDS:

- Mulya Amri
- Dewa Ayu Diah Angendari
- Anisa Pratita Kirana Mantovani
- Janitra Haryanto
- Raka Wicaksana

Executive Summary

This policy report covers how India and Indonesia have sought to regulate data. Booming digital economies in both countries have created demands to develop legislative frameworks to regulate data – how data is collected, processed, stored, and shared. Rules governing data will significantly influence the development course and growth of India and Indonesia's digital economies. As hundreds of millions of citizens connect online, the governments of both countries will have to robustly manage how data, the mode through which users operate online, will be handled.

Politics around data regulations, however, have remained fitful in both countries. India has been hurtling toward creating a new policy framework and law to manage data, with differences around what data is, how organisations should handle it, and how the government should regulate this divide. So far, Indonesia has governed data through a patchwork of different sectoral regulations issued by separate agencies. This fragmented landscape could soon give way to a new, comprehensive law on personal data protection. Once operational, the remit and writ of legislations in both countries will likely be deep and so will the impact it will have on privacy and citizen's rights, the state's role in governing data, and digital innovation trends in India and Indonesia.

In both countries, draft legislations have been influenced by the European Union's General Data Protection Regulation (GDPR) framework, a user-centred data

protection approach imbued with notions of consent and accountability. These user-centric data governance ideas are balanced by a preference for a statist approach toward data regulation in both countries that underscores sovereignty at the expense of privacy. The critical challenge will be to see how new data laws in both countries will balance these two irreconcilable objectives.

Another key challenge concerns the implementation and enforcement of these data laws once enacted. Provisions call for a new regulator(s) to manage and oversee issues under the burgeoning data remit. But questions remain on the independence of the future data regulators and whether they will be able to exercise judgment and mediate conflicts, keeping in mind various public and private interests. There are also questions concerning coordination and capacity – will firms and public organisations have the necessary staff to manage queries concerning data and be responsible for compliance? Both countries will have to manage and overcome expected institutional deficits once their data legislations are enacted, and regulators created. Finally, the politics around data in both countries will complicate effective regulation and enforcement – privacy activists and related civil society organisations will likely pressure governments to enact strong laws that balance both privacy and accountability without sacrificing these priorities at the altar of state control.

Table of Contents

Introduction

India and Indonesia are two Asian powers that are also large, populous democracies and developing countries whose policies have sizable systemic effects. Both countries have dynamic economies with thriving digital firms populating their industrial landscape. Internet use and penetration are rising and driving innovation in India and Indonesia's digital sectors. Soon enough, both countries will have booming digital economies that will serve as critical sources of transnational investment and function as increasingly central parts of their economy as the pandemic restructures global economies around the digital. Despite thriving digital sectors and economies, India and Indonesia's digital future hinges on the laws adopted to regulate digital innovation and cross-border digital transactions. Rules that regulate cybersecurity and artificial intelligence hinge on the fundamental factor that fuels digital innovation and trade – data. How both countries regulate data will signal their intentions and priorities to external partners keen to invest in their economies and to domestic firms who require greater clarity when developing digital products and services for the global market.

This report records and reveals how India and Indonesia have sought to regulate data. Pressures driven by booming digital economies have compelled policymakers and regulators to devise a set of coherent and

comprehensive rules to collect, manage, store, and process personal data. Personal data refers to identifiable information individuals provide to various services and companies to communicate and engage in commerce online. The rise in internet usage, growing internet penetration, and increase in ownership of mobile platforms and devices have shattered data usage records in India and Indonesia. Hundreds of millions of people in both countries manage their lives online, providing bits and pieces of information on their daily lives to online services and companies for greater convenience and utility. The record increase in data use has not been met by domestic rules that effectively govern the conditions and restrictions these companies have to adhere to as they collect personal information.

Pressures to create a new data protection law in both countries vary. In India, the demand to create a new framework to manage personal data emanates from the right-to-privacy discussion, which arose from the government's investments towards creating a digital identity for all Indian citizens. New Delhi responded by entrusting the formulation of the new bill to an expert committee that judged data as being economically valuable enough to warrant being entirely stored within India, though some of these provisions have since been loosened. In Indonesia, demands to protect data resulted from several data breaches that led to firms compromising personal data. Security gaps have influenced the push for an overarching data protection law in Indonesia.

Existing regulations in both India and Indonesia fall short of expectations; this has also sensitised policymakers to review existing rules governing the collection and management of personal data. Sectoral laws dominate both jurisdictions, but their efficacy has been limited, mostly due to fragmentation in Indonesia and deficient enforcement in India. The impetus to create new data protection frameworks has been driven by the urgent need to upgrade and supersede existing rules governing data. International considerations also intervened here. The European Union's General Data Protection Regulation (GDPR) framework has served as

a lodestar for the drafters of data legislations in New Delhi and Jakarta. Without clear global rules on data, the GDPR has been relied on during the drafting of certain aspects of both draft bills. Privacy features heavily, and so does personal consent that firms collecting data have to respect. The rights of users found sway in both legislations.

That said, there was heavy emphasis on protecting data to assist state purposes, an important factor which manifested itself in the guise of "data sovereignty" or data that also belonged to the state. Going ahead, impulses that protect individual users' privacy and rights will have to be balanced with state interests that are aligned toward amassing data for public use. Balancing public and private needs – the interests of the state and those of users – as well as the priorities of domestic and foreign tech firms will be difficult for India and Indonesia. Both countries strive to enact a data protection law to govern personal data. These political burdens will have to be borne by institutions to regulate data that are yet to be either created (India) or sanctioned (Indonesia). Institutional challenges may yet mar the implementation of these two legislations once they have received consent.

This report describes and analyses how India and Indonesia have attempted to regulate data, focusing on the political and institutional factors and actors. The first section unpacks India's efforts to regulate data, focusing on the Personal Data Protection (PDP) Bill that was drafted by a select committee in July 2018 and thereafter revised. The second section focuses on Indonesia's efforts, and, likewise, covers the range of regulations and pressures that have led to discussions around Indonesia's new data protection law. The third section compares and contrasts both countries' experiences, drawing out some broad takeaways vis-à-vis the regulation of data in Asia. The conclusion delineates some of the challenges and opportunities that lie ahead for both countries along this pathway.

India – Regulating Data

Introduction

Since February 2019, when the government of India unveiled its National E-Commerce Policy, which placed considerable importance on data, even going so far as to regard it as a national resource unlike any other, discussions concerning the regulation of data have progressed. Data is now commonly referred to as the new "oil" in India, with political and business leaders calling for data to be placed under sovereign control to power India's development. Such statements are being made by Indian officials abroad and within parliamentary committees, as well as being reflected in rules that seek to govern different aspects of data domestically, most notably the draft Personal Data Protection Bill 2018 and 2019.

The past couple of years have seen several policy interventions on data governance by various Indian government ministries and departments. While connected by the shared "data sovereignty" vision and the need to use data to pursue development and empower vulnerable communities, there appear to be several inconsistencies and loopholes in these policies.

The first significant policy move on data localisation started with a notification from the Reserve Bank of India (RBI) in April 2018, compelling the storage and processing of all payments data in India. WhatsApp, Google Pay, MasterCard and several foreign companies

prioritised compliance with this directive to retain their position in India's burgeoning payments sector. The RBI directive was followed by several notifications mandating various forms of data localisation across multiple industries, including healthcare, e-commerce, and insurance. The most sweeping of these rules was a draft of the August 2018 Personal Data Protection Bill. The draft bill contained a mirroring provision, which mandated that a copy of all personal data be stored in India. It also had a provision restricting cross-border transfers for all data that the government designates as "critical personal data."

While the Srikrishna Committee, which authored the first data protection bill, specified a number of reasons justifying this measure in its accompanying report, two, in particular, stood out. First is the long-winded process that Indian law enforcement agencies must go through to access data stored within foreign jurisdictions. Indian authorities have recognised this issue as a significant hindrance to carrying out criminal investigations. Second, data localisation could enable Indian companies to use data-driven decision-making tools to access and use data for their economic benefit. That said, there is more to the process of regulating India's data that needs to be accounted for.

This section will aim to provide the context around discussions to legislate and regulate data in India, underline key actors and their conceptualisations of data, and examine how these preferences and perceptions have influenced India's personal data protection bill(s).

India's Digital Economy

The Indian government has driven India's digital transformation. New Delhi is the custodian and manager of Aadhaar, India's flagship biometric digital identity programme, which has enrolled 1.2 billion Indian citizens. India remains the only country that has provided a biometric-based digitally verifiable identity to most of its adult population; this identity has allowed citi-

zens to engage with and participate in a thriving digital economy. With secure, verified identification, Indian citizens can undertake transactions without additional supporting documents. In a recent judgment, the Indian Supreme Court exalted Aadhaar's significance as a pivotal "symbol of India's digital economy" that has unleashed multiple avenues for personal and commercial interactions.

Aadhaar has emerged as a critical instrument that the government deploys to disburse subsidies and benefits by cutting out the human interface. With the Aadhaar Act, the Indian government has institutionalised the digital transfer of subsidies, ensuring Indian citizens are not deprived of their entitlements. Aadhaar has become a key component of several critical welfare programmes, including the Mahatma Gandhi National Rural Employment Guarantee Act (MNREGA) that provides public employment and the Public Distribution System (PDS).

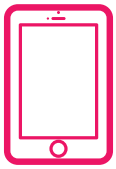
The Modi government has used Aadhaar to promote financial inclusion through the Jan Dhan Yojana programme that creates bank accounts for Indian citizens. From 2014 to 2018, around 500 million bank accounts were linked to Aadhaar, allowing the government to transfer welfare payments directly.[1] The government has boosted financial access through the Jan Dhan programme (JAM), as a result of which 85% of Indian citizens have bank accounts. These bank accounts, together with the 1.2 billion-strong Aadhaar database, 1.1 billion mobile phone users, and 600 million internet users extend financial access to unbanked Indians. Tying bank accounts to Aadhaar through robust verification standards allows government officials to root out nefarious activities like money laundering and terrorist financing.

[1] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

500
million bank accounts were linked to Aadhaar (2014-2018)

85%
of Indian citizens now have bank accounts

600
million internet users



1.1
billion mobile phone users

The institution of a goods and services tax (GST) has streamlined business tax payments, bringing all transactions onto a single digital platform. The government got more than 10 million businesses onto the platform, and the initiatives still act as a driving force for companies to move their operations online.[2] The Indian government has also established an e-marketplace where big and small firms can vie for government contracts and where the government can procure their services. Forty-two percent of transactions in this marketplace involve small and medium-sized enterprises, and efforts are ongoing to bring in more start-ups, small-scale producers, and other market actors. The portal was designed to eliminate human interface, which could privilege or bias certain actors over others, while increasing coverage and access.

New Delhi has furthered digitalisation by rolling out initiatives to encourage the adoption of digital tools and platforms. The Digital India initiative, introduced in 2015, aims to bridge and redress digital gaps in soci-

[2] Ibid.

ety and transform India's economy into a knowledge economy that is digitally empowered.[3] Digital India involves three main components – creating accessible digital infrastructures, providing services digitally, and promoting digital literacy amongst citizens.[4] By 2025, this initiative is expected to contribute between USD550 billion to USD1 trillion to India's GDP.[5]

Public investments on the digital front have crowded in private investments to spawn a thriving digital economy. The value of India's core digital sectors, like information technology (IT), communication services, and electronics manufacturing, was roughly 7% of India's GDP in 2017-2018 or nearly USD200 billion.[6] By 2025, these core sectors' potential value is estimated to be USD435 billion, twice its current value.[7] While previously not considered a part of India's digital economy, sectors like agriculture, education, financial services, healthcare, and retail are becoming a part of the digital economy as they slowly digitise.[8]

Despite these policies and strides taken, uneven patterns of digitisation exist across sectors. Sectors like information and communications technology (ICT), professional services, and healthcare, with more digitised firms, are represented in the bottom quartile of digital adoption. At the same time, some top-quartile companies hail from sectors like transportation and con-

[3] MEITY, "India's Trillion-Dollar Digital Opportunity", 2019, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.

[4] Onkar Singh, "Digital India: Unleashing Prosperity", *International Journal of Advanced Research in Computer Science* 7, 2016, http://libproxy1.nus.edu.sg/login?url=https://search-proquest-com.libproxy1.nus.edu.sg/docview/1860624209?accountid=13876.

[5] Prerna Sharma, "Regulating A Digital Economy: An Indian Perspective", *Brookings*, 2018, https://www.brookings.edu/blog/up-front/2018/04/25/regulating-a-digital-economy-an-indian-perspective/.

[6] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[7] Ibid.

[8] Ibid.

struction.[9] Gaps between small and large firms could be bridged as small companies are faster in adopting digital payment technologies, social media, and video conferencing systems. The rapid pace of digitisation has also allowed lower-income states to grow faster than higher-income states when it comes to internet subscriptions.[10] Between 2014 and 2018, seven of the ten states with the highest growth rates of internet subscriptions had a lower per capita GDP than the national average.[11] That said, the Indian digital economy's growth trajectory has not reached its peak yet, as nearly 90% of retail transactions are still cash-based, and less than half of the population have internet subscriptions.[12]

Some key players, like Airtel, Reliance Jio, Vodafone, and Idea, have adopted attractive pricing strategies to incentivise Indian customers to purchase their products and technologies in the telecom sector.[13] The drastic drop in mobile data prices has also allowed these telecom companies to cut prices and expand their customer base.[14] Being the fastest growing digital economy globally, India has become extremely attractive for global technology titans; there has been a rise in partnerships between Indian firms and global technology titans, like the Jio-Facebook collaboration and the most recent Jio-Google partnership.[15]

---

[9] Ibid.

[10] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[11] MEITY, "India's Trillion-Dollar Digital Opportunity", 2019, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.

[12] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[13] MEITY, "India's Trillion-Dollar Digital Opportunity", 2019, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.

[14] Ibid.

[15] Bloomberg quint, "Why Jio-Facebook May Work Better Than A Google Or Amazon Combination", 2020, https://www.bloombergquint.com/business/why-jio-facebook-may-work-better-than-a-google-or-amazon-combination.

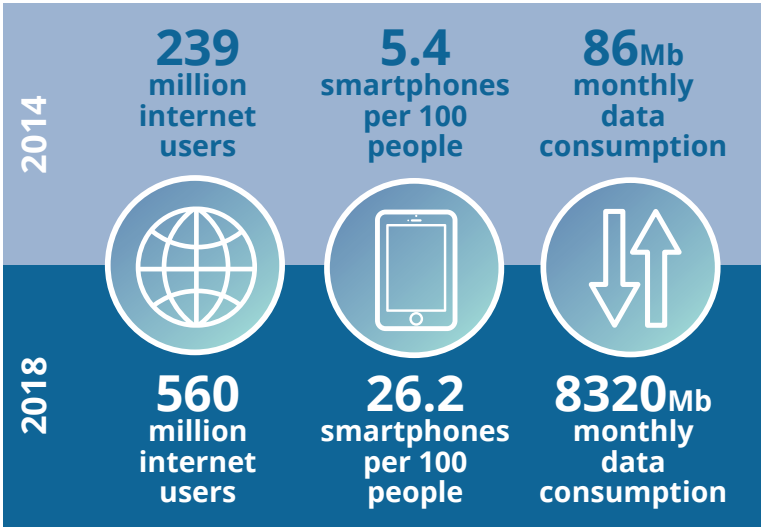
Though India's digital economy placed last amongst 17 major advanced digital economies in terms of digital adoption, India ranked second in digital adoption growth, at 90% since 2014.[16] The emergence of a thriving digital economy can be attributed to sustained investments made over the past two decades concerning ICTs that have incentivised telecom companies to invest, further encouraged by rapid digitisation and a growing number of citizens using digital tools in daily activities. The rapid growth of India's digital economy has compelled global tech firms to deepen their commitment to India individually and through domestic partners. Competition between domestic and foreign tech firms also centre on the key input driving India's digital transformation – data.

Data

Rapid digitalisation has had a cascading effect on the input or unit of production driving digital interactions – data. Booming rates of internet usage and digital penetration have resulted in the plummeting of the cost of data while increasing its use. India is the world's fastest-growing market for digital consumers and is the second-largest market for internet subscriptions and instant messaging service users globally.[17] In just four years, between 2014 and 2018, data usage increased exponentially. In 2014, there were 239 million internet users, 5.4 smartphones per 100 people, and monthly data consumption per connection of 86Mb. By 2018, all of these figures had risen exponentially – there were 560 million internet users, 26.2 smartphones per 100

[16] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[17] MEITY, "India's Trillion-Dollar Digital Opportunity", 2019, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.



people, and the monthly consumption of data had grown a hundredfold to reach an average of 8320Mb.[18]

On average, in 2018, Indian mobile users consumed 8.3GB of data monthly, compared with a consumption rate of 5.5GB in China, and 8 to 8.5GB in advanced digital economies.[19] Monthly consumption rose to 12GB in 2019, with estimates that this number will increase to 25GB by 2025.[20] This recent spike is attributed mainly to another dip in data pricing. In 2014, the monthly price of data (per 1Gb as a percentage of monthly GDP) was 6.1%, and these prices fell to 0.1% by 2018,[21] following a massive disruption caused by Reliance Jio's entry into

[18] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[19] MEITY, "India's Trillion-Dollar Digital Opportunity", 2019, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.

[20] "India's data consumption may touch 25 G.B. per month per user by 2025: Ericsson", *PTI News,* 16 June 2020, http://www.ptinews.com/news/11567036_India--s-data-consumption-may-touch-25-GB-month-per-user-by-2025--Ericsson.

[21] Ibid.

the market in 2016.[22] Other factors driving this increase in data consumption include affordable smartphones, which increased the number of mobile internet users, particularly in rural areas; and how Indian citizens consume media and culture, which has become more video-oriented, thereby increasing data use.[23] India's growth in data consumption has yet to reach its peak – monthly mobile data consumption per person is growing at a rate of 152% every year.[24]

With growing data usage come concerns over the loss of individual privacy as users concede personal information to telecom companies, platforms, and various services as they engage online. In a UNCTAD (United Nations Conference on Trade and Development) report, 90% of India's internet users expressed privacy concerns.[25] Privacy concerns over how data is collected, stored, and used have compelled the Indian government to regulate data through legislation. One critical component would involve the government and a range of actors sorting out what they perceive as data and how it should be managed given competing interests, including the need to control data to further economic potentials in a thriving digital economy.

[22] Krishnan, Varun B., "How much mobile data do Indians use in a month?", *The Hindu,* 26 August 2019, https://www.thehindu.com/news/national/indian-mobile-data-usage-over-7-gb-per-month/article29259546.ece.

[23] "India's data consumption may touch 25 G.B. per month per user by 2025: Ericsson", *PTI News,* 16 June 2020. http://www.ptinews.com/news/11567036_India--s-data-consumption-may-touch-25-GB-month-per-user-by-2025--Ericsson.

[24] McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation" (repr., McKinsey & Company, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[25] UNCTAD, *Digital Economy Report 2019, Value Creation and Capture: Implications for Developing Countries.* United Nations, 2019.

Conceptualising Data

The stratospheric use of data and concerns over how it will be managed, controlled, and monetised has meant that perceptions of India's personal data often vary depending on who you ask and their respective interests. With the rise of a "data" economy, citizens are increasingly using personal devices to transact and communicate with different entities, thereby raising issues related to privacy and ownership of the personal information collected, processed, and stored for various purposes. So, on the one hand, there is a sense that the Indian public are concerned about data storage and usage and how their data are being misused or abused but are unable to refrain from moderating their use because of convenience and changing habits.[26] There appears to be a growing desire among citizens to engage in a transactional manner with entities that collect and share their data. Indian citizens have also increasingly embraced the cultural aspects of the digital economy and this has led to massive media consumption on personal devices, a trend COVID-19 has accelerated.

That said, there is evidence that public concern over personal information and data is rising; surveys conducted point to some anxiety over how the personal data of citizens is handled directly by entities that collect data, including the state, and indirectly after data is sliced and shared to firms that use them for discretionary purposes.[27] Indian citizens are becoming more aware that personal information is being captured, digitised, and shared in ways that are harmful to their interests. A realisation is dawning that the process of collecting and storing personal information through devices is, in some ways, depersonalising, which could result not just in a loss of privacy but also "a sense of the self"; this is driving some of the political pressures

[26] Dvara Research, "What do Indians think about privacy and data protection", https://www.dvara.com/blog/2017/11/16/privacy-on-the-line-what-do-indians-think-about-privacy-data-protection/.

[27] Interview with policy analyst, Carnegie India, 12 July 2020.

surrounding data regulation.[28] Citizens, some from the poorest segments, are questioning whether their personal information can be seen as independent of themselves or can be protected and owned without their consent or involvement. The increasing use of various apps and services is taking place under multiple campaigns initiated by the Modi government to digitise India, which has fostered indigenous and foreign platforms offering multiple services to Indian citizens.

The Indian private sector has an interest in the promulgation of robust rules covering data as they handle customers' information. Until recently, most Indian firms believed the data they collected belonged to them and not the users from whom they harvest the information.[29] This was information they could use to augment analytic capacities, enhance existing products and services, and design newer applications for public and private use. Discussions around India's data protection bill have recast such views, compelling Indian firms to rethink their role, approach, and policies concerning the personal data they have collected, from being outright owners to holders or "fiduciaries" who possess a distinct set of responsibilities.[30] That said, there has been pushback from big tech and industry. Telecom service providers like Reliance Jio have strongly encouraged the Indian government to institute strict requirements on foreign and domestic firms to hold and process data within India, otherwise known as data localisation.[31] Most small and medium-sized technology firms, particularly start-ups, are keen to work with laws covering data and how it should be handled. An uncertain regulatory environment complicates their business operations. As firms and businesses outside the technology space digitise, there will be increasing pressure to carefully manage data and not exploit customers' personal information without internal guidelines.

[28] Ibid.

[29] Interview with a former MEITY official, 23 July 2020.

[30] Interview with Think Tank official, 13 July 2020.

[31] Basu, A., and Amber Sinha, "The Realpolitik of the Reliance-Jio Facebook Deal", 29 April 2020, https://thediplomat.com/2020/04/the-realpolitik-of-the-reliance-jio-facebook-deal/.

The sheer abundance of data has raised concerns about privacy and ownership, which has compelled the Indian state to intervene. There appears to be an understanding that the Indian government could do more to protect personal data. From the Indian state's perspective, data is conceptualised as a tool that can assist bureaucrats and policymakers to design policies, disburse welfare and subsidies, realign incentives, and provide services.[32] Protecting data helps Indian policymakers fortify public digital infrastructures like Aadhaar and the India stack apparatus that incentivise innovators and entrepreneurs to develop applications for public use; data is required to facilitate this outcome.[33] Data, both personal and anonymised, also helps with the crafting of targeted policies that remove inefficiencies that have cost the Indian state billions over the decades. Another statist perspective looks at data as critical to protecting the lives of citizens from growing cyber threats, including cybercrime, which calls for their protection and accessibility. These perceptions intersect with an existing regulatory approach that often did not regulate or enforce personal data protection provisions.

Regulating Data

IT Act 2000

While no specific data protection legislation has been enacted by India yet, the existing framework that governs personal data is the Information Technology Act (2000) ("IT Act"), which contains, under Section 43A, rules regarding security practices and procedures

[32] Interview with a former MEITY official, 23 July 2020.

[33] Raman, Anand, and Greg Chen, "Should other countries build their own India Stack?", 6 April 2017, https://www.cgap.org/blog/should-other-countries-build-their-own-india-stack.

when handling personal information.[34] The IT Act was amended in 2008 with the addition of subordinate legislation that deals with data, known as the Reasonable Security Practices and Procedures Rules (RSPP), which protect sensitive personal data.[35] The law itself does not proactively enforce rules regarding data collection and protection but allows citizens to claim compensation should companies breach RSPP rules. Section 72 and 72A of the IT Act mandate criminal punishment should a government official or service provider disclose personal information without personal consent or if done to cause harm or wrongful loss.[36] Privacy rules issued by the government have been piecemeal and only apply should RSPP not be viable.

However, questions have long existed regarding RSPP's legal validity since there is no independent legal statute that compels organisations and firms to protect data. It is increasingly evident that the IT Act has not been sufficiently enforced, which has precipitated other regulators drafting their own rules to manage the consequent gaps. Other sectors have not relied on the RSPP but have chosen to draft sectoral rules that govern data. The Reserve Bank of India has issued circulars and notifications that oblige banks and other financial institutions to safeguard customer data. That said, it is essential to remember that banks in India have always been heavily regulated. Several of the new rules that banks have had to adhere to concerning cybersecurity emanate more from a desire to manage them closely than from considerations regarding data protection.[37] Other regulatory agencies like Telecom Regulatory Authority of India (TRAI) and Securities and Exchange

[34] Burman, Anirudh, "Will India's data protection law protect privacy and promote growth?", https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

[35] Ibid.

[36] Bhandari, Vidya, and Renuka Sane, "Protecting Citizens from the State post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna report and the Data protection bill 2018", http://docs.manupatra.in/newsline/articles/Upload/7B08CF55-E27D-4A44-A292-3882F08E9053.pdf.

[37] Ibid.

Board of India (SEBI) have specific rules governing data but seldom enforce them effectively. New Delhi also relies on two additional tools that track information flows – the Central Monitoring System (CMS), which provides government officials with instant access to internet traffic flowing through specific networks, and the Networks Traffic Analysis (NETRA), which analyses internet traffic through terms like "kill" or "bomb".[38]

Srikrishna Committee Report and Personal Data Protection Bill 2018

The impetus to draft a data protection law grew out of a historic Indian Supreme Court judgment affirming the constitutional right to privacy. The question of whether Indian citizens had a fundamental right to privacy arose out of a constitutional challenge to Aadhaar, India's biometric digital identity database, in 2012. The government insisted that the Indian Constitution did not guar-

[38] CMS was announced through a press release in 2009 and NETRA in 2014. See Press Information Bureau, *Centralised System to Monitor Communication,* 26 November 2009, http://pib.nic.in/newsite/.

antee a right to privacy, a question that came under a nine-judge bench who had to decide whether this right existed constitutionally. On 24 August 2017, the Court in *Justice KS Puttaswamy V Union of India* declared that privacy was a fundamental right under Part III of the Indian Constitution that lists the fundamental rights of Indian citizens, which include rights related to equality, freedom of speech and expression, freedom of movement, etc.[39] Under the Constitution, these fundamental rights cannot be stripped by law, and all rules and executive actions must not infringe them. Unlike other fundamental rights, however, the right to privacy as construed by the Puttaswamy judgment is not an absolute right but is subject to specific tests and benchmarks and competing considerations like the interests of the state and its citizens.[40] The plurality opinion authored by Justice Chandrachud held that the right to privacy was not independent of other constitutional freedoms but an essential aspect of human dignity and "an inalienable natural right".[41] In the opinion, Chandrachud ties the right to privacy to the growing digital economy, referring to the risks citizens face when transacting digitally, including the dangers of data mining and the risk of losing data, as well as underscoring the need for a comprehensive data protection law.[42]

While *Puttaswamy* was being heard, the Indian government formed an expert committee chaired by Justice BN Srikrishna (Srikrishna Committee) to review existing data protection rules and norms in India and recommend a pathway forward to replace them. Reports indicate that the Committee's work and deliberations, particularly concerning the bill, drew on the assistance of the Vidhi Center for Legal Policy, a think tank that

[39] Supreme Court of India, KS Puttaswamy vs. Government of India, 2017, https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[40] Ibid.

[41] Ibid.

[42] Ibid.

conducted research and drafted the bill.[43] After deliberations, the Committee released a "White Paper on Data Protection" in 2017 and soon after, a draft law, "The Personal Data Protection Bill 2018", with provisions to erect a comprehensive data protection framework for India.[44] The draft legislation sought to protect individual rights and autonomy concerning personal data, stipulate explicit norms through which data should be processed by entities collecting personal data, and set up a body that would regulate data processing. The bill also openly recognised the perils posed by a rapidly digitising economy for Indian citizens and sought to create rules that updated the existing IT Act.

The initial bill consisted of rules governing the handling of personal data by both the government and private firms and organisations ("data fiduciaries") based in India and abroad. Processing is only allowed once individual consent is provided; for consent to be valid, it has to be freely given, specific, clear of jargon, and capable of being withdrawn.[45] The bill also made explicit consent mandatory for organisations processing sensitive data; citizens and consumers, or "data principals", have rights concerning their data and they can demand that those who store and process it, or "data fiduciaries", safeguard their personal information.[46] These fiduciaries have particular obligations while processing and managing personal data, which involves providing notifications and clarity on the nature and purposes of data processing. Obligations apply to both private firms and the government, and require that they process the data in a "fair and reasonable way" that "respects individual privacy". The 2018 bill also limited the potential for abuse by enumerating conditions under which data

[43] Narayanan, Dinesh, and Venkat Ananth, "Vidhi and the making of India's data protection law", https://economictimes.indiatimes.com/prime/economy-and-policy/vidhi-and-the-making-of-indias-data-protection-law/primearticleshow/77768876.cms?from=mdr.

[44] Government of India, Ministry of Information Technology, "Personal Data Protection Bill 2018", https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[45] Ibid.

[46] Ibid.

must be processed and a set of requirements that fulfil these conditions.

The 2018 bill also called for the establishment of a Data Protection Authority (DPA) to oversee and regulate data and its handling between the "data principals" and "data fiduciaries".[47] The DPA was enshrined with vital investigatory and supervisory responsibilities, and the authority to impose penalties and sanctions on entities that transgress rules. That said, questions surrounding the body's autonomy were raised since most of the regulators would be parachuted in from the government.[48]

Finally, the most contentious part of the bill was a provision that required one copy of personal data to be stored within Indian territory to ensure Indian law enforcement officials had access to that data; this provision has come to be known as "data localisation".[49] Certain types of personal data, such as critical personal data with sensitive information, were required to be stored only in India. Though the bill provided exemptions to the processing of personal data and data principals' rights if their data was used for national security purposes, the processing must be done proportionately and only when necessary. Sufficient protections were also added into the bill to prevent mass surveillance.

Unsurprisingly, sizeable Indian technology companies – Reliance, Paytm, and PhonePe – already have data centres in India or can pay for their data to be stored in local data centres.[50] Large Chinese companies – Alibaba and Xilinx – have taken pro-localisation stances, possibly because they have data centres set up in India. But this move toward data localisation was vocally opposed by several US tech companies. Facebook Public Policy Vice President Nick Clegg and Google CEO Sundar Pichai, along with lobbying groups such as the US-India

[47] Ibid.

[48] Burman, Anirudh, "Will a GDPR-Style Data Protection Law Work For India?", *Carnegie India,* 21 August 2019.

[49] Ibid.

[50] Basu, A., and Karthik Nachiappan, "The battle for data sovereignty, India and Digital worldmaking", Seminar Magazine, July 2020.

Strategic Partnership Forum (USISPF), US-India Business Council (USIBC), and National Association of Software and Service Companies (NASSCOM), made several trips to New Delhi to emphasise that message.[51]

The industry-driven lobbying worked in tandem with US government efforts, as data localisation became an increasingly vital part of the agenda in bilateral trade talks. In fact, Secretary of State Mike Pompeo reportedly contemplated limiting the number of H1B visas granted to Indian citizens if the localisation provisions were not relaxed. President Trump himself made a public statement explicitly denouncing data localisation at the G20 Osaka Summit.[52] The lobbying by US and Western government officials and the tech industry appears to have worked. When IT Minister Ravi Shankar Prasad introduced a revised version of the bill in December 2019, the mirroring provision was gone.

Personal Data Protection Bill 2019

The first iteration of India's personal data protection bill languished for nearly 18 months before Indian officials released an updated version of the bill in December 2019. The revised version offers strong individual protections concerning data processing by firms. Still, there are apparent differences, particularly concerning the government's exceptions from the first legislation that give the government considerable scope to accumulate citizens' data without constraint. The controversial provision that mandated storing a copy of all personal data in India, or data localisation, has been relaxed, applying localisation to only sensitive and critical personal data, the definitions of which have also been clarified.

There is more clarity concerning data categorisation under the new version of the bill – data can be classified as personal data, non-personal data, sensitive

[51] Basu, A., and Amber Sinha, "The Realpolitik of the Reliance-Jio Facebook Deal", 29 April 2020, https://thediplomat.com/2020/04/the-realpolitik-of-the-reliance-jio-facebook-deal/.

[52] Ibid.

personal data or critical personal data. Non-personal data is simply anonymised data.[53] Personal data, under the IT Act, which terms it "personal information", is any information that relates to a natural person that either directly or indirectly, in combination with other information available or likely to be available is capable of identifying such a person. The PDP bill supplements this with any inference drawn from such data for profiling.[54] Sensitive personal data includes passwords; financial data, such as bank account and payment instrument details; health data, which contains records and history of both physiological and mental conditions; sexual orientation; and biometric information.[55] The bill expands this to include genetic data, transgender status, intersex status, caste or tribe, and religious and political belief or affiliation.[56] Another type of data proposed by the bill is critical personal data, the definition of which allows the government to decide without limiting its authority to do so. The bill also strictly localises this data, making exceptions only for transfers to countries or organisations considered capable of providing protection and transfers that protect vital interests.[57]

Consent, in the context of data collection in India, which is primarily defined by the newly proposed Personal Data Protection Bill 2019 ("2019 bill"), has been criticised for being a mechanism private companies can

[53] Mehrotra, Karishma, "Explained: Data, Their Types, and Other Terms Described in India's PDP Bill", *The Indian Express,* 13 December 2019, https://www.indianexpress.com/article/explained/this-word-means-data-their-types-and-other-terms-described-in-indias-pdp-bill-6164247/.

[54] Thakore, Talwar & associates, "Data Protected India", *Linklaters,* March 2020, https://www.linklaters.com/en/insights/data-protected/data-protected---india.

[55] Thakore, Talwar & associates, "Data Protected India", *Linklaters,* March 2020, https://www.linklaters.com/en/insights/data-protected/data-protected---india.

[56] Ray, Saladitya, "Justice Srikrishna data protection draft bill is now public, highlights, and what happens next", *MediaNama,* 27 July 2018, https://www.medianama.com/2018/07/223-sri-krishna-bill-submitted/.

[57] Wimmer, Kurt, and Maldoff, Gabe, "India Proposes Updated Personal Data Protection Bill", *InsidePrivacy,* 12 December 2019, https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/#:~:text=Critical%20personal%20data%3A%20As%20with,be%20transferred%20outside%20of%20India.

exploit to escape liability for harm. The issue lies in the bill's reduction of consent to a concept that focuses on the avoidance of liability for harm instead of ensuring citizens' interests in terms of their fundamental right to personal privacy.[58] The 2019 bill still adopts a system of blanket consent, whereby no provisions require "data fiduciaries", the entity that collects and processes an individual's data, to seek consent from a data principal for new processing – only that they "shall notify the data principal of important operations in the processing of personal data through periodic notifications" under Clause 30(2) ("data principal" refers to the individual whose data is being collected and processed). This clause fails to include the requirement to seek consent for the processing of data for a purpose other than that which was stated at the time of consent, thus impeding data handling transparency and making it difficult for data principals to hold fiduciaries accountable.[59]

One recommendation that appears is that consent should be required incrementally, and that purposes of data usage should be defined narrowly so that data principals are fully aware of how their data is being used, which should mainly be to improve services that the data principals should be allowed to enjoy. Though reducing consent fatigue remains essential, the focus of consent should be on the autonomy of the data principal in regard to their data, which is to say that any policy regarding personal data should include provisions for data principals to withdraw consent at any point without the threat of legal consequences, as well as provide data principals with the *choice* to know about and consent to the new processing. Legal analysts have pointed out that the bill does not leave data principals with provisions to ensure this clean exit.

The 2019 bill has also been criticised for facilitating government control over data without ensuring proper procedural checks and balances. Significantly, the provi-

[58] Government of India, "The Personal Data Protection Bill", 2019, Bill 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[59] Ibid, 5-6.

sion that obliged government processing of data to be "necessary and proportionate" has been culled in the latest version of the bill; furthermore, another provision was added, giving the government total discretion to exempt any agency or department from any part of the law.[60] This move leaves the current policy vacuum around India's surveillance intact, which appears to be incompatible with a robust privacy protection framework.

The new governing body that ostensibly has the rule-making and adjudication power necessary to resolve trade-offs is the Data Protection Authority ("DPA"), according to the 2018 bill. However, the new 2019 bill limits these powers; it transfers them to the government, namely the ability to notify other categories of sensitive personal data and determine and notify significant data fiduciaries.[61] This expansion of powers results from the 2019 bill's provisions regarding the Constitution of the DPA. The 2018 bill had provisions that included independent members in the DPA's governing committee, particularly experts from interest groups who could represent specific non-governmental interests; the 2019 bill replaces them entirely, through a clause that only permits government nominees.[62]

The 2019 bill, out of line with other statutory agencies' practices, does not allow part-time members in the DPA's committee, which thus effectively leaves out expertise from academics, researchers, practitioners, and technical experts, who could have brought independent input to the DPA's functioning. The key players responsible for the appointment of members themselves also pose an added dimension to the DPA's independence. While the 2018 bill stipulated that the Chief Justice of India, or another judge of the Supreme Court, head the selection committee, the 2019 bill alters this so that the selection committee is a body led by government

[60] Government of India, "The Personal Data Protection Bill", 2019, Bill 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[61] Ibid, 5.

[62] Ibid, 21.

executives, i.e., the Cabinet Secretary and Secretaries in-charge of Legal Affairs and Electronics and Information Technology, thereby transforming the DPA into merely another governmental arm and weakening the enforcement of data protection laws, as it allows government hierarchies to perpetuate in a regulatory body that is meant to supervise personal data processing in both the private sector and, more importantly, government agencies.[63]

The ease with which the government can exempt government agencies from the provisions compromises the bill's goal of ensuring individuals' rights to their privacy. The inapplicability of the bill to the Unique Identification Authority of India, for example, is concerning as it holds all Aadhaar data. Justice Srikrishna himself calls the 2019 bill "unconstitutional", claiming it could turn India into an Orwellian state. He subsequently advocated for the new bill to be challenged in the Supreme Court, should it be passed in its current form, pointing out how the safeguards put in place in the 2018 bill to ensure the DPA's independence, and to ensure protection against government data misuse in general, were absent from the new bill. The revised bill also does not adequately spell out when the DPA will be created and how quickly it will enforce incumbent rules in terms of a timeline. The new law also removes references to the timeline outlined in the previous version, giving the government carte blanche to determine when and how the law will come into place once enacted.

The 2019 bill increases the government's authority through exemptions for its agencies to process personal data for purposes that are too broadly defined, under Chapters 3 and 9.[64] State functions such as carrying out evidence-based policy-making and provision of benefits or services lack specificity to their definitions, and the exemptions leave much room for abuse, particularly in instances where the government could access information without sufficient consent. The updated legislation also expects companies and organisations to transfer

[63] Ibid, 21-22.

[64] Ibid, 8-9.

non-personal data (NPD) to the government to assist public and policy-planning functions, creating problems related to privacy and intellectual property protection.[65]

So far, there's a clear recognition in India that data creates economic value, including enormous social and public value.[66] As mentioned, India has been at the forefront of debates around data localisation or the domestic retention of personal data collected in India. Data localisation featured in India's first Personal Data Protection Bill unveiled in July 2018 by the Justice Srikrishna Committee, and was emphasised in the second iteration of the bill, released in December 2019 and now being discussed in parliament. As deliberations on the PDP Bill continue, another committee discussing non-personal data released its report on what the Indian government should do with NPD, the implications of which could matter more than the bill regulating personal data.

Governing Non-Personal Data

In September 2019, the Indian Ministry of Electronics and Information Technology (MEITY) formed a committee of experts to discuss whether an NPD governance framework was required to deal with the anonymised data generated. The Committee was tasked to make specific suggestions to the government on how to regulate NPD.[67] The Committee consulted representatives from various sectors, including business, think tanks, and civil society, to solicit their views and ideas. NPD, the Committee's focus, refers to anonymised data or data that does not contain any personally identifiable

[65] Ibid, 20.

[66] Also reflected in the 2019 Indian Economic Survey. See the Government of India, Ministry of Finance, "2019 Indian Economic Survey", https://library.iima.ac.in/public/Economic_Survey_2019_20_Vol_2.pdf.

[67] Gupta, A., and S. Jaju. "Summary of the report of the Committee of Experts on Non-Personal Data", 14 July 2020, https://www.ikigailaw.com/summary-of-the-report-of-the-committee-of-experts-on-non-personal-data/#acceptLicense.

information; in essence, this means that no individual or living person can be identified by accessing this data.[68]

Interestingly, the 2019 Data Protection Bill defines non-personal data unhelpfully as "anything that is not personal data", while providing the government the right to access both non-personal data and "anonymised personal data" when it deems fit. However, these two categories should be treated differently.[69] In practice, NPD includes climate trends collected by weather services and apps or traffic patterns gathered by a public transit operator or private cab service. The Committee had to, in effect, recommend a framework and a policy that the government can adopt to leverage the data collected from 1.2 billion Indian citizens that different entities, government and non-governmental actors like small businesses and other organisations, can use to improve their capabilities, operations, and services.[70]

The need to regulate NPD ostensibly emanates from two motivations. First, like personal data, NPD has unsurpassed economic value that requires regulation to ensure it is used for the public benefit and not misused or appropriated. And second, anonymised data being collected could be used to better governance. These objectives have guided the government's approach to data in the last few years. In August 2017, India's telecommunication regulator released a consultation paper that extolled data's economic value and called for sufficient protections to ensure personal data receives adequate safeguards.[71] Soon after that, NITI Aayog released India's National Strategy for Artificial Intelligence, which stated that data concentration amongst a few tech firms prevented data access for an entire technology eco-

[68] Ibid.

[69] Government of India, "The Personal Data Protection Bill", 2019, Bill 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[70] Government of India, "Report by the Committee of Experts on Non-Personal Data Governance Framework", https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

[71] Telecom Regulatory Authority of India, "Consultation Paper on Free Data", https://www.trai.gov.in/sites/default/files/CP_07_free_data_consultation_0.pdf.

system.[72] The AI strategy suggested that data must be openly shared for good governance. This impulse was reinforced by the Srikrishna Committee, which drafted India's first PDP Bill, which also called for the protection of community data, notwithstanding provisions covering personal data.

These developments predated the formation of the NPD Committee, headed by former Infosys co-founder Kris Gopalakrishnan. The Committee's report calls for NPD generated in India to be harnessed by domestic agencies and companies to generate economic gains.[73] It recommends a separate NPD regulation that enables different actors like the government, businesses, and other organisations to request anonymised data for particular purposes. In effect, the report proposes a regulatory structure that would obligate data sharing by entities collecting data, as well as their registration with a new data regulator to leverage data for private use.[74] To ensure a level playing field that does not favour big companies or the government, the Committee also proposed establishing a new regulator, the Non-Personal Data Authority, to govern how NPD is used and deployed. The Committee's hope is that data sharing, given the record amounts of public and private data being collected, will "spur innovation at an unprecedented scale."[75]

Whether mass innovation occurs or not, the NPD Committee's report has heightened fears that the government plans to create a digital state propelled by data. This approach does signal to American and Indian tech firms, who organise their businesses and operations around data collected on their platforms, that data cannot be withheld and that the time has come to disman-

[72] NITI Aayog, "National Strategy for Artificial Intelligence", June 2018, https://niti.gov.in/writereaddata/files/document_publication/National-Strategy-for-AI-Discussion-Paper.pdf.

[73] Government of India, "Report by the Committee of Experts on Non-Personal Data Governance Framework", https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

[74] Ibid, 40-44.

[75] Ibid, 30.

tle data silos in the public's interest. The key question going ahead is whether tech firms will comply with this policy approach should an NPD legislation be enacted, which could compel them to roll back investments and operations in India. Moreover, anonymised data becoming more accessible could also create security risks, particularly related to identification. The stakes are high. New Delhi has to balance between privacy concerns, security risks, and investment opportunities as it decides how it will regulate both personal data and NPD.

Conclusion – India

On 11 December 2019, the Indian government introduced the revised Personal Data Protection Bill. Ravi Shankar Prasad, Indian Minister for Electronics and Information Technology, announced that the legislation would be discussed at a joint parliamentary committee before being submitted to the lower house of parliament; this decision troubled many experts and analysts who thought that, as per custom, the legislation would have gone to the Standing Committee on Information Technology for additional scrutiny. Questions, as a result, swirl around the bill, given its significance for domestic and foreign firms engaged in India's digital economy and critics who fear the bill solidifies government control of personal information. The updated data protection bill does little to quell reservations regarding the latter concern; instead, serving as grist for more. Going ahead, foreign firms will have to adjust to a complicated, undeniably state-heavy regulatory terrain in India around data protection.

Given rapid digitisation and pervasive use of social media platforms by Indian citizens, there was a demand to regulate data collection in India. In its first iteration, the bill sought to create a comprehensive data protection framework that outlined responsibilities for citizens, organisations, and firms that hold personal information. The legislation's original intent was to develop rules to protect individual privacy and prevent misuse of personal data. Individuals have to explicitly give

consent, notwithstanding questions around whether consent is meaningful or efficacious, before their data was collected and used or monetised. Firms, or data fiduciaries, have to adhere to several rules while collecting and processing data. The previous bill also called for the establishment of a data protection authority, a data regulator, that would monitor regulatory compliance vis-à-vis data collection and protection and impose sanctions when violations occur. This authority, given a sweeping mandate, will have power over tech companies and any firm across sectors that obtain information from customers.

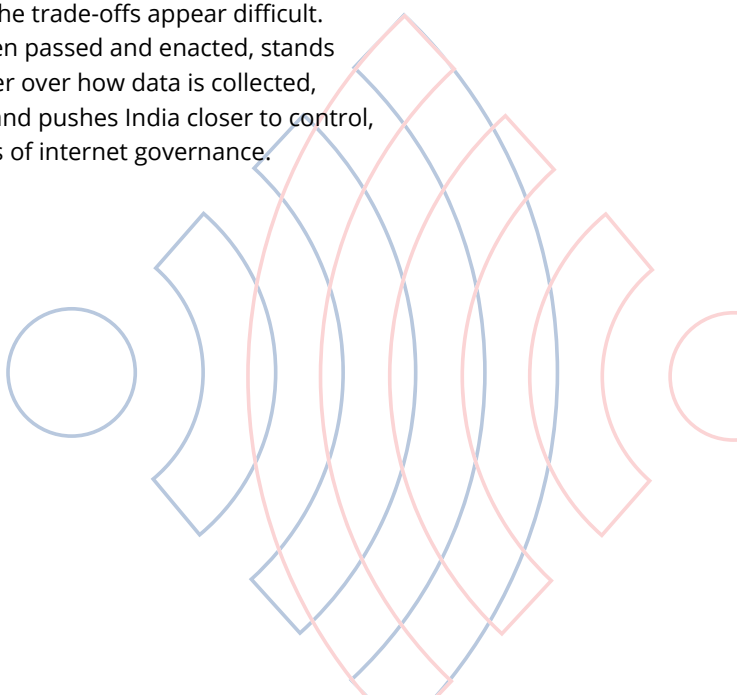
Three issues come to the fore with the revised 2019 bill. First, the legislation enhances state power and control relative to citizens' rights. The legislation gives the government considerable power to collect and hold data that New Delhi deems pivotal to state sovereignty and the larger public interest. Moreover, the bill places fewer restrictions on Indian government agencies, which already hold Indian citizens' sensitive data and information gathered through the Aadhaar database. Government agencies are exempt from stringent rules governing data provided they can make a case for either national security or public order reasons. The government will also have the authority to demand that technology companies like Facebook, Twitter, and Google share personal and anonymised non-personal data for policy-making purposes, particularly welfare and social policies. The government's role vis-à-vis data protection has veered sharply to the other direction, from expecting the state to follow data rules, as outlined in the original bill, to exempting it. Unequivocally, the government appears to have prioritised state control of data over enhanced data protection for citizens.

Second, the revised bill confers power to the new data protection authority (DPA) to draft specific rules, set compliance procedures, and settle disputes that arise. Critically, the body will shape how consent requirements are framed and applied. Membership within the DPA is tilted toward the involvement of high-level government officials. It is unclear how the new authority will evolve as the amount of data online rises exponen-

tially as more and more Indian citizens go online. What also remains vague is whether the proposed regulator can ably discharge functions under its future remit, which could sow uncertainty among firms looking for clear rules and enforcement.

Third, the new bill softens provisions that mandated data localisation or rules that expect firms collecting personal data to retain a copy of it in India. The new legislation obliges tech companies to store sensitive data, like financial and biometric data, on Indian servers but allows for data to be processed abroad under certain conditions. Though data localisation is tempered, the new bill contains a critical provision – identity verification – that could affect how social media platforms like Facebook operate and how citizens use such content-driven platforms. Platforms like Facebook will be required to offer users a way to verify their identity and display a public sign detailing verification before they communicate online. With this move, the government looks to stem the spread of fake news and misinformation sprouting out of these platforms.

India's latest data protection bill does not resemble its initial version. Revised provisions generate more questions concerning whether India can advance globalisation, particularly given rapid digitisation and more widespread state control. The trade-offs appear difficult. The 2019 data bill, when passed and enacted, stands to augment state power over how data is collected, processed, and used, and pushes India closer to control, not openness, in terms of internet governance.



Indonesia – Regulating Data

Introduction

When the internet first became widely used in Indonesia in the 1990s,[76] data security and privacy began to be seen as fundamental human rights to be safeguarded by the state.[77] Indonesia's constitution (*Undang-Undang Dasar Republik Indonesia 1945*) acknowledges this right. Article 28G, verse (1) of the constitution states that "every person deserves protection for themselves, their family, their honour, their dignity, and their belongings, and they also deserve the sense of security and protection from any threats that push them to do or not do something, for it is a human right."[78]

This serves as the legal framework for data protection regulations in Indonesia, where data privacy is regarded as a component of human rights. Additionally, Law No. 39/1999 on Human Rights highlights the freedom of privacy in regard to communication through electronic means.[79]

[76] See Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2017, *Sejak Kapan Masyarakat Indonesia Menikmati Internet.* Available at https://stei.itb.ac.id/id/blog/2017/06/19/sejak-kapan-masyarakat-indonesia-nikmati-internet/. [Accessed 24 June 2020].

[77] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan", *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

[78] The 1945 Constitution of the Republic of Indonesia.

[79] Indonesian Law No. 39/1999 on Human Rights.

As Indonesia's internet penetration rises, issues related to data protection started to affect various aspects of people's lives. The discourse on data protection no longer just revolves around the protection of users' data; increasingly it is more about how the data is collected, stored, processed, and used.

The Urgency of Data Protection Regulations

Four key issues that highlight the urgency for data protection regulations in Indonesia are:

1) Public perception of data privacy

Internet penetration level in Indonesia reached 73.7% in 2020.[80] This is equivalent to 201.58 million internet users from a total population of 273.52 million people.[81] Indonesia is a top-five market globally for US tech giants Facebook and Twitter.[82] There were 160 million active social media users in January 2020, the result of a 8.1 percent increase from April 2019.[83]

Internet penetration level
73.7%

160 million
active social media users

[80] See Asosiasi Penyelenggara Jasa Internet & Indonesia Survey Center, 2020, *Laporan Survei Internet APJII 2019-2020 (Q2)*. Available at https://apjii.or.id/downfile/downloadsurvei/infografis_apjii.pdf%20. [Accessed 26 March 2021].

[81] See Ibid.

[82] Johny Plate in Reuters, 2019, "Indonesia needs to establish a data protection law urgently". Available at https://www.reuters.com/article/us-indonesia-communications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Accessed 3 June 2020].

[83] We Are Social and Hootsuite, 2020, "Digital Indonesia", https://datareportal.com/reports/digital-2020-indonesia. [Accessed 3 June 2020].

The term "data is the new oil" represents how tech companies gain benefit from people's digital activities. The Cambridge Analytica scandal of 2018 was one such experience where millions of Facebook users' personal data was used without consent.[84, 85]

Another issue is the high number of internet users who are not equipped with adequate knowledge about data privacy and how they should manage their personal data. Wahyudi Djafar, Deputy Director of Research at ELSAM, a human rights NGO, noted how common it is for the public to post sensitive personal data (home address, phone number, etc.) on various social media platforms.[86]

Although several civil society organisations have been calling for increasing public awareness on personal data, a structural effort by the government is needed to safeguard against personal data risks. Providing a comprehensive legal instrument and/or regulatory body on personal data protection is an example of this structural approach.

2) Economic opportunities of having data protection regulations

Indonesia, like many other Southeast Asian countries, is experiencing robust growth in its digital economy. Between 2015 and 2020, the value of Indonesia's digital economy grew from USD8 billion to USD40 billion.[87]

---

[84] Salna, 2018, *The Jakarta Post.* "Facebook faces Indonesian Police investigation over the data breach", https://www.thejakartapost.com/life/2018/04/06/facebook-faces-indonesian-police-investigation-over-data-breach.html. [Accessed 3 June 2020].

[85] Yuniar, R., 2018, "This Week in Asia. Facebook's Cambridge Analytica scandal puts Indonesia's tech firms on the spot", https://www.scmp.com/week-asia/business/article/2143763/facebooks-cambridge-analytica-scandal-puts-indonesias-tech-firms. [Accessed 3 June 2020].

[86] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan", *ELSAM* (Online). Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

[87] Jakarta Globe, 2020, "Jokowi hopes to unleash digital economy potential". Available at https://jakartaglobe.id/tech/jokowi-hopes-to-unleash-indonesias-digital-economy-potential/. [Accessed 3 June 2020].

Value of Indonesia's digital economy

2015: USD8b
2020: USD40b
2025: USD150b (est.)

In 2025, it is predicted that the value of the country's digital economy will reach USD150 billion.[88] In 2017, President Joko Widodo issued Presidential Regulation no. 74/2017 on the National E-Commerce Roadmap, 2017-2019.[89] This policy emphasises the government's initiative to improve Indonesia's economic growth through the development of its digital economy.

Robust data protection regulations have already been adopted in some nations, such as the General Data Protection Regulation (GDPR) by European Union countries, as well as the Privacy Framework adopted by Organisation for Economic Cooperation Development (OECD) and Asia-Pacific Economic Cooperation (APEC) countries.

But Indonesia is lagging behind due to the absence of a general data protection regulation. This risks damaging the country's bargaining power in several trade negotiations concerning the digital economy. Indonesia faces issues when trading data with other nations who already have these regulations. The inability to trade data will be an obstacle for the expansion of Indonesia's economic activities. Thus a data privacy law is essential

[88] McKinsey & Company, 2016, "Unlocking Indonesia's digital economy". Available at https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Accessed 3 June 2020].

[89] See Kementerian Komunikasi dan Informatika, 2017, *Inilah Road Map E-Commerce Indonesia 2017-2019.* Available at https://kominfo.go.id/content/detail/10309/inilah-road-map-e-commerce-indonesia-2017-2019/0/berita. [Accessed 26 June 2020].

if Indonesia is to continue attracting foreign investments.[90]

3) The threat of data breaches

The rise of the digital economy in Indonesia comes with a challenging issue – digital companies do not only provide services to their users but also collect their personal data. Notwithstanding this, e-commerce activities in Indonesia are also expanding vastly. A report by We Are Social and HootSuite estimated that 88% of people in Indonesia have purchased products online. Thus, it is no surprise that many of Indonesia's e-commerce companies are experiencing rapid growth.

However, the digital economic landscape is not immune to crime and has had to deal with incidents in the past, including the theft of users' personal information due

[90] Yatim, S., 2019, "The privacy battle in Indonesia - the longer the battle, the more consumers stand to lose". *The Jakarta Post.* Available at https://www.thejakartapost.com/academia/2019/02/21/the-privacy-battle-in-indonesia-the-longer-the-battle-the-more-consumers-stand-to-lose.html. [Accessed 3 June 2020].

to data breaches.[91, 92, 93] Data breaches tend to occur in the socio-political domain. For example, the Indonesian General Election Commission (*Komisi Pemilihan Umum*) experienced a breach of 2.3 million voters' information.[94] The urgency of personal data protection has become even more critical during the Covid-19 pandemic, as government institutions collect data on patients and suspected cases. There have been reported incidents of personal data breaches.[95]

The cases of data breach are still being investigated today; they provide cautionary tales on the risks of a lack of legislative protection for personal data. First, Indonesia's digital ecosystem (whether relating to private-owned or government-owned entities) is prone to digital hacking. As a nation with a massive number of internet users, it should be a key priority for the Indonesian government to protect data across all sectors from digital attacks.

Second, given the absence of a general data protection regulation, the government cannot effectively execute legal enforcement. In the case of Tokopedia, as it is a private business platform, a general data protection regulation would have guided the government to take appropriate measures in sanctioning Tokopedia, should the platform be proven to be accountable for the mas-

[91] The Jakarta Post, 2020, "Data breach jeopardizes more than 15 million Tokopedia users, report finds". Available at https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Accessed 3 June 2020].

[92] Tempo.co, 2019, "Bukalapak confirms an attempted customer data breach". Available at https://en.tempo.co/read/1186473/bukalapak-confirm-of-an-attempted-customer-data-breach. [Accessed 3 June 2020].

[93] The Jakarta Post, 2020, "E-commerce platform Bhineka.com reported to be the latest target of data theft". Available at https://www.thejakartapost.com/news/2020/05/13/e-commerce-platform-bhinneka-com-reported-to-be-latest-target-of-data-theft.html. [Accessed 3 June 2020].

[94] Setiawan, R., 2020, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", *Tirto.* Available at https://tirto.id/fA5B. [Accessed 24 June 2020].

[95] Tempo.co, 2020, "Ministry still Tracing Indonesia's Covid-19 patients' data leak". Available at https://en.tempo.co/read/1356052/ministry-still-tracing-indonesias-covid-19-patients-data-leak. [Accessed 28 June 2020].

sive data breach. Furthermore, research from ELSAM noted that several technology companies in Indonesia have not adopted any data protection policies, partly because there is no regulation promulgated by the Indonesian government to comply with.[96]

4) Debates on the draft Personal Data Protection Law

Personal data protection has gained the attention of Indonesia's civil society organisations (CSO). CSOs such as ELSAM, ICT Watch, and SAFEnet have urged the government to adopt the draft Personal Data Protection (PDP) law.[97, 98, 99] The government, through the Ministry of Communications and Informatics (MoCI), has also urged the legislative body (House of Representatives or DPR) to pass this law.[100] The draft has been listed in the national legislation programme, to be reviewed and adopted as a law, but the process has been suspended due to a lack of prioritisation. An interview with Novel Ariyadi, a cybersecurity expert in Indonesia, indicates that this impediment was political: "There is no open and reliable reason why the DPR has not passed the law."[101]

[96] See ELSAM, 2019, *Penyalahgunaan Data Pribadi Meningkat, Perlu Akselerasi Proses Pembahasan RUU Perlindungan Data Pribadi.* Available at https://elsam.or.id/5806-2/. [Accessed 26 June 2020].

[97] ELSAM, 2019, "Pentingnya UU Perlindungan Data Pribadi". Available at https://elsam.or.id/pentingnya-uu-perlindungan-data-pribadi/. [Accessed 3 June 2020].

[98] Jawa Pos, 2019, "ICT Watch desak UU Perlindungan Data Pribadi segera dirampungkan". Available at https://www.jawapos.com/oto-dan-tekno/teknologi/01/08/2019/ict-watch-desak-uu-perlindungan-data-pribadi-segera-dirampungkan/. [Accessed 3 June 2020].

[99] AntaraNews, 2019, "SAFENet harap menkominfo Johnny G Plate selesaikan UU PDP". Available at https://www.antaranews.com/berita/1129032/safenet-harap-menkominfo-johnny-g-plate-selesaikan-uu-pdp. [Accessed 3 June 2020].

[100] Johny Plate in Reuters, 2019, "Indonesia needs to establish a data protection law urgently". Available at https://www.reuters.com/article/us-indonesia-communications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Accessed 3 June 2020].

[101] An interview with Novel Ariyadi, cybersecurity and public policy expert in Indonesia, 19 June 2020.

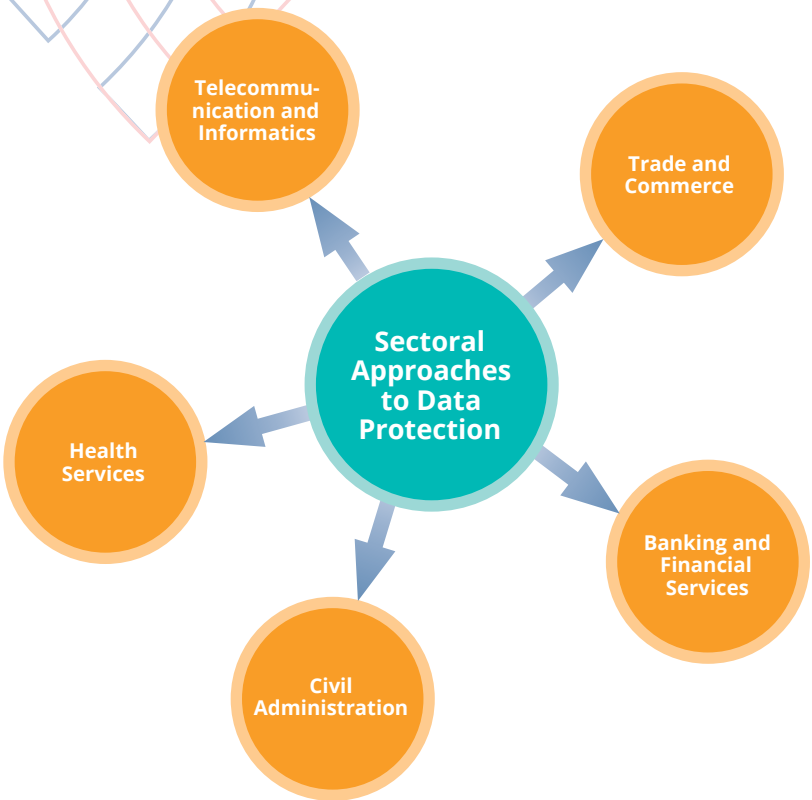
At the regional level, the political pressure to issue this law can be seen in how ASEAN has prompted member states to adopt improved personal data protection laws. ASEAN has established a Framework of Personal Data Protection through ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN). The framework aims to strengthen personal data protection for citizens of ASEAN nations and bolster cooperation amongst member states. This cooperation is mainly driven by the promotion of regional and global trade, as well as information flows.[102]

Even though this framework was not intended to create obligations under domestic laws, Indonesia is lagging behind compared to Singapore, Malaysia, Thailand, and the Philippines. Furthermore, as ASEAN states trade heavily with Europe, businesses must comply with EU regulations. With the enactment of the GDPR, many ASEAN countries have started to review their data protection laws.

[102] ASEAN, ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN).

Sectoral Approaches to Data Protection

Personal data protection in Indonesia is governed by at least 30 regulations issued by various government bodies and ministries.[103] To delve deeper into how data protection is regulated and enforced, this section identifies five sectors most affected by massive flows of data. By examining these sectors, we conclude that data protection in Indonesia is still heavily sectoral, and data regulators (i.e., government institutions) handle data protection according to their own policies.



[103] Djafar, W., Sumigar, B. R. F., and Setianti, B. L., 2016, *Perlindungan Data Pribadi di Indonesia; Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia.* Jakarta: ELSAM.

In this sector, the notion of data protection revolves around the confidentiality of a person's information flow and communication.[104] Although information tapping is prohibited as per Law No. 36/1999, telco operators are still given the authority to record their users' telecommunication activities for proof-of-transaction purposes, upon request from the service user.[105]

As digital services expand, data protection regulations in the telecommunication and informatics sector also broaden to cover the use of data by electronic systems, as stated in Law No. 11/2008 on Electronic Information and Transaction, also known as *"UU ITE"*. This law emphasises that any flow of personal data should be authorised before the data is moved from one person to another.[106] However, this also creates another loophole, because proving that data is being moved unlawfully often requires a complicated process if deliberated in a court of law.[107]

[104] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan". *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

[105] Ibid.

[106] Indonesian Law No. 11/2008 on Information and Electronic Transaction.

[107] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan". *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

Another problem that arises from *"UU ITE"* is the adoption of the "right to be forgotten" principle, as exemplified by a ruling by the Court of Justice of the European Union (CJEU). This adoption requires electronic systems to erase any "irrelevant" electronic information and/or documents from its database and services. However, the regulation does not explain in detail the types of information that can be considered as "irrelevant".[108] This loophole may cause further problems in potential interference with freedom of speech in Indonesia.

To increase protection of how personal data is collected, stored, processed, and used, the MoCI has issued several regulations (*Peraturan Pemerintah & Peraturan Menteri*) that describe more detailed aspects of data management between the user and the electronic system. For example, MoCI Regulation No. 20/2016 on Protection of Personal Data in the Electronic System outlines the rights of the data owner and the responsibilities of the electronic system's manager with respect to the management of users' data.[109] However, these regulations are not fully adhered to by the majority of electronic system managers operating in Indonesia, because they see the regulations as weak (viz., not yet a law).[110] Therefore, it may be argued that these regulations do not have strong legal binding power over electronic system managers in Indonesia.

[108] Ibid.

[109] Indonesian MoCI Regulation No. 20/2016 about The Protection of Personal Data in the Electronic System.

[110] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan". *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

Data Protection Regulations in Telecommunication & Informatics			
No.	Example(s) of Regulation	Key Point(s) on Data Protection	Loopholes
1	Law No. 36/1999 on Telecommunications	• This law emphasises the confidentiality of a person's information flow and communication. Information tapping is prohibited.	• The law still allows telco operators to record users' telecommunication activities for proof-of-transaction purposes.
2	Law No. 11/2008 on Information and Electronic Transactions	• The flow of any personal data should be authorised before data is moved from one actor to another.	• This requires a complicated legal process to prove that the data is being moved unlawfully.
3	Law No. 19/2006 on the Amendment of Law No. 11/2008 on Electronic Information and Transaction	• The adoption of the "right to be forgotten" principle • It requires electronic systems to erase any "irrelevant" electronic information and/or documents from its database and services.	• The definition of "irrelevant" information is not clear. Therefore, if any information can be erased based on this unclear definition, it might endanger freedom of speech in Indonesia.
4	MoCI Regulation No. 20/2016 on The Protection of Personal Data in the Electronic System	• This regulation emphasises the responsibilities of electronic system managers in managing their collected data.	• This is seen as not legally binding for electronic system managers in Indonesia, leading to low levels of compliance.

Trade and Commerce

As a country that is increasingly conducting trade and commerce in the digital environment, Indonesia's data protection regulations in this sector are related to those that exist in the telecommunications and informatics sector. For example, Law No. 7/2014 on Trade states that any transaction that uses electronic systems (*e-commerce*) should comply with Law No. 11/2008 on Electronic Information and Transaction or "*UU ITE*".[111]

Surprisingly, Law No. 8/1999 on Consumer Protection does not emphasise the importance of personal data protection, but rather the availability of precise information regarding a seller's product or service to the consumer.[112] This regulation highlights the fact that data protection regulations in the trade and commerce sector are still based on regulations that apply to the telecommunications and informatics sector.

Data Protection Regulations in Trade and Commerce

No.	Example(s) of Regulation	Key Point(s) on Data Protection	Loopholes
1	Law No. 7/2014 on Trade	• With the growing number of e-commerce transactions, this law states that data protection on e-commerce transactions should be executed per Law No. 11/2008 on Information and Electronic Transaction (*UU ITE*).	• Indonesia's data protection regulation in trade and commerce is heavily reliant on regulations governing the telecommunication sector. • Government actors that oversee telecommunication sector regulations should also play a role in legal enforcement if there is data leakage in the commerce sector.
2	Law No.8/1999 on Consumer Protection	• Instead of emphasising the protection of customers' data, this law points out the importance of information regarding sellers' products or services.	

[111] *Indonesian Trade Law No. 7/2014.*

[112] *Indonesian Law No.8/1999 on Consumer Protection.*

In this sector, the data protection regulations focus more on the principles of data confidentiality. It also requires banks and financial service providers to secure any personal information that they collect from the customer (i.e., financial statements, bank accounts credentials, etc.).[113] Regulated through the Banking Law No. 10/1998, data collection processes are legally permitted, as the data protection regulation in this sector argues that banks and other financial service providers should have sufficient capacities to store their customers' data safely.[114]

As the advancement of technology brings various innovations to financial services, the government established a new public institution called "Otoritas Jasa Keuangan" or OJK (*Financial Service Authority*), which oversees banks and other financial service providers. OJK issued several regulations on data protection in the financial sector. For example, OJK Circular No. 14/SEOJK.07/2014 on Confidentiality and Security of Consumer Data and/or Information lists sensitive data points requiring protection as they are often used to verify a customer's identity, such as the name of the customer's biological mother, customer's date of birth, address, etc.[115]

[113] Gazali, D., S. and Rachmadi, U., 2010, "Hukum Perbankan", *Sinar Grafika.* Jakarta, p. 30.

[114] Indonesian Banking Law No. 10/1998.

[115] OJK Letter No. 14/SEOJK.07/2014 on The Customer's Confidentiality and Data and/or Information Security.

Data Protection Regulations in Banking and Financial Services		
No.	Example(s) of Regulation	Key Point(s) on Data Protection
1	Indonesian Banking Law No. 10/1998	• Banks are required to protect the secrecy of all information related to their customers.
2	OJK Circular No. 14/ SEOJK.07/2014 on Confidentiality and Security of Customer Data and/or Information	• Considering the rapid adoption of technology in Indonesia's financial sector, these regulations emphasise the need to protect not only customers' financial data but also other information that can reveal a customer's identity (i.e., date of birth, name of user's biological mother, etc.).
3	OJK Regulation No. 77/ POJK.01/2016 on Lending Services based On Technology and Information	
4	OJK Regulation No. 13/ POJK.01/2018 on Digital Finance Innovation on Financial Sector	

Health Services

Data protection regulations in this sector have been primarily focused on protecting the medical records of a patient as classified information. Regulated in several laws, data protection in the health sector acknowledges the patient's right to manage their own data, because such medical records are confidential information that belongs to the said patient. However, Health Law No. 36/2009 does not impose any administrative or criminal penalties for medical record breaches and also does not provide any recovery mechanism for the patient if their medical record is compromised.[116] This creates a loophole in regard to law enforcement on data protection in the health sector.

Data Protection Regulation in Health Services

No.	Example(s) of Regulation	Key Point(s) on Data Protection	Loopholes
1	Law No. 36/2009 on Health	• Patient's medical records are classified as sensitive data and must be protected. • The patient has the right to manage their own medical records.[117]	• The law does not stipulate penalties against data breaches or a recovery mechanism for the patient if their medical records are leaked.

[116] *Indonesian Health Law No. 36/2009.*

Civil Administration

Data protection in this sector relies heavily on the state's capability to store and protect citizens' data. Law No. 23/2006 on Civil Administration regulates the state's rights and responsibilities to keep, treat, and protect the correctness of citizens' data.[118] However, as the law has gone through amendment processes several times, there are different definitions regarding which data should be "protected" and "classified" as "sensitive data".[119] For example, in the initial regulation, it is stated that the Personal & Family ID Number is categorised as sensitive data. However, in its next amendment (*Law No. 24/2013),* the ID Number is no longer classified as "sensitive data", and instead other data points such as fingerprint and retina data have been classified as "sensitive data".[120]

Since the state also executes a civil registration process that stores a large number of vital data points, Law No. 43/2009 on Records/Archive Management was issued to specify the retention period of any stored data or information as a period of ten to twenty-five years.[121]

[117] *Indonesian Health Law No. 36/2009.*

[118] Indonesian Law No. 23/2006 on Civil Administration.

[119] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan". *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

[120] Indonesian Law No. 24/2013 on the Amendment of the Indonesian Act No. 23/2006 on Resident Administration.

[121] Indonesian Law No. 43/2009 on Record Management.

[122] Law No. 43/2009 on Record Management.

Data Protection Regulations in Civil Administration

No.	Example(s) of Regulation	Key Point(s) on Data Protection	Loopholes
1	Law No. 23/2006 on Civil Administration	• The state has the responsibility to store and protect citizens' vital data. • Personal and Family ID Number, Date of Birth, Information on Physical Disability are some of the data points that are considered as sensitive data.	• Different definitions on which data is sensitive can create confusion for legal enforcement given multiple and differing definitions of vital data points within these regulations. • This problem stems from the obscurity of general data classification in Indonesia.
2	Law No. 24/2013 on the Amendment of Law No. 23/2006 on Civil Administration	• Information about Physical Disability, Fingerprint, Retina, and Personal Signature are some of the data points which are considered as sensitive data.	
3	Law No. 43/2009 on Records Management	• All data and information stored by the government have a 10 to 25-year retention period. After the retention period, the data can be "destroyed", or "opened to the public" if it does not contain any personal information.[122]	• Considering that data tends to be difficult to erase, this regulation has not provided precise mechanisms on how the data is being "destroyed" after it passes its maximum retention period.

Based on the explanations above, this study concludes two critical points about the landscape of data protection regulations in Indonesia. First, data protection regulations are still sector-based, where each sector has its own definition of data to be protected and subsequently, which information is to be classified as "sensitive". This occurs due to the lack of an overarching institutional regulation that governs data protection. Instead, responsibility is given to each sector's data regulator, which controls and defines these data mechanisms (i.e., Ministry of Home Affairs with civil registration data, OJK with financial and banking data, Ministry of Health with medical record data, etc.). MoCI, however, holds a more

significant responsibility because it has the Law on Electronic Information and Transaction or "*UU ITE*", which is regularly referenced by other data regulators when they are dealing with sensitive data (i.e., Indonesian Ministry of Trade relies on "*UU ITE*" to regulate trading in the electronic system).

Second, there are loopholes in the definition of data and information in each sector's regulations. For example, "*UU ITE*" requires electronic system managers to erase "irrelevant information" from their platform or database. But, this law does not provide details on the definition of "irrelevant information". This creates a potential conflict with other regulations, such as Law No. 14/2008 on Transparency of Public Information.

These loopholes can create further confusion during law enforcement. That said, this study highlights the need for Indonesia to have a general data protection regulation that provides a more comprehensive legal basis for the execution of a data management policy. It also highlights the need to have an independent and overarching regulatory body or commission to oversee the legal enforcement processes of data protection and regulation in Indonesia.

There is still plenty of room for improvement in personal data protection. The following sections will discuss how the government conceptualises personal data, explores the discourse on personal data protection, and outlines the roles of several key actors in the formulation of the draft personal data protection law.

Regulatory Approach to the Personal Data Protection Law

Data Conceptualisation by the Indonesian Government

As mentioned above, three regulations explicitly define personal data: Law No. 23/2006 on Civil Administration, MoCI Regulation No. 20/2016 on Personal Data Protection (PDP) in Electronic Systems, and Government Regulation No.71/2019 on the Implementation of Electronic Transactions and Systems. The first two define personal data as data on individuals that is stored, maintained, verified, and protected by the government. This definition, however, does not specify what counts as personal data. A broader definition can be found in the latter regulation, which defines personal data as any data regarding a person that can be used to identify an individual, whether directly or indirectly, by using electronic or non-electronic means.

This definition is also adopted in the draft PDP law, which is envisioned to be the umbrella regulation for existing regulations on data privacy. The draft puts personal data into two categories: general and specific data. General data includes name, gender, nationality, religion, and other data that if combined with other information can identify an individual. Specific data includes health-related information, biometrics, genetics, sexual orientation, political preferences, criminal records, children's data, financial data, and other data described in other existing regulations. However, the draft does not explicitly define what is sensitive data even though it is regarded as essential and requires more protection compared to general personal data.[123] In other contexts, for instance, European Union Data Protection Directive 1995, sensitive data is classified based on the level of harm or threat that might occur to the data owner should their data be accessed by

[123] Rosadi, S. D., and Pratama, G. G., 2018, "Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia", *Veritas, 4.*

irresponsible parties. The absence of a definition of sensitive data could potentially trigger multiple interpretations during the implementation phase.

Aside from the definition of personal data, the draft PDP law includes several concepts not stated in the existing sectoral regulations on data privacy. It adopts the concept of the right to be forgotten, meaning an individual can request data deletion.[124] Previously the erasure of an individual's personal data by operators of electronic systems can only occur based on a court order. The draft also incorporates the concepts and responsibilities of data controllers, data processors, types of personal data, data rights, data transfer, and requirements for data protection officers.[125]

MoCI highlights four main objectives of the PDP law.[126] First, to establish a comprehensive regulation to harmonise existing but scattered sectoral regulations.

[124] Zeller, B., Trakman, L., Walters, R., and Rosadi, S. D., 2019, "The Right to Be Forgotten – The EU and the Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)".

[125] Ministry of Communication and Informatics, 28 January 2020, *Presiden Serahkan Naskah RUU PDP ke DPR RI.* Available at https://www.kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-indonesia-akan-jadi-negara-asia-tenggara-kelima-yang-miliki-uu-pdp/0/siaran_pers. [Accessed 5 June 2020].

[126] Interview with Hendri Sasmitha Yuda, Head of Sub Directorate Personal Data Protection, The Ministry of Communication and Informatics, 18 June 2020.

This is critical in ensuring that the enforcement of data protection is standardised across all sectors. Second, to establish data security by preventing and addressing possible threats. This will raise awareness across sectors and obligate organisations to build secure data protection systems. Third, to accelerate the expansion of Indonesia's digital economy by building trust, transparency, and accountability among consumers, private organisations, and other stakeholders. Fourth, to regulate cross-border data flow. The draft law is ambitious and takes a comprehensive approach covering both the public and private domains.

Nevertheless, the formulation of the law encountered great challenges. Drafting was initiated in 2010, and yet the latest draft is still under review by the House of Representatives (*Dewan Perwakilan Rakyat* or DPR).[127] MoCI admits that there are challenges, such as getting agreement among ministries and government bodies to harmonise sectoral regulations, to ensuring that the law is enforced across all sectors. This is an attempt to balance personal data protection and digital innovation.

Discourses on Personal Data Protection and Rights over Data

The draft PDP law reflects strongly the General Data Protection Regulation (GDPR), which is already implemented in the European Union. According to MoCI, the GDPR is regarded as one of the most comprehensive data protection regulations in the world. The EU model treats privacy as a fundamental human right. This aligns with the Indonesian constitution. It also attempts to balance protecting these rights with the need to ensure the smooth functioning of the digital economy. MoCI claims to apply these principles to the draft law.

[127] Referring to http://www.dpr.go.id/uu/detail/id/353, the draft had been reviewed at the working meeting of Commission I with the Government (MoCI, The Ministry of Home Affairs, and The Ministry of Justice and Human Rights) on 25 February 2020. [Accessed 27 June 2020].

However, the draft law is not immune to criticism. There are at least three main issues with the law: 1) ambiguity of definitions, 2) inconsistency of data sovereignty, and 3) potential conflict of interest in the government in regard to citizens' data. First, concerning the definition, although the draft law attempts to define personal data, there are still potential discrepancies in interpretation due to the broad definition. For example, there are no specific rules on the use of "cookies".

Second, data sovereignty. President Joko Widodo has mentioned on many occasions that Indonesia must prioritise data sovereignty. However, the existing regulation does not reflect this statement. The amendment of PP PSTE 71, which allows data to be stored, processed, and managed outside of the Indonesian territory is deemed a threat to data sovereignty.[128] This is understandable as overseeing Indonesian citizens' data located in other countries is not a simple task. There are transborder laws and sovereignty issues that must be considered. As the debate is complex, MoCI has clarified that they have access to and can supervise the data. Moreover, the government is convinced that in this digital era, Indonesia must not rely on "analogue" regulations. This means that regulations on data management are more important than those on physical features, such as data centres.[129]

Third, the draft PDP law emphasises consent as a legal basis in collecting, storing and using data. Data processors must obtain consent from and notify the person involved before sharing or transferring their personal data.[130] Failing to do so risks the incurring of a jail sen-

[128] CNN Indonesia, 2019, "PP PSTE 'titipan asing' yang gadai kedaulatan data di Indonesia". Available at https://www.cnnindonesia.com/teknologi/20191108152910-185-446726/pp-pste-titipan-asing-yang-gadai-kedaulatan-data-indonesia. [Accessed 19 June 2020].

[129] Republika, 2019, "PP PSTE Jadi Bentuk Kedaulatan Data". Available at https://nasional.republika.co.id/berita/q1w1pt370/pp-pste-jadi-bentuk-kedaulatan-data. [Accessed 19 June 2020].

[130] Umali, T., 5 June 2019, "Indonesia drafts the Personal Data Protection Act", OpenGovAsia.com. Available at https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/. [Accessed 5 June 2020].

tence or fine. Aside from the issue of consent, the draft law also specifies that data owners have the right to: 1) know the purpose of data processing, 2) agree/disagree with having their data processed, 3) withdraw consent, 4) demand and receive compensation for violations of their data rights. It aims to empower data owners to not only decide how their data is collected, processed, and used, but also to exercise their rights.

Nevertheless, the draft law allows for exemption under five circumstances, namely: 1) in the interest of national defence and security, 2) when required by the judicial process according to regulations, 3) in the interest of the country, specifically economic or financial interests, 4) for the enforcement of a professional code of ethics, and 5) for aggregate data intended for statistical and scientific research. These exemptions are beneficial for government bodies or ministries, but there are concerns that they could give too much power to the government to access citizens' data.

Another concern regarding the current draft PDP law is the lack of discussion at the meta-level. This includes discussions on who should be able to control one's data and how data controllers should employ the data. This discussion is heating up, especially as regulations on data privacy are about to be implemented, but there is still a low level of understanding and awareness about data privacy. The likelihood of data exploitation is still high.

Concerns over Implementation

Aside from the challenges at the formulation stage, there are other challenges in ensuring compliance and enforcement. One concern is the response period requirement for data processors and data controllers. In the current draft, data processors are given 3 x 24 hours to terminate data processing and 2 x 24 hours to grant access to personal data should the data owner request it.

This timeframe is considered very short, and organisations might find it hard to meet this condition.[131] In comparison, the GDPR allows organisations to process similar requests within one month upon receiving the request. Malaysia's regulation provides 21 days' notice. Not every organisation has the ability or resources to adopt and comply with the regulation at short notice. Therefore, a transition period and a massive campaign are crucial. MoCI plans to apply a two-year transition period to enhance the knowledge of every stakeholder affected by this regulation.

Second, the government needs to issue technical guidelines for industries and other sectors as a follow-up to this law, after it is issued. Otherwise, there will be ambiguities. For instance, electronic system providers must employ standardised technology and certification for data protection.

Third, one of the most heated debates concerns the absence of an independent body charged with supervision and enforcement. This is crucial so as to avoid misuse and commercialisation by the government and to ensure compliance by all parties.[132] In many other countries, an independent supervisory body is tasked with receiving, investigating, and responding to complaints, providing advice, and raising public awareness over data privacy.[133]

Criticism arises as the absence of this independent body might trigger distrust from the public during enforcement. Furthermore, there is a potential conflict of interest as MoCI will have multiple roles as watchdog, data processor and data controller. MoCI argues that the decision not to have an independent supervisory body was taken for the sake of bureaucratic efficiency.

---

[131] Interview with anonymous, representing the private sector in Indonesia, 25 June 2020.

[132] Fauzan, R., 12 February 2020, "Pengamat: RUU Perlindungan Data Pribadi Masih Punya Kelemahan". *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20200212/101/1200621/pengamat-ruu-perlindungan-data-pribadi-masih-punya-kelemahan. [Accessed 5 June 2020].

[133] Ibid.

However, they are still open to considering the establishment of an implementing agency under the coordination of the government.

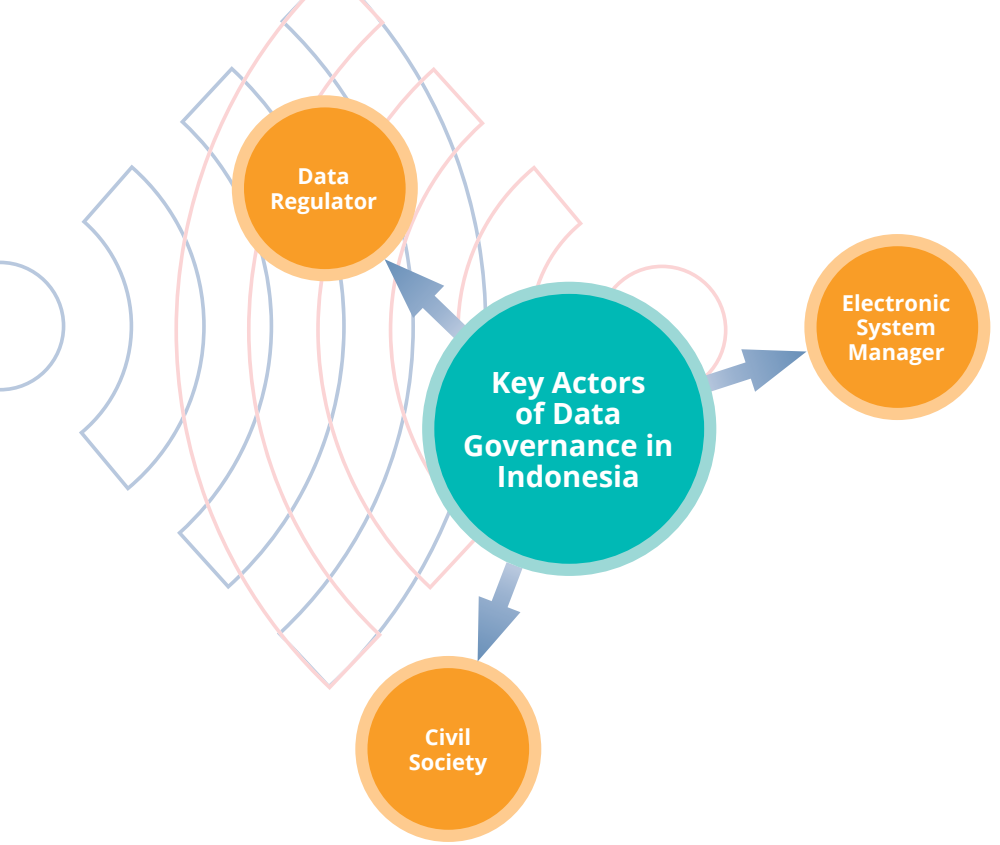
As the draft law adopts concepts from the GDPR, another issue is the readiness of stakeholders in terms of data governance and culture, technology, and human resources. The GDPR has been criticised for being difficult to implement. Indonesia's draft PDP law requires organisations to apply strict data governance within each organisation, but not every sector has a standard data protection policy in place. In Indonesia's case, only the banking and financial sector already practises a data protection policy.[134] The draft law also orders organisations to appoint a data protection officer (DPO) within the organisation. However, the availability of qualified DPOs has been questioned. In practical terms, the relevant ministry also needs to issue a national work competency standard (NWCS) to ensure the effectiveness of DPOs.

The government also needs to take awareness of data privacy into account. One of the main objectives of the law is to guarantee the rights of citizens as data owners. Nevertheless, enforcement of this law will be ineffective if data owners are not fully aware of their rights. Therefore, it is necessary to build up digital literacy on data privacy through public education.

Key Actors of Data Governance in Indonesia

The formulation of the draft PDP law, as well as its subsequent implementation and enforcement, is highly related to the actors who are involved in data governance. This section analyses the key actors of data governance in Indonesia based on their contributions and interests in the formulation of the draft PDP law.

[134] Interview with Novel Ariyadi, a cybersecurity practitioner, 19 June 2020.



Data Regulator

The data regulator regulates activities related to the use of personal data. It consists of the executive branch and the legislative branch. The relationship between these two branches is arguably less turbulent, and on many occasions, the spokesperson of each institution has stated that they are working together harmoniously. However, there are three critical issues that arose:

1. Formation of a data protection body
2. Location of the data centre
3. Data sharing with the private sector

As the draft law looks to the GDPR as a model, the urgency to have a data protection body might be based on the practice in European countries. For example, the United Kingdom has established the Information Commissioner's Office (ICO), an independent body to ensure

the fulfilment of UK citizens' information rights. A critical feature of this body is its impartiality, which allows it to operate in a more neutral stance. In Indonesia's case, whether the body should be entirely independent or under the structure of a government institution is still being debated. MoCI presented a plan to establish such a body without elaborating on the partiality of the body.

The responses of lawmakers in the House of Representatives vary. In 2019, a member of the House stated that establishing a new body would be costly.[135] In the following year, another member of the House endorsed the plan, adding that an independent body was needed to prevent the government from misusing the authority.[136] The debate on whether there should be an independent data protection body reflects different standpoints between the executive and legislative branches. According to the director of TIFA Foundation, Shita Laksmi, a dedicated body should be established.[137] However, she added that it was unlikely for an independent body to be established separate from the government due to the government's reluctance to fund an organisation that was not under its overview. Despite the debate, the latest progress signals that a dedicated body will be created when the law is issued.

The location of the data centre is another important issue. In 2018, the then Minister of ICT, Rudiantara, argued that the data centre did not have to be located in Indonesia.[138] He added that a data centre located in Indonesia was only essential for storing personal data. Other data could be stored in a cloud server. A member

[135] Annur, C. M., 2019, "DPR Kritik Ide Pembentukan Lembaga Perlindungan Data Pribadi", *Katadata.* Available at https://katadata.co.id/berita/2019/07/18/dpr-kritik-ide-pembentukan-lembaga-perlindungan-data-pribadi. [Accessed 5 June 2020].

[136] Burhan, F. A., 2020, "Cegah Pemerintah Salah Gunakan Data Pribadi, DPR Minta Lembaga Khusus", *Katadata.* Available at https://katadata.co.id/berita/2020/02/25/cegah-pemerintah-salahgunakan-data-pribadi-dpr-minta-lembaga-khusus. [Accessed 5 June 2020].

[137] Interview with Shita Laksmi.

[138] Kominfo, 2018, *Rudiantara Sebut Data Center Tak Perlu di Indonesia.* Available at https://kominfo.go.id/content/detail/14742/rudiantara-sebut-data-center-tak-perlu-di-indonesia/0/sorotan_media. [Accessed 30 June 2020].

of the House agreed and argued that only data with high confidentiality should be stored in a data centre in Indonesia.[139] A year after, the stance of both institutions has changed. When the Electronic Transaction Law was established in late 2019, social media platforms operating in Indonesia were required to have a data centre in Indonesia. Both branches agreed on this issue.

The third key debate is on whether data should be shared between government institutions and the private sector. The Ministry of Home Affairs stated that they were sharing Indonesian citizens' personal information with 1,227 private institutions.[140] The objective of this initiative was to ease the use of digital technology, by cutting procedural requirements when signing up for a digital service. The House responded to the initiative by disregarding the ministry's decision, arguing that it would compromise the security of personal data.[141] The debate between the ministry and the House on this issue does not change the state of data sharing by the Ministry of Home Affairs with the private sector.

A more detailed description of key actors and their interests in data governance in Indonesia is as follows:

[139] OkeNews, 2018, *Evita Nursanty: Pusat Data dengan Tingkat Confidentiality Tinggi Wajib Berada di Indonesiatara Sebut Data Center Tak Perlu di Indonesia.* Available at https://nasional.okezone.com/read/2018/10/01/337/1958125/evita-nursanty-pusat-data-dengan-tingkat-confidentiality-tinggi-wajib-berada-di-indonesia. [Accessed 30 June 2020].

[140] Damarjati, D., 2019, "Kemendagri: 1.227 Lembaga Bisa Akses Data Penduduk, Termasuk Swasta", *DetikNews.* Available at https://news.detik.com/berita/d-4634210/kemendagri-1227-lembaga-bisa-akses-data-penduduk-termasuk-swasta. [Accessed 5 June 2020].

[141] Astuti, N. A. R., 2019, "Komisi II DPR Tak Setuju Dukcapil Beri Akses Data Penduduk ke Swasta", *DetikNews.* Available at https://news.detik.com/berita/d-4635216/komisi-ii-dpr-tak-setuju-dukcapil-beri-akses-data-penduduk-ke-swasta. [Accessed 30 June 2020].

Data Regulator Key Actors.

Branch	Key Actors	Interests and Roles
Executive Branch	Ministry of Communications and Informatics (MoCI)	• **Key actor** in the formulation of the law: ◦ The Directorate General of ICT Applications is in charge of overseeing companies, to ensure the security of their electronic system/platform.[142] ◦ Appointed by the president to lead the issue. • **Notable stance** in the formulation of the law: ◦ MoCI suggested establishing a Personal Data Protection Body.[143] ◦ MoCI used the EU's General Data Protection Regulation (GDPR) as a benchmark.[144] ◦ MoCI argued that the government would appoint a third-party data officer.[145] • The formulation of the law is mainly maintained by the Sub-Directorate of Personal Data Protection Governance.[146]

[142] See Direktorat Aplikasi dan Informatika, n.d., *Tugas dan Fungsi Direktorat Jenderal Aplikasi dan Informatika.* Available at https://aptika.kominfo.go.id/profile/tugas-danfungsi/#:~: text=Tugas%20Pokok,di%20bidang%20penatakelolaan%20aplikasi%20informatika. [Accessed 5 June 2020].

[143] Annur, 2019.

[144] Fauzan, R., 2020, "RUU Perlindungan Data Pribadi Gunakan GDPR Uni Eropa Sebagai Acuan", *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20191202/282/1176768/ruu-perlindungan-data-pribadi-gunakangdpr-uni-eropa-sebagai-acuan. [Accessed 5 June 2020].

[145] Fauzan, R., 2020, "Pelaku Dagang-el Soroti Salah Satu Ketentuan UU Perlindungan Data Pribadi", *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20200304/266/1209168/pelaku-dagang-el-sorotisalah-satu-ketentuan-uu-perlindungan-data-pribadi. [Accessed 30 June 2020].

[146] See Kementerian Komunikasi dan Informatika, n.d., *Struktur Organisasi.* Available at https://aptika.kominfo.go.id/profil/struktur-organisasi/. [Accessed 4 June 2020].

Branch	Key Actors	Interests and Roles
	Ministry of Law and Human Rights	• **Key actor** in the formulation of the law: ◦ The Ministry of Law and Human Rights has been appointed by the president to lead the issue. ◦ The Directorate General of Laws and Regulations oversees the harmonisation of overlapping regulations in each government sector.[147] • **Notable stance** in the formulation of the law: ◦ The interest of the Ministry of Law and Human Rights is to protect the data sovereignty of Indonesian digital platform users. • The formulation of the law is mainly maintained by the Directorate of Law and Regulation Harmonisation II.[148]
	Ministry of Internal Affairs	• **Key actor** in the formulation of the law: ◦ The Ministry of Home Affairs has been appointed by the president to take charge of the issue. ◦ The Directorate General of Demography and Civil Registrations is responsible for protecting the collected personal data of Indonesian citizens.[149] • **Notable stance** in the formulation of the law: ◦ Cooperating with 1,227 institutions, including private companies, to share the personal data held by the Civil Registration Agency or Dukcapil (from e-KTP or electronic ID cards).[150] • The formulation of the draft PDP law is mainly maintained by the Directorate General of Demography and Civil Registration.[151]

[147] See Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, n.d., *Direktorat Harmonisasi Peraturan Perundang-undangan II.* Available at http://ditjenpp.kemenkumham.go.id/struktur-djpp/ditharmonisasi.html. [Accessed 11 July 2020].

[148] Ibid.

[149] See Kementerian Dalam Negeri, n.d., *Struktur Organisasi.* Available at https://www.kemendagri.go.id/page/read/7/struktur-organisasi. [Accessed 11 July 2020].

[150] Damarjati, 2019.

[151] See Kementerian Dalam Negeri, n.d.

Branch	Key Actors	Interests and Roles
	National Cyber and Cryptic Body (BSSN)	• **Notable stance** in the formulation of the law: ◦ Endorsing the government to establish the law.[152] ◦ Arguing that the law does not necessarily talk about protecting society from surveillance, but rather about misuse of data in online lending and electronic transactions.[153]
Legislative Branch	Commission I, Indonesian House of Representatives (DPR)	• **Notable stance** in the formulation of the law: ◦ Commission I member Satya criticised the government's plan to establish a Data Protection Body as being "financially costly".[154] ◦ Commission I member Yan endorsed the government's plan to establish a Data Protection Body to avoid abuse of power by the government.[155] ◦ Chairwoman of Commission I Meutya Hafid stated that "the law would cover obligations for companies to build data centres in Indonesia".[156]

Source: author.

Aside from the four government institutions in the executive branch, there are other ministries involved in the formulation of the draft law: Ministry of Commerce, Ministry of Finance, Ministry of Health, Ministry of En-

[152] Kartika, M., 2019, "BSSN Dukung RUU Perlindungan Data Pribadi Segera Disahkan", *Republika.* Available at https://republika.co.id/berita/q1zhdy428/bssn-dukung-ruu-perlindungan-data-pribadi-segera-disahkan. [Accessed 5 June 2020].

[153] CNN Indonesia, 2019, *BSSN Tanggapi Penyadapan Tanpa UU Perlindungan Data Pribadi.* Available at https://www.cnnindonesia.com/teknologi/20190812183821-185-420671/bssn-tanggapi-penyadapan-tanpa-uuperlindungan-data-pribadi. [Accessed 5 June 2020].

[154] Annur, 2019.

[155] Burhan, 2020, "Cegah Pemerintah Salahgunakan Data Pribadi", DPR Minta Lembaga Khusus.

[156] Gatra, 2020, *RUU Data Pribadi Akan Atur Pusat Data hingga Rekaman CCTV.* Available at https://www.gatra.com/detail/news/471976/politik/ruu-data-pribadi-akan-atur-pusat-data-hingga-rekaman-cctv-. [Accessed 5 June 2020].

ergy and Mineral Resource. Previously, other ministries that have sectoral regulations on data protection were involved.[157] However, according to the representative of the Ministry of ICT, Hendri Sasmita Yuda, currently, these ministries tend to be involved only during consultative sessions held by the ministry.[158]

Electronic System Manager

The electronic system manager can be defined as any organisation that collects, processes, and stores information from citizens or users. The key actors in this category range from government institutions to non-government institutions: e-commerce, social media companies, and other technology industries, ministerial bodies, national commissions, and so forth. Electronic system managers are the first to be scrutinised whenever an incident takes place given that they are the owner and manager of the electronic system.

Each key actor influences the formulation of the law differently. For private companies, they advocate their interests in two ways: collectively through interest groups/business associations, and individually through self-representation. They usually provide suggestions to the data regulator through public interviews/events to show their interests indirectly, or through a private dialogue with the government to convey their interests directly.

Government institutions that manage electronic systems in their operations do not necessarily have a strong public stance in the formulation of the law, other than that they are supporting it. As there is not much of the government's stance to investigate further, this section will focus on the interests and roles of private sector key actors as electronic system managers.

[157] Government and ministerial regulations are, by structure, positioned lower than a law.

[158] Interview with Hendri Sasmita Yuda from the Ministry of ICT.

The key actors from the private sector and their interests are as follows:

Electronic System Manager Key Actors.

Advocacy Method	Key Actors	Interests and Roles
Collective, by public statements	Asosiasi Cloud Computing Indonesia (ACCI)	• ACCI is an association of cloud computing companies in Indonesia. • **Notable stance** in the formulation of the law: ◦ ACCI advocated for data sovereignty, i.e., that data servers are to be located in Indonesia.[159] ◦ ACCI pushed MoCI to hold e-commerce companies accountable for data breaches, based on PP 71/2019.[160]
Collective, by direct consultation	Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI)	• AFPI is an association that manages Fintech Peer to Peer (P2P) Lending or Fintech Online Funding sector in Indonesia.[161] • Acknowledged by the Financial Services Authority (OJK) as an official association of IT-based lending and borrowing service providers in Indonesia, according to the letter No. S-5 / D.05 / 2019.[162] • **Notable stance** in the formulation of the law: ◦ AFPI endorsed the formulation of the law as it promotes trust among financial technology users.[163]

[159] Setyowati, D., 2019, "Pelaku Industri Telekomunikasi Minta Pusat Data Wajib Ada di Indonesia", *Katadata.* Available at https://katadata.co.id/berita/2019/02/06/pelaku-industri-telekomunikasi-minta-pusat-data-wajibada-di-indonesia. [Accessed 5 June 2020].

[160] CNN Indonesia, 2020, *Kominfo Didesak Sanksi Tokopedia dan Bhinneka soal Akun Bocor.* Available at https://www.cnnindonesia.com/teknologi/20200512165045-185-502615/kominfo-didesak-sanksi-tokopediadan-bhinneka-soal-akun-bocor. [Accessed 4 June 2020].

[161] AFPI, n.d., *About.* Available at https://afpi.or.id/en/about. [Accessed 30 June 2020].

[162] Ibid.

[163] Burhan, F. A., 2020, "Asosiasi Bahas UU Fintech hingga Data Pengguna di Istana", *KataData.* Available at https://katadata.co.id/berita/2020/01/24/asosiasi-bahas-uu-fintech-hingga-data-pengguna-di-istana. [Accessed 30 June 2020].

Advocacy Method	Key Actors	Interests and Roles
Collective, by public statements	Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)	• APJII is an association of Indonesian internet service providers. • **Notable stance** in the formulation of the law: ◦ APJII urged for the law to be enacted as soon as possible, to protect the personal data of Indonesian citizens.[164]
Collective, by public statements	Asosiasi Big Data dan AI (ABDI)	• ABDI is an association of technology companies that deal with data technology, data analytics, data controllers, and data science. • **Notable stance** in the formulation of the law: ◦ ABDI stated that it would participate in the discussion on the law and other policies that relate to the state of the big data industry.[165] ◦ ABDI commented on PP 71/2019 that the data centre should be located in Indonesia.[166]

[164] Buletin APJII, 2019, "Perlindungan Data Pribadi Mutlak Diperlukan", *APJII.* Available at https://blog.apjii.or.id/index.php/2019/08/20/perlindungan-data-pribadi-mutlak-diperlukan/. [Accessed 30 June 2020].

[165] See ABDI, n.d., *About.* Available at https://www.abdi.id/tentang-abdi/. [Accessed 30 June 2020].

[166] Kamaliah, A. Kata Asosiasi Soal Data Center Tak Harus di Indonesia, *DetikInet.* Available at https://inet.detik.com/law-and-policy/d-4775013/kata-asosiasi-soal-data-center-tak-harus-di-indonesia. [Accessed 5 June 2020].

Advocacy Method	Key Actors	Interests and Roles
Collective, by public statements	Indonesian e-Commerce Association (iDEA)	• E-commerce companies are the most-targeted actor when a data breach takes place. • Some e-commerce companies whose users' data have been compromised include: Tokopedia, Bukalapak and Bhinneka. • iDEA is an association of e-commerce companies in Indonesia. • **Notable stance** in the formulation of the law: ◦ iDEA admitted to the use of personal data to track consumer behaviour in e-commerce.[167] ◦ iDEA stated that they have not been invited by the government to participate in discussions on the law.[168]
Individuals	Technology and Social Media Companies	• Technology and social media companies are rather off-the-grid in the discussion on the law. • Some technology and social media companies related to the discussion are Facebook and Google. • **Notable stance** in the formulation of the law: ◦ Facebook and Google agreed to build data centres in Indonesia with an arrangement on the protocol of data transfers.[169]

Source: author.

[167] CNN Indonesia, 2018, *idEA Akui Jejak Data Pribadi Untuk Baca Perilaku.* Available at https://www.cnnindonesia.com/teknologi/20181025185542-185-341482/idea-akui-jejak-data-pribadi-untuk-baca-perilaku. [Accessed 30 June 2020].

[168] Burhan, 2020, "Asosiasi Bahas UU Fintech hingga Data Pengguna di Istana".

[169] Ihsannudin, 2019, "Menkominfo: Google dan Facebook Berencana Bangun Pusat Data di Indonesia", *Kompas.* Available at https://nasional.kompas.com/read/2019/12/06/09533131/menkominfo-google-danfacebook-berencana-bangun-pusat-data-di-indonesia. [Accessed 30 June 2020].

Concluding from the summary above, all key actors in the electronic system manager category support the formulation of the law. They are confident that the law will provide a more secure ecosystem for their businesses. However, their stances on the law's specific contents vary. Local cloud computing companies tend to push for the data server location to be in Indonesia. On many occasions, ABDI and ACCI advocated this agenda. They argue that to preserve data sovereignty, it is crucial to keep the physical server in the local area. However, according to Indonesian IT expert Tony Seno Hartono, this does not necessarily resonate with reality. In an interview with Center for Digital Society (CfDS), Hartono argued that the location of a data server was only one of three points required to ensure data sovereignty.[170] The other two are the state of data privacy and data security.

Conceptually, data privacy means data should only be visible to authorised users. Data security, on the other hand, involves security measures embedded in the data to ensure its confidentiality, integrity, and accessibility. Tony further mentioned that in a cloud computing ecosystem where data was stored in the cloud, the state of data privacy and security defined the matter more than the location of the server.

Civil Society

Civil society consists of non-government and non-profit organisations and academia that focus on advocating for better data governance. It constantly scrutinises the performance of data regulators in protecting the digital rights of users, as well as urges electronic system managers to increase the security of their platforms.

There is mixed information on which specific civil society organisations were involved in the formulation of the law. Based on interviews with several civil society representatives, data regulators have not been inviting civil society organisations for consultation during

[170] Interview with Tony Seno Hartono.

the formulation of the law. However, a government representative stated that the data regulator had been consulting with civil society organisations. Given this contradictory information, communication between the civil society and data regulators may have been informal. Several civil society organisations have publicly supported the law.

The detailed key actors and their interests are as follows:

Civil Society Key Actors.

Sub-Category	Key Actors	Interests and Roles
Civil Society Organisation	Southeast Asia Freedom of Expression Network (SAFEnet)	• SAFEnet is a civil society organisation focusing on the fulfilment of right to access information, right to expression, and right to feel safe. • **Notable stance** in the formulation of the law: ◦ Director of SAFEnet Damar Juniarto stated that: (1) the government has to protect personal data, not only data that are prone to be bought and sold, but also those that are life-threatening; (2) the government should establish the law quickly; (3) the law would create a more sovereign Indonesia.[171]
Civil Society Organisation	ICT Watch	• ICT Watch is a civil society organisation that aims to develop Indonesia's human capital for digital literacy, online speech, and cyber governance.[172] • **Notable stance** in the formulation of the law: ◦ Urges the government to establish the law soon.[173]

[171] CNN Indonesia, 2019, *SAFE Net Respons Pidato Jokowi soal Perlindungan Data Pribadi.* Available at https://www.cnnindonesia.com/teknologi/20190816203213-185-422140/safe-net-respons-pidato-jokowi-soalp-erlindungan-data-pribadi. [Accessed 5 June 2020].

[172] Rizkinaswara L., 2019, "ICT Watch", *Aptika Kominfo.* Available at https://aptika.kominfo.go.id/2019/07/ictwatch/. [Accessed 30 June 2020].

[173] Damar, A. M., 2019, "ICT Watch Desak Pemerintah Segera Sahkan UU Perlindungan Data Pribadi", *Liputan6.* Available at https://www.liputan6.com/tekno/read/4027861/ict-watch-desak-pemerintah-segerasahkan-uu-perlindungan-data-pribadi. [Accessed 5 June 2020].

Sub-Category	Key Actors	Interests and Roles
Civil Society Organisation	Indonesia Cyber Security Forum (ICSF)	• ICSF is a community of cybersecurity professionals and experts. • **Notable stance** in the formulation of the law: ◦ ICSF suggested that the data regulator establish an independent Personal Data Protection Body.[174]
Academia	Institute for Policy Research and Advocacy (ELSAM)	• ELSAM is a human rights organisation that focuses on establishing a democratic political system in Indonesia by promoting civil society activism and protection of human rights. • **Notable stance** in the formulation of the law: ◦ ELSAM suggested that the data regulator establish an independent Personal Data Protection Body.[175] ◦ ELSAM asked the government, specifically the Ministry of Home Affairs, to not hand over personal data to any institution without the permission of the data owner.[176] ◦ ELSAM criticised the government for not providing an option for users to delete their accounts.[177]

Source: author.

[174] Fauzan, R., 2020, "Pengamat: RUU Perlindungan Data Pribadi Masih Punya Kelemahan", *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20200212/101/1200621/pengamat-ruu-perlindungan-data-pribadi-masih-punya-kelemahan. [Accessed 5 June 2020].

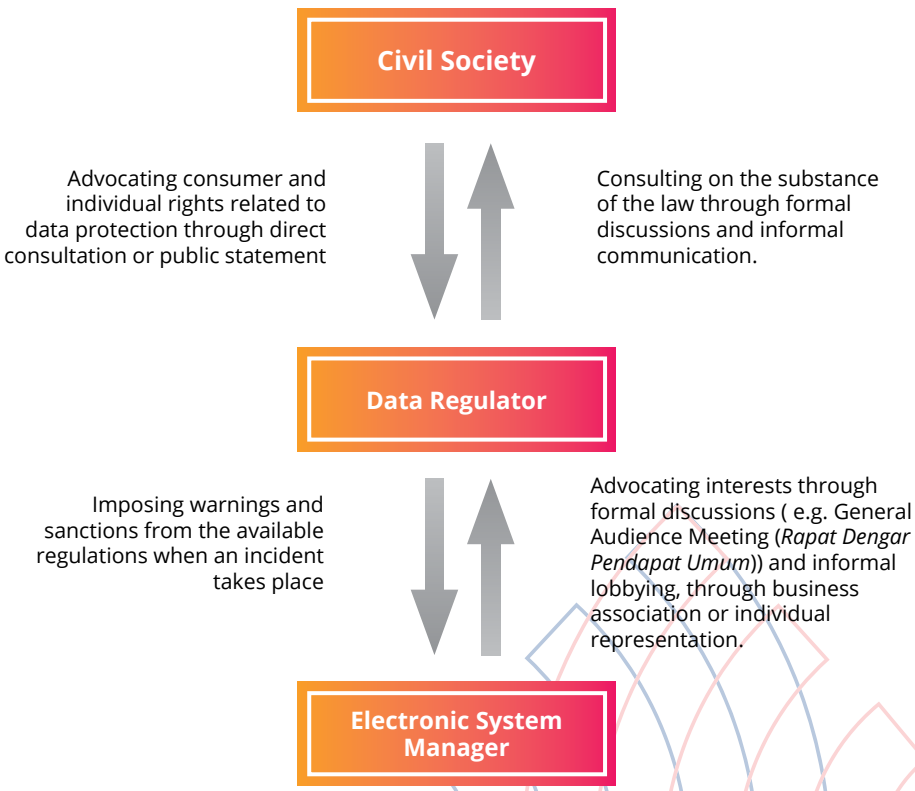
[175] Pertiwi, W. K., 2020, "ELSAM: Harus Ada Pengawas UU PDP di Luar Pemerintah", *Kompas.* Available at https://tekno.kompas.com/read/2020/01/31/12580067/elsam--harus-ada-pengawas-uu-pdp-di-luarpemerintah?page=all. [Accessed 5 June 2020].

[176] Ristianto, C., 2020, "Kemendagri Diminta Kaji Ulang Kerja Sama Data Kependudukan", *Kompas.* Available at https://nasional.kompas.com/read/2019/08/02/13161321/kemendagri-diminta-kaji-ulang-kerja-sama-datakependudukan. [Accessed 5 June 2020].

[177] Kumparan, 2020, *Regulasi Tokopedia Larang Pengguna Hapus Akun, Langgar Hak Data Pribadi.* Available at https://kumparan.com/kumparan-news/regulasi-tokopedia-larang-pengguna-hapus-akun-langgar-hak-datapribadi-1tNCp40Q9au. [Accessed 5 June 2020].

Other than said institutions, MoCI staff Hendri Sasmita Yuda also mentioned that there were members of civil society consulted by the ministry in formulating the law: e.g., experts from notable institutions, namely Gadjah Mada University, University of Indonesia, and Diponegoro University. They were invited to both formal and informal discussions held by MoCI or MoCI staff. However, further public information on the involvement of these key actors is not available.

Relationship between Actors



The highlight of the data governance discourse in Indonesia is the formulation of the PDP law. This is due to the current situation, where data regulation is still dispersed in many sectoral regulations, and enforcement is lacking.

The roles and interests of key actors are concluded as follow:

1. Data regulators, electronic system managers, and civil society form relations centred on the data regulator as it holds the authority in formulating the law. Civil society and electronic system managers hold advocacy roles as they are provided with formal and informal communication channels during consultations with the data regulator.

2. The key actors among data regulators (three ministries and the House of Representatives) seem aligned in their desire to establish the law. However, debates emerged concerning the formation of a data protection body, the location of the data centre, and the sharing of data with the private sector.

3. The key actors in electronic system managers support the general idea of the law. Private actors raised concerns more vocally compared to other types of key actors. However, each private actor has its unique concerns on the substance of the law, depending on the interests of the business entity or the association.

4. Civil society key actors insist on the formulation of the law as soon as possible. However, each key actor channels its interests differently. There are two ways for civil society organisations and academia to advocate their concerns: giving public statements and conducting direct consultation with the data regulator. The issues of concern raised by civil society key actors are the formation of an independent data protection body, intersectoral data sharing, and options provided by electronic system managers for their users to delete their accounts.

Conclusion for Indonesia

This chapter is meant to provide an overview of data protection regulations in Indonesia and to highlight the urgency in adopting an overarching data protection regulation in the form of a PDP law, currently being reviewed by lawmakers. The EU's GDPR has been the main source of inspiration for Indonesia's draft PDP law.

The urgency to create an overarching data protection regulation stems from four problems: 1) the public's low level of awareness and knowledge about data privacy despite the high number of internet users and digital activities; 2) the growing digital economy, the growth of which is hindered by the lack of a data protection regulation; 3) several cases of data breach showed that Indonesia's digital ecosystem is susceptible to digital crimes and without the appropriate regulations, legal prosecution of the crimes would be difficult; 4) intense political pressures that built up during the drafting for the PDP law.

Data protection is currently governed through a disjointed, sectoral approach. Five sectors are most relevant to data protection: 1) The telecommunication and informatics sector focuses on data confidentiality. MoCI has expanded this to cover digital data through regulations such as "*UU ITE*" and *Permenkominfo No. 20/2016*. 2) The trade and commerce sector is still heavily reliant on regulations from the telecommunications and informatics sector, despite the growth of digital economy activities. 3) The banking and financial services sector focuses on customer data confidentiality, and this is bolstered by several banking regulations on the level of data protection required. 4) The health sector does not have any regulation that clearly lays down sanctions if a medical record leakage occurs, despite the classification of medical records as data that needs to be protected. Lastly, 5) the civil administration sector regulates protection and storage of citizens' data.

The definition of personal data was explained in Government Regulation No.71/2019 and adopted in the draft PDP law. The proposed PDP law itself is meant to

be the overarching regulation on data privacy. MoCI explained that the law is meant to harmonise sectoral regulations, enact preventive measures against data-related crimes, accelerate the growth of Indonesia's digital economy, and regulate cross-border data flow.

Despite the urgency of adopting this regulation, this law is still under legislative review. Several noteworthy issues regarding the draft PDP law are: the formation of a data protection body, location of the data centre, and whether the government should share Indonesians' public information with the private sector. While the first two issues have been resolved, the last issue is still outstanding.

Other challenges that have hindered the adoption of this law are: concerns on compliance and enforcement. These include: the short timeframe given to data processors and data controllers, lack of technical guidelines, lack of an independent supervising body, low level of readiness of stakeholders with respect to data protection regulations, and lack of awareness of data privacy among data owners. Among the most contentious drawbacks of the draft law is the absence of an independent supervisory body.

There are three key actors in data governance: data regulators, electronic system managers, and civil society. Data regulators, which regulate the usage of personal data, can be divided into the executive branch and the legislative branch. The executive branch consists of

MoCI, Ministry of Law and Human Rights, Ministry of Home Affairs, and the National Cyber and Cryptic Body (BSSN), each with different focus and responsibility in regard to data protection.

There is a wide range of actors that could be identified as electronic system managers. It could be any public or private organisation that uses its users' data. Private sector key actors tend to have more inputs to give than their government counterparts, and they provide such inputs collectively through trade associations. Individual technology and social media companies tend to be less engaged in public conversations about the law. All key actors generally support the law, but there are still contending views on specific contents.

Civil society organisations are usually more critical towards data regulators. Data regulators said that they have consulted civil society organisations in the formulation of the law, but several civil society organisations have said that they have not been consulted.

Current Implementation Challenges

The implementation of better data governance in Indonesia is challenged by three main factors: 1) the state's low capacity to establish a robust regulation, 2) the low level of compliance among Indonesian citizens, and 3) other major events that divert attention from the data regulation process. Personal data protection is currently governed through multiple, disjointed sectoral regulations, hindering the process of data governance, and making it difficult to adopt intersectoral standards in governing data.

The issue also stems from a low level of awareness on data protection among citizens. Due to poor digital literacy, many Indonesians lack awareness on what personal information they can safely share and with whom they can share this with. Data protection may not be an immediate concern for many Indonesians, resulting in less political urgency for the policymakers. This lack of digital literacy could also potentially reduce the

effectiveness of the PDP law, should it be established. Therefore, there is a critical need to establish technical guidelines and campaigns to assist individuals and small and medium-sized enterprises in understanding and complying with the law.

Lastly, Indonesia, as with many other countries, is facing challenging conditions related to the Covid-19 pandemic. The government is under pressure to show better responsiveness in handling the pandemic. With the number of cases continuing to rise, the recent adoption of the controversial "Job Creation Law" has taken the spotlight as a massive number of students and activists rallied in the streets to demand its cancellation. Among the many issues that the country is currently facing, personal data protection is seen as being less urgent. Although discussions on the draft PDP law by the House of Representatives and the government is ongoing, it is difficult to foresee an immediate adoption of the law. Despite major incidents of personal data breaches involving e-commerce platforms and government institutions, the issue does not seem to be gaining much public attention. Therefore there is a need for policymakers to do more to attract public attention to this issue.

Comparing Data Governance – India and Indonesia

Having reviewed the data protection regulations in India and Indonesia, we now turn to a comparative analysis of the two countries.

Rising Internet Penetration

Internet use is rising in both countries. More and more citizens are getting online and using the internet to manage their lives and livelihoods. Like citizens of developed countries, Indian and Indonesian citizens are increasingly using the internet through mobile platforms, which has given much space to domestic and foreign technology firms to create apps that serve specific market needs and wants. In 2018, nearly 65% of Indonesians, or roughly 172 million people, were online. Among the 65%, almost 95% use social media. Numbers are equally high in India and increasing by the year. In 2014, India had 239 million internet users; this rose exponentially to 560 million in 2018.

Thriving Digital Economies

Both countries have thriving digital economies, with firms producing applications and services used by their respective populations to communicate, transact, and

engage in e-commerce. Increasingly, a slew of economic activities in areas like healthcare, education, entertainment, and retail commerce require and use digital information and knowledge as factors of production. In 2015, Indonesia's digital economy was valued at USD8 billion, and in just five years, the digital economy grew fivefold to nearly USD40 billion in 2019. It is estimated that this valuation will rise to USD150 billion in 2025. India's digital economy, comprising different sectors like IT, electronics, and manufacturing, constitute roughly 7% of India's GDP in 2018 or USD200 billion. By 2025, India's digital economy's value is expected to be USD435 billion, more than twice the current amount.

Sectoral Data Governance

Both countries are looking to adopt comprehensive legislation to regulate data. In Indonesia, the lack of a national law and regulatory authority to supervise and administer data-related issues and conflicts has led to sectoral rules that protect citizens' and users' personal information. Personal data in Indonesia is currently governed by at least 30 different regulations issued by various government agencies. Each of these sectors has specific definitions of data and how it should be handled and by whom. The fragmented data landscape creates confusion for firms and citizens who have to adhere to different standards. That said, data matters are governed by the Electronic Information and Transactions Law (EITL), which is supplemented by two regulations – Government Regulation No. 71 of 2019 regarding Provisions of Electronic Systems and Transactions (GR 71) and Minister of Communications & Informatics Regulation No. 20 regarding Protection of Personal Data in Electronic System (PDP Regulation).

In India, the Information Technology Act (2000) governs cyberspace issues, including cybercrime, social media platforms, etc. The provisions of the IT Act also cover data-related matters, specifically regarding the protection of personal data. Specific provisions that cover sensitive personal information or data (SPDI) mandate

that companies have privacy policies, require consent be obtained when collecting or transferring personal information, and inform those from whom data is collected. SPDI rules also place obligations on all entities located in India that process personal information on behalf of individuals. In India, certain regulators do have specific rules to manage how firms and other organisations handle personal information they collect. For example, the Reserve Bank of India has specific regulations that affect payment data. All user data collected within Indian borders will have to be localised so that the RBI can access this data. India's telecom authority (TRAI) has guidelines on protecting personal data. Other industries and sectors are governed by the IT Act, similar to Indonesia's ETIL, which sets broad rules on how firms must protect personal information gathered in different ways. The inadequacies of the IT Act and demands posed by rising digitisation and volumes of data collected has compelled New Delhi to devise a new comprehensive law that addresses existing gaps.

Pressures to Regulate Data

Pressures to regulate data emanate from different sources. In Indonesia, the need to protect citizens' data, as they transact with services online, emanates out of the potential for data leaks that result in personal data being compromised, including sensitive personal information. Security gaps concerning digital platforms have contributed to data being misused or compromised. Data protection is connected to growing concerns around cybersecurity. Though problems related to cybercrime are relevant in India, they have not featured in discussions around data. Pressures to protect the personal information of Indian citizens emerge from constitutional discussions tied to privacy, which was enshrined as a right under India's constitution in 2017. Aadhaar, India's biometric database, has sensitised Indian citizens to the importance of personal information that could be deployed for public and private ends.

Defining Data

How the proposed laws define data in both countries reveals how policymakers conceptualise data and seek to regulate it. The draft Indonesian law classifies personal data as either general data or specific data. General data includes personal information like name, gender, religion, and nationality that identify an individual. In contrast, specific data covers ostensibly sensitive information like sexual orientation, health condition, political preferences, financial records, etc. The draft personal data protection bill breaks down data into three categories: personal data or information that can identify an individual; specific data, which includes sensitive information, such as health-related data, biometrics, genetics, sexual orientation, political preferences, criminal records, children's data, financial data, etc. The draft does not explicitly define sensitive data although it is regarded as essential and requires more protection compared to "general" personal data.

Several categories of data exist in India. The first is personal data or information related to an individual, which could be used to identify them. Sensitive personal data refers to sensitive information like financial data, health data, sexual orientation, genetic data, biometric data, religious beliefs, caste or tribe, etc. The original bill's data-mirroring requirement meant that a copy of all data has to be stored in India, but the revised version has relaxed this provision. Only certain types of data have to be held in India now. Personal data can be transferred out of India, but "sensitive" personal data must be stored in India, with allowances provided for a copy elsewhere if specific conditions are met. Critical personal data has to be stored in India without exception and cannot be transferred out except when authorised by government authorities.

Consent

Both draft legislations in India and Indonesia reference consent and extol its importance. Provisions concerning consent in India's bill resemble consent provisions in the EU's GDPR. Entities that collect data in India, or "data fiduciaries", must obtain consent from individuals, or "data principals", who provide their personal information. The draft data bill also mandates data fiduciaries to obtain parental consent before collecting children's data. That said, the bill also has some consent exemptions that excuse fiduciaries from collecting data when the situation demands it vis-à-vis national security or law enforcement considerations. Likewise, Indonesia's bill enshrines consent as the basis for the handling of personal data, unless otherwise provided by any regulation. Consent for collecting, processing, storing, publishing, and destroying personal data must be obtained in Bahasa. Under the draft bill, organisations must receive explicit consent to collect personal data such as name, sex, nationality, religion, medical records, biometrics, and sexual orientation.

GDPR

The GDPR has influenced both India's and Indonesia's draft data legislations. Without global rules governing data, the EU's data protection regulation has informed how New Delhi and Jakarta have opted to legislate data protection. Under Indonesia's draft law, users are expected to provide personal data to "data controllers" and "data processors", who will process the data on behalf of the controllers; this process resembles GDPR rules. The Indonesian bill also uses privacy notions that sit at the core of the GDPR, which also meshes with the Indonesian constitution, which attempts to balance civil rights concerning personal information with providing conditions that allow for innovation to occur in a digital economy. India has also relied on the GDPR to set a framework that digital firms can follow to collect individual data through their platforms. Other aspects of the GDPR that India incorporated include rules for notice and prior consent for collecting and using data, conditions to process data, and certain restrictions to ensure that data collected is limited to a specific service.

Data Sovereignty

Despite a desire to nationalise data and unlock its economic value, India and Indonesia have found it difficult to legislate this objective, but not without cause. Data sovereignty or rules that advocate for the national retention of data were preferred in India. The first version

of the data bill had rules that mandated data localisation or storing a copy of all data in India. This desire was whittled down in the second iteration of the bill, which relaxed requirements governing the transfer and sharing of personal data that was not deemed sensitive. The intent to nationalise data was ostensibly thwarted by foreign tech firms and governments that opposed localisation. The Indonesian government also prioritised data sovereignty, but subsequent regulations did not reflect this impulse, mainly STE 71, which allows for data to be stored, processed, and managed abroad as long as it is accessible. Both countries appeared to have settled for accessibility over complete control.

Data Regulators

One key aspect of both legislations is the institutional authority that will be tasked to regulate data. The Indian legislation calls for establishing a Data Protection Authority (DPA) to oversee and enforce the provisions of the bill, including consent, use of data, and how data is shared across borders. The DPA's mandate is expansive and vast, including a range of functions and requirements and entities it will cover, both government and non-governmental. As a result, questions loom around whether the DPA will have sufficient capacity to discharge its functions; failure of which could lead to under-regulation or cross-regulation, particularly by agencies like the RBI that handle personal data now. Moreover, the bill also assigns considerable power to government officials who will staff and oversee the authority, raising doubts about whether the government will subject itself to the bill's rules. In contrast, Indonesia's bill lacks an overarching independent body that will supervise and enforce the legislation's provisions, thereby possibly jeopardising compliance. Instead, the MoCI will serve as the data watchdog and will serve as data controllers and data processors; thus far, MoCI has resisted calls for the establishment of an independent data regulator, citing efficiency considerations while conceding their openness to establishing an agency to implement the bill once it is enacted.

Institutional Concerns

In both countries, issues exist concerning the implementation of the proposed data laws once they are enacted. Compliance and enforcement are challenges. Provisions call for a new regulator to manage and oversee issues under the data remit. There will be a lag in the transition from existing sectoral rules in both countries to the new laws, which raises questions on how quickly the new regulator will be able to effectively discharge specific responsibilities and enforce incumbent regulations. Another related and vital concern is the independence of the future data regulator and whether it will be able to exercise judgment, keeping in mind the government's interests and that of other actors, especially the private sector. In other words, will the government comply with new data rules or will it exempt itself? And what kind of enforcement powers will the new bodies have over entities that breach rules governing the collection and sharing of data?

Besides these concerns, there are also questions concerning coordination on data issues – will firms and other organisations have the necessary staff to manage queries concerning data, particularly regarding compliance? In India, data fiduciaries or firms and organisations collecting data will have to appoint data protection officers (DPO), register with the relevant authorities, conduct data protection impact assessments, and submit their data processing functions for annual audits. The draft Indonesian data law also mandates organisations to appoint data protection officers (DPO) to oversee and manage new data rules within the organisation. It is questionable whether this goal will be realised, given Indonesia's low level of public digital awareness. Both countries will have to manage and overcome expected institutional challenges once their legislations are enacted.

India-Indonesia Data Governance Comparison

Aspects	India	Indonesia
Backdrop	India has one of the fastest-growing digital economies in the world. Aadhaar, a flagship biometric digital identity programme of 1.2 billion citizens in India, has supported India's thriving digital economy through the use of Aadhaar in government programmes such as the Jan Dhan programme. The Indian government furthered the digital push through public investments, government initiatives, and supporting policies. The telecom industry has encouraged rapid digitisation by cutting the cost for digital tools that manage daily activities, data, and internet subscriptions. Indian mobile data users have spiked rapidly in recent years due to the decline in data pricing. This rapid digitisation has compelled Indian internet users to express their concerns over online privacy (source: UNCTAD report) and to urge the government to adopt a data protection regulation.	Four problems prompted the adoption of data protection regulations in Indonesia. The first one is the **public's low level of awareness and knowledge about data privacy**, despite the large number of internet users in the country. The second reason is that **the lack of a data protection regulation hinders Indonesia's digital economy's rise**. Another problem stems from **the looming threat of further data leakage**, which has already occurred in several sectors, such as the economic, medical, and socio-political domains. This showed Indonesia's digital ecosystem's weakness, due to a lack of any overarching regulation that could legally impose punishments for such breaches. The last point of urgency is the **political pressure on the drafting of the Personal Data Protection Law**. As more stakeholders are urging the promulgation of a comprehensive PDP Law in the country, it has pressured the government to adopt a data protection regulation.

Aspects	India	Indonesia
Government regulations that address data protection	India has no data law. A rough framework of it exists in the **IT Act (2000) under Section 43A about security practices and procedures of data handling.** This situation was ameliorated with the addition of **Reasonable Security Practices and Procedures Rules (RSPP)**, protecting sensitive data. A historic Indian Supreme Court judgment became the catalyst of the Indian government's drafting of a data protection law. A draft law, **Personal Data Protection Bill 2018,** was then introduced as India's comprehensive data framework. An updated version of the bill released in 2019 **(Personal Data Protection Bill 2019)** was subjected to criticism when introduced in the Lok Sabha. It was deemed to give the government control over civilians' data without proper checks and balances.	As with India, Indonesia currently has no specific legislation on data governance. In Indonesia's case, **data protection is approached sectorally as there is no overarching regulation governing it.** The report explained the sectoral approach to data protection in various government sectors: telecommunication and informatics, trade and commerce, banking and financial services, health services, and civil services. Each sector has its specific focus on data protection and manages it through sector-specific regulations. This approach makes data protection regulation in Indonesia still unharmonious and sector-based. Loopholes in each sector's regulation also exacerbate this. In 2019, the government drafted **the Personal Data Protection Law** to become the regulatory framework for Indonesia's data protection. However, this bill was suspended in its adoption by the House of Representatives due to the lack of prioritisation.
Data Regulators	In the 2018 bill, the governing body with rule-making and adjudication capacity in data governance is **the Data Protection Authority (DPA).** In the 2019 bill, the DPA's power remained but with more governmental involvement. A criticism of the 2019 version of the DPA was the absence of independent members in the government body, which was seen as depleting DPA's independence in regard to the enforcement of data protection laws.	In the draft PDP law, one of the most heated debates concerned **the absence of an independent body in charge of enforcement and supervision.** This provision was heavily criticised as it could create distrust from citizens over the enforcement of the law and the government's potential conflict of interest. The absence of an independent body was explained by the government as being due to the need to increase bureaucratic efficiency. There is also an ongoing debate in the House of Representatives on the establishment of an independent body. **However, it is worth noting that this decision is not final and that the government is still open to establishing an independent body.**

Aspects	India	Indonesia
Data governance actors	1. **Data principals: citizens and consumers who provide personal data to operators.** 2. **Data fiduciaries: Government, private firms, and organisations that process and manage personal data.**	3. **Data regulator: government body that regulates activities involving the usage of personal data. It is divided into two branches, the executive branch (e.g., MoCI & Ministry of Internal Affairs) and the legislative branch.** 4. **Electronic system manager: any organisation that uses its users' data for their services (e.g., social media companies).** 5. **Civil society: civil society entities (e.g., NGOs and academia) that advocate for data governance in Indonesia.**
Data categorisation	Under the PDP bill 2019, data is classified into **personal data, non-personal data, sensitive personal data, and critical personal data**. 1. **Personal data: any information relating to a natural person that is directly or indirectly capable of identifying such a person.** 2. **Non-personal data: anonymised data.** 3. **Sensitive personal data: includes financial data, health data, sexual orientation, biometric information, genetic data, intersex status, caste or tribe, and religious/political belief.**	Under the draft PDP law, personal data is split into two categories, **general data and specific data.** 1. **General data: personal data such as full name, gender, nationality, and religion that is capable of identifying an individual.** 2. **Specific data: includes data such as health-related information, biometrics, genetics, sexual orientation, political preferences, etc. that are described in other existing regulations.** It is worth noting that the draft does not explicitly define sensitive data despite the importance of safeguarding it.

Aspects	India	Indonesia
Journey towards adopting a data law	The rapid digitisation in Indian society has significantly raised public concerns over personal information and data. The realisation that personal information collected can result in a loss of privacy compels the government to enact a PDP law. Indian firms are also now rethinking their role in managing personal data and have urged the government to establish a PDP regulation that can help their business and product operations. All of the reasons above compelled the Indian government to draft the PDP Bill 2018.	Quite similar to the urgency to adopt the PDP law, as mentioned above, the absence of a specific PDP law has been disadvantageous for Indonesia's rapidly digitising society. With one of the largest internet user populations globally, many Indonesians surprisingly are not equipped with adequate knowledge about data privacy; a PDP law would alleviate the risks associated with this lack of knowledge. As with India, Indonesia was also compelled by the burgeoning digital economy sector of the country, which is currently disadvantaged by the lack of a PDP regulation. Pressure from key actors such as electronic system managers and civil society also pushed for the government's response in creating the draft of the PDP law in 2019.
Implementation concerns	The PDP bill 2019 has come under scrutiny for some of its provisions. One of the concerns is regarding **consent**, as it was deemed to have adopted a "blanket consent" system, which impedes the transparency of data handling. The 2019 Bill was also criticised over **the increase of government authority in managing personal data** as showcased by **the reduction of the DPA's power and independence**.	Ensuring compliance and enforcement is central to the challenge of formulating the PDP law in Indonesia. However, there are several drawbacks in the current draft, should it be passed. The first one is regarding **the short period given for data processors and data controllers to terminate and grant access to personal data.** The second one pertains to **the need for technical guidelines for industries and other sectors after this law is passed to reduce ambiguities.** Lastly, is **the absence of an independent body**, which raised questions about the trustworthiness of the government in supervising and enforcing the data protection law.

Conclusion

Both India and Indonesia lack comprehensive legislation(s) on data governance. Both are in the process of adopting overarching personal data protection regulations and both have concerns regarding the implementation of personal data protection regulations. However, there are also differences in the way both countries are progressing towards new regulations. For example, there are different levels of urgency among the regulators in both countries. India's draft legislation includes provisions for the establishment of an independent body to oversee data protection, while Indonesia's draft does not. This section concludes with a summary of India's and Indonesia's key challenges and opportunities in implementing a robust personal data protection regulation.

Key Challenges

India

India's key challenges are socio-political in nature. Digitisation levels are uneven across firms in different sectors. ICT firms, professional services, and healthcare are represented in the bottom quartile of digital adoption, while transportation and construction companies are in the top quartile. The massive use of data has prompted a large number (90%) of India's internet users to express their concerns regarding online privacy. There is a growing realisation that the process of data collection can be depersonalising and could result in a significant loss of one's privacy. Before the issuance of the bill initiated by the Srikrishna Committee, the private sector's perspective was that the collected data was their property, not the users'. Moreover, challenges exist when trying to ascertain whether the central government will be exempt from the new data legislation, as currently envisaged, which would raise questions regarding the newly entrenched norms related to privacy.

Indonesia

In Indonesia, existing data protection regulations are heavily sectoral, whereby different sectors of government have their own perception/scope of data protection. Personal data protection is governed by at least 30 regulations issued by various government bodies and ministries, covering telecommunication and informatics, healthcare, trade and commerce, civil administration, and banking and financial services. This approach leads to fragmented and sector-oriented data protection regulations, as there are no overarching set of policies regarding personal data. The lack of a comprehensive regulation results in different perspectives on which data should be protected and classified as "sensitive".

Other than these regulatory issues, Indonesia's challenge also lies in its society. A large number of internet

users are lacking in their awareness and knowledge about data privacy, yet have their data collected and processed. It is not unusual to find Indonesian internet users posting sensitive information about themselves or their families. There have been several incidents of data breaches, both on private-owned and government-owned platforms. The government's inability to effectively exercise legal enforcement on data breaches can become a challenge to protecting people's data.

Along with ongoing discussions on establishing a new personal data regulation, heated debates over the establishment of a data protection body, data classification, and data sharing with private sectors are underway. There is currently no data protection body that regulates and supervises data protection in Indonesia. The need to establish a data protection body has not been addressed in the current draft PDP law as there is no mandate to create the institution in the law. This has been debated by many stakeholders. The MoCI plans to establish the data protection body under its structure, but the Parliament is divided between approving MoCI's plan or keeping the body separate. The current draft identifies "general" and "specific" data in regard to data classification, but "sensitive" data is not explicitly defined despite its importance. This gap could cause future misinterpretations.

Other issues of the current draft include (1) short period for data processors and data controllers to terminate and grant access to personal data, and (2) the need for technical guidelines for industries after the law is passed. Ultimately, Indonesia still has to improve the capability of relevant stakeholders to implement robust data governance measures.

Key Opportunities

Despite the many challenges faced by India and Indonesia, both countries have the opportunity to strengthen data governance.

India

Although India ranks last out of the 17 major advanced economies in terms of digital adoption, impetus toward sustained digitisation has been created by the Aadhaar programme. So far, India is the only large populous developing country to have provided a biometric-based digitally verifiable identity to most of its adult citizens. With secure, verified identification, Indian citizens can enter into transactions without the need for additional documents, thus cutting bureaucratic red tape. In turn, this programme has stimulated India's digital economy, which then triggered discussions concerning privacy.

Moreover, the Indian government under Prime Minister Modi has initiated several policy initiatives, such as the Jan Dhan programme, which boosted financial access to the unbanked, and the Digital India initiative, which promoted strong digital infrastructure, digital services and digital literacy for Indian citizens. Such initiatives will drive robust data governance demands in the future.

The establishment of the Srikrishna Committee has also created opportunities for India's data governance. Despite concerns regarding the bill's drafting and several provisions, the development of the ICT Law, the 2018 Personal Data Protection Bill, and the 2019 Personal Data Protection Bill shows that India is gradually moving toward a comprehensive data protection law.

Indonesia

Indonesia's key opportunities for better data governance are similar to that of India. For Indonesia, the recent (mid-2020) release of the National Strategy on

Artificial Intelligence (AI) signals Indonesia's commitment to developing its AI for digital governance. A chapter of the National Strategy emphasises the importance of certification for Indonesian talents. This strategy is expected to emphasise pre-existing standards, both international and national. The purpose of certification is to narrow the gap between the supply (labour) and the industry's demand (labour market). Despite its current lack of national-level discussion and low popularity among lawmakers, the National AI Strategy might push stakeholders to complete the Personal Data Protection Bill as soon as possible to keep up with the fast evolving technology and the increasingly massive data usage.

Other than the new strategy, various digital programmes have been launched by Indonesia's MoCI. The fast growth of the digital economy, coupled with numerous e-commerce platforms emerging within the Indonesian market, is why the government is keen to engage in the enhancement of digital awareness, digital literacy, and digital skills. This ambition is delivered through the ministry's comprehensive training programmes.

Aside from the change of strategy, social factors also influence motivations to provide robust data governance in Indonesia. Due to the cyber incidents (such as data breaches linked to Indonesia's most prominent e-commerce platforms) in the last few years, the government is under increased political pressure to deal with the issue. The changing level of commitment to provide better data regulation is also influenced by Indonesian NGOs that have expressed concern over the government's "slow" progress in adopting the PDP law.

Ultimately, the success of adopting personal data protection regulations in the world's two largest developing democracies remains to be seen. To what extent will India and Indonesia adopt the principles of the EU's General Data Protection Regulation? Whatever the result is, the world will be watching as they may be used as references or benchmarks for other developing countries.

Bibliography

ABDI, n.d., *About.* Available at https://www.abdi.id/tentang-abdi/. [Accessed 30 June 2020].

AFPI, n.d., *About.* Available at https://afpi.or.id/en/about. [Accessed 30 June 2020].

Annur, C. M., 2019, "DPR Kritik Ide Pembentukan Lembaga Perlindungan Data Pribadi", *Katadata.* Available at https://katadata.co.id/berita/2019/07/18/dpr-kritik-ide-pembentukan-lembaga-perlindungan-data-pribadi. [Accessed 5 June 2020].

Annur, C. M., 2019, "Survei APJII: Penetrasi Pengguna Internet di Indonesia Capai 64,8%", *Katadata.* Available at https://katadata.co.id/berita/2019/05/16/survei-apjii-penetrasi-pengguna-internet-di-indonesia-capai-648. [Accessed 26 June 2020].

AntaraNews, 2019, "SAFENet harap menkominfo Johnny G Plate selesaikan UU PDP". Available at: https://www.antaranews.com/berita/1129032/safenet-harap-menkominfo-johnny-g-plate-selesaikan-uu-pdp. [Accessed 3 June 2020].

ASEAN. ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN).

Asosiasi Penyelenggara Jasa Internet, 2019, *Hasil Survei Penetrasi dan Perilaku Pengguna Internet di Indonesia 2018.* Available at https://apjii.or.id/content/read/39/410/Hasil-Survei-Penetrasi-dan-Perilaku-Pengguna-Internet-Indonesia-2018. [Accessed 26 June 2020].

Astuti, N. A. R., 2019, "Komisi II DPR Tak Setuju Dukcapil Beri Akses Data Penduduk ke Swasta", *DetikNews.* Available at https://news.detik.com/berita/d-4635216/komisi-ii-dpr-tak-setuju-dukcapil-beri-akses-data-penduduk-ke-swasta. [Accessed 30 June 2020].

Basu, A. and Amber Sinha, "The Realpolitik of the Reliance-Jio Facebook Deal", 29 April 2020, https://thediplomat.com/2020/04/the-realpolitik-of-the-reliance-jio-facebook-deal/.

Basu, A. and Karthik Nachiappan, "The battle for data sovereignty, India and Digital worldmaking", Seminar Magazine, July 2020.

Bhandari, Vidya and Renuka Sane, "Protecting Citizens from the State post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna report and the Data protection bill 2018", http://docs.manupatra.in/newsline/articles/Upload/7B08CF55-E27D-4A44-A292-3882F08E9053.pdf.

Bloomberg quint, "Why Jio-Facebook May Work Better Than A Google Or Amazon Combination", 2020, https://www.bloombergquint.com/business/why-jio-facebook-may-work-better-than-a-google-or-amazon-combination.

Buletin APJII, 2019, "Perlindungan Data Pribadi Mutlak Diperlukan", *APJII.* Available at https://blog.apjii.or.id/index.php/2019/08/20/perlindungan-data-pribadi-mutlak-diperlukan/. [Accessed 30 June 2020].

Burhan, F. A., 2020, "Asosiasi Bahas UU Fintech hingga Data Pengguna di Istana". *KataData.* Available at https://katadata.co.id/berita/2020/01/24/asosiasi-bahas-uu-fintech-hingga-data-pengguna-di-istana. [Accessed 30 June 2020].

Burhan, F. A., 2020, "Cegah Pemerintah Salahgunakan Data Pribadi, DPR Minta Lembaga Khusus", *Katadata.* Available at https://katadata.co.id/berita/2020/02/25/cegah-pemerintah-salahgunakan-data-pribadi-dpr-minta-lembaga-khusus. [Accessed 5 June 2020].

Burman, Anirudh. "Will India's data protection law protect privacy and promote growth?", https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

CNN Indonesia, 2018, *idEA Akui Jejak Data Pribadi Untuk Baca Perilaku.* Available at https://www.cnnindonesia.com/teknologi/20181025185542-185-341482/idea-akui-jejak-data-pribadi-untuk-baca-perilaku. [Accessed 30 June 2020].

CNN Indonesia, 2019, *BSSN Tanggapi Penyadapan Tanpa UU Pelrindungan Data Pribadi*. Available at https://www.cnnindonesia.com/teknologi/20190812183821-185-420671/bssn-tanggapi-penyadapan-tanpa-uu-perlindungan-data-pribadi. [Accessed 5 June 2020].

CNN Indonesia, 2019, *SAFE Net Respons Pidato Jokowi soal Perlindungan Data Pribadi.* Available at https://www.cnnindonesia.com/teknologi/20190816203213-185-422140/safe-net-respons-pidato-jokowi-soal-perlindungan-data-pribadi. [Accessed 5 June 2020].

CNN Indonesia, 2020, *Kominfo Didesak Sanksi Tokopedia dan Bhinneka soal Akun Bocor*. Available at https://www.cnnindonesia.com/teknologi/20200512165045-185-502615/kominfo-didesak-sanksi-tokopedia-dan-bhinneka-soal-akun-bocor. [Accessed 4 June 2020].

CNN Indonesia, 2019, "PP PSTE 'titipan asing' yang gadai kedaulatan data di Indonesia". Available at https://www.cnnindonesia.com/teknologi/20191108152910-185-446726/pp-pste-titipan-asing-yang-gadai-kedaulatan-data-indonesia. [Accessed 19 June 2020].

Damar, A. M., 2019, "ICT Watch Desak Pemerintah Segera Sahkan UU Perlindungan Data Pribadi", *Liputan6.* Available at https://www.liputan6.com/tekno/read/4027861/ict-watch-desak-pemerintah-segera-sahkan-uu-perlindungan-data-pribadi. [Accessed 5 June 2020].

Damarjati, D., 2019, "Kemendagri: 1.227 Lembaga Bisa Akses Data Penduduk, Termasuk Swasta", *DetikNews.* Available at https://news.detik.com/berita/d-4634210/kemendagri-1227-lembaga-bisa-akses-data-penduduk-termasuk-swasta. [Accessed 5 June 2020].

Direktorat Aplikasi dan Informatika, n.d., *Tugas dan Fungsi Direktorat Jenderal Aplikasi dan Informatika.* Available at https://aptika.kominfo.go.id/profile/tugas-dan-fungsi/#:~:text=Tugas%20Pokok,di%20bidang%20penatakelolaan%20aplikasi%20informatika. [Accessed 5 June 2020].

Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan", *ELSAM.* Available at https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Accessed 24 June 2020].

Djafar, W., Sumigar, B. R. F., Setianti, B. L., 2016, *Perlindungan Data Pribadi di Indonesia*; *Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM.

Dvara Research, "What do Indians think about privacy and data protection", https://www.dvara.com/blog/2017/11/16/privacy-on-the-line-what-do-indians-think-about-privacy-data-protection/.

ELSAM, 2019, *Penyalahgunaan Data Pribadi Meningkat, Perlu Akselerasi Proses Pembahasan RUU Perlindungan Data Pribadi.* Available at https://elsam.or.id/5806-2/. [Accessed 26 June 2020].

ELSAM. 2019, "Pentingnya UU Perlindungan Data Pribadi". Available at https://elsam.or.id/pentingnya-uu-perlindungan-data-pribadi/ . [Accessed 3 June 2020].

Fauzan, R., 2020, "Pelaku Dagang-el Soroti Salah Satu Ketentuan UU Perlindungan Data Pribadi", *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20200304/266/1209168/pelaku-dagang-el-soroti-salah-satu-ketentuan-uu-perlindungan-data-pribadi. [Accessed 30 June 2020].

Fauzan, R., 2020, "RUU Perlindungan Data Pribadi Gunakan GDPR Uni Eropa Sebagai Acuan", *Bisnis.com.* Available at https://teknologi.bisnis.com/read/20191202/282/1176768/ruu-perlindungan-data-pribadi-gunakan-gdpr-uni-eropa-sebagai-acuan. [Accessed 5 June 2020].

Gatra, 2020, *RUU Data Pribadi Akan Atur Pusat Data hingga Rekaman CCTV.* Available at https://www.gatra.com/detail/news/471976/politik/ruu-data-pribadi-akan-atur-pusat-data-hingga-rekaman-cctv-. [Accessed 5 June 2020].

Gazali, D., S. and Rachmadi, U., 2010, "Hukum Perbankan", *Sinar Grafika.* Jakarta, p. 30.

Government of India, Ministry of Information Technology, "Personal Data Protection Bill 2018", https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

Government of India, Ministry of Finance, "2019 Indian Economic Survey", https://library.iima.ac.in/public/Economic_Survey_2019_20_Vol_2.pdf.

Government of India, Ministry of Electronics and Information Technology, "India's Trillion-Dollar Digital Opportunity", *2019*, https://meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity.

Government of India, "The Personal Data Protection Bill, 2019", Bill 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

Government of India, "Report by the Committee of Experts on Non-Personal Data Governance Framework", https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

Gupta, A and S. Jaju, "Summary of the report of the Committee of Experts on Non-Personal Data", 14 July 2020, https://www.ikigailaw.com/summary-of-the-report-of-the-committee-of-experts-on-non-personal-data/#acceptLicense.

Ihsannudin, 2019, "Menkominfo: Google dan Facebook Berencana Bangun Pusat Data di Indonesia", *Kompas.* Available at https://nasional.kompas.com/read/2019/12/06/09533131/menkominfo-google-dan-facebook-berencana-bangun-pusat-data-di-indonesia. [Accessed 30 June 2020].

Indonesian Banking Law No. 10/1998.

Indonesian Health Law No. 36/2009.

Indonesian Law No. 11/2008 on Information and Electronic Transaction.

Indonesian Law No. 23/2006 on Civil Administration.

Indonesian Law No. 24/2013 on the Amendment of the Indonesian Act No. 23/2006 on Resident Administration.

Indonesian Law No. 39/1999 on Human Rights.

Indonesian Law No. 43/2009 on Record Management.

Indonesian Law No.8/1999 on Consumer Protection.

Indonesian MoCI Regulation No. 20/2016 about The Protection of Personal Data in the Electronic System.

Indonesian Trade Law No. 7/2014.

Jakarta Globe, 2020, "Jokowi hopes to unleash digital economy potential". Available at https://jakartaglobe.id/tech/jokowi-hopes-to-unleash-indonesias-digital-economy-potential/. [Accessed 3 June 2020].

Jawa Pos, 2019, "ICT Watch desak UU Perlindungan Data Pribadi segera dirampungkan". Available at https://www.jawapos.com/oto-dan-tekno/teknologi/01/08/2019/ict-watch-desak-uu-perlindungan-data-pribadi-segera-dirampungkan/. [Accessed 3 June 2020].

Johny Plate in Reuters, 2019, "Indonesia needs to establish data protection law urgently". Available at https://www.reuters.com/article/us-indonesia-communications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Accessed 3 June 2020].

Kamaliah, A., "Kata Asosiasi Soal Data Center Tak Harus di Indonesia", *DetikInet.* Available at https://inet.detik.com/law-and-policy/d-4775013/kata-asosiasi-soal-data-center-tak-harus-di-indonesia. [Accessed 5 June 2020].

Kartika, M., 2019, "BSSN Dukung RUU Perlindungan Data Pribadi Segera Disahkan", *Republika.* Available at https://republika.co.id/berita/q1zhdy428/bssn-dukung-ruu-perlindungan-data-pribadi-segera-disahkan. [Accessed 5 June 2020].

Kementerian Dalam Negeri, n.d., *Struktur Organisasi.* Available at https://www.kemendagri.go.id/page/read/7/struktur-organisasi. [Accessed 11 July 2020].

Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, n.d., *Direktorat Harmonisasi Peraturan Perundang-undangan II.* Available at http://ditjenpp.kemenkumham.go.id/struktur-djpp/dit-harmonisasi.html. [Accessed 11 July 2020].

Kominfo, 2018, *Rudiantara Sebut Data Center Tak Perlu di Indonesia.* Available at https://kominfo.go.id/content/detail/14742/rudiantara-sebut-data-center-tak-perlu-di-indonesia/0/sorotan_media. [Accessed 30 June 2020].

Krishnan, Varun B., "How much mobile data do Indians use in a month?", *The Hindu,* 26 August 2019, https://www.thehindu.com/news/national/indian-mobile-data-usage-over-7-gb-per-month/article29259546.ece.

Kumparan, 2020, *Regulasi Tokopedia Larang Pengguna Hapus Akun, Langgar Hak Data Pribadi*. Available at https://kumparan.com/kumparannews/regulasi-tokopedia-larang-pengguna-hapus-akun-langgar-hak-data-pribadi-1tNCp40Q9au. [Accessed 5 June 2020].

McKinsey Global Institute, "Digital India: Technology To Transform A Connected Nation", repr. McKinsey & Company, 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

McKinsey & Company, 2016, "Unlocking Indonesia's digital economy". Available at https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Accessed 3 June 2020].

Mehrota, Karishma, "Explained: Data, Their Types, and Other Terms Described in India's PDP Bill", *The Indian Express*, 13 December 2019, https://www.indianexpress.com/article/explained/this-word-means-data-their-types-and-other-terms-described-in-indias-pdp-bill-6164247/.

Ministry of Communication and Informatics, 28 January 2020, *Presiden Serahkan Naskah RUU PDP ke DPR RI.* Available at https://www.kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-indonesia-akan-jadi-negara-asia-tenggara-kelima-yang-miliki-uu-pdp/0/siaran_pers. [Accessed 5 June 2020].

Narayanan, Dinesh and Venkat Ananth, "Vidhi and the making of India's data protection law", https://economictimes.indiatimes.com/prime/economy-and-policy/vidhi-and-the-making-of-indias-data-protection-law/primearticleshow/77768876.cms?from=mdr.

NITI Aayog, "National Strategy for Artificial Intelligence", June 2018, https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

OJK Letter No. 14/SEOJK.07/2014 on The Customer's Confidentiality and Data and/or Information Security.

OkeNews, 2018, *Evita Nursanty: Pusat Data dengan Tingkat Confidentiality Tinggi Wajib Berada di Indonesiatara Sebut Data Center Tak Perlu di Indonesia.* Available at https://nasional.okezone.com/read/2018/10/01/337/1958125/evita-nursanty-pusat-data-dengan-tingkat-confidentiality-tinggi-wajib-berada-di-indonesia. [Accessed 30 June 2020].

Pertiwi, W. K., 2020, "ELSAM: Harus Ada Pengawas UU PDP di Luar Pemerintah", *Kompas.* Available at https://tekno.kompas.com/read/2020/01/31/12580067/elsam--harus-ada-pengawas-uu-pdp-di-luar-pemerintah?page=all. [Accessed 5 June 2020].

PTI News, "India's data consumption may touch 25 GB per month per user by 2025: Ericsson", *PTI News*, 16 June 2020.

Press Information Bureau, *Centralised System to Monitor Communication*, 26 November 2009, http://pib.nic.in/newsite/.

Raman, Anand and Greg Chen, "Should other countries build their own India Stack?", 6 April 2017, https://www.cgap.org/blog/should-other-countries-build-their-own-india-stack.

Ray, Saladitya, "Justice Srikrishna data protection draft bill is now public, highlights and what happens next", *MediaNama*, 27 July 2018, https://www.medianama.com/2018/07/223-sri-krishna-bill-submitted/.

Republika, 2019, "PP PSTE Jadi Bentuk Kedaulatan Data". Available at https://nasional.republika.co.id/berita/q1w1pt370/pp-pste-jadi-bentuk-kedaulatan-data. [Accessed 19 June 2020].

Ristianto, C., 2020, "Kemendagri Diminta Kaji Ulang Kerja Sama Data Kependudukan", *Kompas.* Available at https://nasional.kompas.com/read/2019/08/02/13161321/kemendagri-diminta-kaji-ulang-kerja-sama-data-kependudukan. [Accessed 5 June 2020].

Rizkinaswara L., 2019, "ICT Watch", *Aptika Kominfo.* Available at https://aptika.kominfo.go.id/2019/07/ict-watch/. [Accessed 30 June 2020].

Rosadi, S. D., and Pratama, G. G., 2018, "Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia", *Veritas*, *4*.

Salna, 2018, *The Jakarta Post,* "Facebook faces Indonesian Police investigation over the data breach", https://www.thejakartapost.com/life/2018/04/06/facebook-faces-indonesian-police-investigation-over-data-breach.html. [Accessed 3 June 2020].

See Kementerian Komunikasi dan Informatika, 2017, *Inilah Road Map E-Commerce Indonesia 2017-2019.* Available at https://kominfo.go.id/content/detail/10309/inilah-road-map-e-commerce-indonesia-2017-2019/0/berita. [Accessed 26 June 2020].

See Kementerian Komunikasi dan Informatika, n.d., *Struktur Organisasi.* Available at https://aptika.kominfo.go.id/profil/struktur-organisasi/. [Accessed 4 June 2020].

Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2017, *Sejak Kapan Masyarakat Indonesia Menikmati Internet.* Available at https://stei.itb.ac.id/id/blog/2017/06/19/sejak-kapan-masyarakat-indonesia-nikmati-internet/. [Accessed 24 June 2020].

Setiawan, R., 2020, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", *Tirto.* Available at https://tirto.id/fA5B. [Accessed 24 June 2020].

Setyowati, D., 2018, "Empat Urgensi UU Perlindungan Data Pribadi di Indonesia", *Katadata.* Available at https://katadata.co.id/berita/2018/04/10/4-urgensi-uu-perlindungan-data-pribadi-di-indonesia. [Accessed 26 June 2020].

Setyowati, D., 2019, "Pelaku Industri Telekomunikasi Minta Pusat Data Wajib Ada di Indonesia", *Katadata.* Available at https://katadata.co.id/berita/2019/02/06/pelaku-industri-telekomunikasi-minta-pusat-data-wajib-ada-di-indonesia. [Accessed 5 June 2020].

Sharma, "Regulating A Digital Economy: An Indian Perspective", *Brookings, 2018,* https://www.brookings.edu/blog/up-front/2018/04/25/regulating-a-digital-economy-an-indian-perspective/.

Siagian, P., 2017, "Hepatitis Patients Struggle with Discrimination in Workplace", *The Jakarta Post.* Available at https://www.thejakartapost.com/life/2017/11/15/hepatitis-patients-struggle-with-discrimination-in-workplace.html. [Accessed 3 June 2020].

Singh, "Digital India: Unleashing Prosperity", *International Journal of Advanced Research in Computer Science* 7, *2016,* http://libproxy1.nus.edu.sg/login?url=https://search-proquest-com.libproxy1.nus.edu.sg/docview/1860624209?accountid=13876.

Telecom Regulatory Authority of India, "Consultation Paper on Free Data", https://www.trai.gov.in/sites/default/files/CP_07_free_data_consultation_0.pdf.

Tempo.co, 2020. "Ministry still Tracing Indonesia's Covid-19 patients' data leak". Available at https://en.tempo.co/read/1356052/ministry-still-tracing-indonesias-covid-19-patients-data-leak. [Accessed 28 June 2020].

Tempo.co, 2019, "Bukalapak confirms of an attempted customer data breach". Available at https://en.tempo.co/read/1186473/bukalapak-confirm-of-an-attempted-customer-data-breach. [Accessed 3 June 2020].

Thakore, Talwar & associates, "Data Protected India", *Linklaters*, March 2020, https://www.linklaters.com/en/insights/data-protected/data-protected---india.

The 1945 Constitution of the Republic of Indonesia.

The Jakarta Post, 2020, "Data breach jeopardizes more than 15 million Tokopedia users, report finds". Available at https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Accessed 3 June 2020].

The Jakarta Post, 2020, "E-commerce platform Bhineka.com reported to be the latest target of data theft". Available at https://www.thejakartapost.com/news/2020/05/13/e-commerce-platform-bhinneka-com-reported-to-be-latest-target-of-data-theft.html. [Accessed 3 June 2020].

Umali, T., 2019, "Indonesia drafts the Personal Data Protection Act. Open Gov Asia". Available at https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/. [Accessed 5 June 2020].

UNCTAD, *Digital Economy Report 2019, Value Creation and Capture: Implications for Developing Countries.* United Nations, 2019.

We Are Social and Hootsuite, 2020, "Digital Indonesia". Available at https://datareportal.com/reports/digital-2020-indonesia. [Accessed 3 June 2020].

Wimmer, Kurt and Maldoff, Gabe, "India Proposes Updated Personal Data Protection Bill", *InsidePrivacy,* 12 December 2019, https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/#:~:text=Critical%20personal%20data%3A%20As%20with,be%20transferred%20outside%20of%20India.

Yatim, S., 2019, "The privacy battle in Indonesia- the longer the battle, the more consumers stand to lose", *The Jakarta Post.* Available at https://www.thejakartapost.com/academia/2019/02/21/the-privacy-battle-in-indonesia-the-longer-the-battle-the-more-onsumers-stand-to-lose.html. [Accessed 3 June 2020].

Yuniar, R., 2018, "This Week in Asia. Facebook's Cambridge Analytica scandal puts Indonesia's tech firms on the spot". Available at https://www.scmp.com/week-asia/business/article/2143763/facebooks-cambridge-analytica-scandal-puts-indonesias-tech-firms. [Accessed 3 June 2020].

Zeller, B., Trakman, L., Walters, R., and Rosadi, S. D., 2019, "The Right to Be Forgotten – The EU and the Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)".

About the Authors

Institute of South Asian Studies, National University of Singapore

Karthik Nachiappan is Research Fellow at the Institute of South Asian Studies, National University of Singapore with a joint appointment at the NUS South Asian Studies Programme. His current research focuses on the political economy of technology in India, specifically the regulation of issues like data, cyber-security, social media and artificial intelligence and how policies influence India's positions on global rules covering these technology issues.

Ronojoy Sen is Senior Research Fellow (and Research Lead, Politics, Society and Governance) at the Institute of South Asian Studies and the South Asian Studies Programme, National University of Singapore. He has worked for over a decade with leading Indian newspapers, most recently as an editor for The Times of India. His latest book is Nation at Play: A History of Sport in India (Columbia University Press/Penguin, 2015). He is also the author of Articles of Faith: Religion, Secularism, and the Indian Supreme Court (Oxford University Press, 2010) and has edited several books, the latest being Media at Work in China and India (Sage, 2015). He has contributed to edited volumes and has published in several leading journals. He also writes regularly for newspapers. He has a Ph.D. in political science from the University of Chicago and read history at Presidency College, Calcutta.

Center for Digital Society (CfDS), Universitas Gadjah Mada

Mulya Amri is a public policy specialist and member of the expert panel at Katadata Insight Center, based in Jakarta. He leads multiple teams of researchers and data analysts from project inception to delivery on topics related to economics, business, and public policy, including digitalisation. Mulya has co-written 20 books and book chapters, mostly on subnational competitiveness and urban governance. He also has 20 years of experience working with government officials, businesses, and civil society groups in Indonesia, Singapore, Brunei, the Philippines, China, and the US. Mulya has a Ph.D in public policy from the National University of Singapore, a Master's in urban planning from the University of California, Los Angeles, and a bachelor's degree from Institut Teknologi Bandung, Indonesia.

Diah Angendari is a lecturer in the Communication Science department and executive secretary at the Center for Digital Society, Universitas Gadjah Mada. Her research focuses on the topic of strategic communication and the use of ICT in communication, including digital literacy, and data privacy.

Anisa Pratita Kirana Mantovani is the Manager of Research Division at the Center for Digital Society, Universitas Gadjah Mada. Her research focuses are cybersecurity in International Relations, digital health, digital literacy, and data privacy, as well as innovative public policy.

Janitra Haryanto is a research project officer at the Center for Digital Society Universitas Gadjah Mada. He has written more than 20 publications on digital and innovative policy topics, including digital economy, and social media, and politics. He is also working as a consultant for the Asian Development Bank (ADB) in one of its youth financial inclusion projects.

Raka Wicaksana has previously been involved in an international youth leadership NGO and research industry that focuses on contemporary digital issues. He currently assists the Director-General of Application and Informatics under the Indonesian Ministry of Communication and Informatics. His research interest mainly covers digital policy formulation and digital transformation agenda.