CIPS
Center for Indonesian Policy Studies

Policy Paper No. 30

Co-regulating the Indonesian Digital Economy

by Ira Aprilianti & Siti Alifah Dina

www.cips-indonesia.org

We would like to thank the Center for International Private Enterprise for their support of this publication

Acknowledgement:
This project is supported by a Grant from the Center for International Private Enterprise in Washington, D.C.

Policy Paper No. 30

Co-regulating the Indonesian Digital Economy

Authors:
Ira Aprilianti & Siti Alifah Dina

Jakarta, Indonesia
January, 2021

EXECUTIVE SUMMARY

The Gross Merchandise Value of the Indonesian digital economy has been growing at an annual rate of over 40% since 2015 and is predicted to reach USD 130 billion by 2025. This makes Indonesia the most promising digital market among its geographic neighbors. To facilitate further growth of the digital economy, the government must ensure the safety of the digital ecosystem for its users while providing an environment conducive to innovation. The government should pursue these goals by focusing on four policy areas: consumer protection, data privacy, cybersecurity, and e-payments.

These areas are important due to the existence of regulatory deficiencies that if resolved, would accelerate the inclusive development of Indonesia's digital economy. Although they are treated separately, at times these areas overlap and impact the nation's digital economy environment.

The existing consumer protection regulatory framework cannot accommodate emerging business models and instead imposes potential barriers to doing business; for example, in the form of licensing requirements for online sellers. Increasingly frequent data breaches and cyberattacks have highlighted the importance of data privacy and cybersecurity; yet here, too, the regulatory framework is incomplete and important bills are still being deliberated.

The regulatory framework of e-payments is more advanced. In this area, the Indonesian government has established a clear policy blueprint and more innovative regulatory approaches, including a regulatory sandbox. The central bank of Indonesia (BI) and the Indonesian government's financial services industry regulator (OJK) maintain a continuous dialogue with businesses, which creates and maintains a regulatory environment conducive to innovation. However, problems with e-payments remain in the areas of cybersecurity and data privacy.

To regulate these areas of the digital economy effectively, a process of co-regulation is required. Co-regulation is a regulatory approach that emphasizes responsibility-sharing between state and non-state actors such as broad-based private sector stakeholders in policymaking and enforcement. It focuses on collaboration in the creation, adoption, enforcement, and evolution of policies and regulations. It is helpful for regulating the digital economy because it may provide the state with necessary data and knowledge, a mechanism for dialogue and flexible adaptation of legislative solutions in the new and fast-changing digital economy, and facilitate regulatory enforcement.

To implement co-regulation, a Public-Private Dialogue (PPD) process needs to be established. The PPD needs to include the key stakeholders, such as government officials, business associations, civil society organizations, academia, and provide sufficient time for the process. Government actors should consider digital tools for collecting public input and to allow businesses to submit a regulatory impact assessment during a regulation's lifetime.

A formal process for sharing responsibility between public and private sectors must also be established. Involving businesses in the regulatory process, for example when testing new policies, helps ensure regulations remain enforceable without stifling innovative processes.

The flexibility of this process allows regulators to accommodate the rapid changes of digital technology. A regulatory sandbox is a practical and positive example of such a process. It provides a policy innovation space for policymakers and businesses to engage in ideation, iteration, and experimentation within temporary, flexible regulatory or legal frameworks.

Finally, a monitoring and evaluation mechanism is needed to periodically review the co-regulation process and ensure that all lessons learned are on-the-record and transparent.

This paper is divided into four sections. Section one highlights the landscape of the Indonesian digital economy, section two describes approaches in regulating the digital economy, and section three explores regulatory challenges. At the end, the paper presents ways to improve the regulatory framework of Indonesia's digital economy.

INDONESIA'S DIGITAL ECONOMY

The digital revolution has transformed the way products and services are developed, produced, and delivered. This has affected businesses from multinational enterprises (MNEs) to startups (OECD, 2015, p.52). Particularly with the rise of the Covid-19 pandemic, consumers are increasingly shifting to online shopping, increasing demand for faster and more secure mobile transaction and payment solutions. The shift of consumers to online commerce has led to new business models that disrupt markets and transform conventional businesses in sectors such as retail, transport and logistics, financial services, manufacturing, agriculture, education, healthcare, and media (BI, 2019; OECD, 2015, p.53–54).

Business sectors in which digital technology is integrated into daily operations form the building blocks of the digital economy (see Box 1). Banks and financial companies are at the forefront of offering digital versions of their conventional services, but non-bank, non-financial start-ups have also built disruptive new payment mechanisms using digital technology. These payment mechanisms have reduced transaction costs for businesses, which pass savings onto consumers. Consumers also benefit from the added convenience of always-available online services (OECD, 2015, p.52).

Box 1.
What is the "Digital Economy"?

The digital economy is made up of businesses that use digital information and the internet to increase efficiency, enhance productivity, enlarge market reach, and reduce operational costs (Rillo, 2018; Kulhmann et al., 2018, p.9; OECD, 2015, p.52).

Perhaps the most familiar example of a digital economic activity is making a purchase through electronic commerce (e-commerce). Consumers use an internet-enabled smartphone or personal computer to search and buy products listed on online marketplaces. Payment is made through an e-payment service. The online marketplace automatically sends a notice to an apps-based logistics service, which picks up the product from the supplier's door and delivers the product to the consumer, as the shipment is traced by a specific code and GPS technology. This can be done without any physical exchange of goods and money, and even between suppliers and consumers who are located in different countries, thanks to advances in technology and in internet connectivity.

The digital economy facilitates inclusive economic growth. For example, digital financial services enable cheap and efficient transactions that would otherwise require cash (Manyika et al., 2016) and provide access to the 44.3% of Indonesian adults who do not have a formal financial account (Schueth & Simorangkir, 2018). Digital financial services also create opportunities for women, who have traditionally had unequal access to bank accounts and digital payment channels, including opportunities for access to services like health insurance (Women's World Banking, 2018).

Indonesia has the largest digital economy in the approximately USD 100 billion digital economy across ASEAN countries, accounting for 41% of the total transaction value in the region (Davis et al., 2019). In 2019, the percentage of transaction value was higher than the relative size of Indonesia's overall economy within ASEAN[1], which was 35%. Indonesia's business-to-consumer (B2C) e-commerce market alone was estimated to be worth USD 13.6 billion in 2019. The B2C market was dominated by travel bookings (58.9%), followed by online shopping and retail categories (14.6%) (J.P. Morgan, 2019).

In the first half of 2020, an estimated 630 digital service providers[2] in Indonesia handled USD 41 billion worth of transactions. Electronic commerce (e-commerce) represented more than half of this value, followed by online travel (24%), ride hailing (15%) and online media (10%) (Davis et al., 2019, p.21). One of the most prominent associations in the sector, the Indonesian E-commerce Association (idEA) represents members in ten business fields: banks, classified advertising, daily deals[3], directory[4], digital infrastructure, logistics, marketplaces, individual online retail shops, payment gateways, and travel. This covers virtually all types of online exchange, between business-to-business, business-to-consumer, consumer-to-consumer, consumer-to-business, and even business-to-government (Rosyidi, 2019, p.212).

Gross Merchandise Value (GMV) in the Indonesian digital economy has been growing at an annual rate of over 40% since 2015 and is predicted to reach USD 130 billion by 2025, making it the most promising digital market in Southeast Asia (Davis et al., 2019, p.4). By comparison, the digital economies of Malaysia, Thailand, and Singapore are growing by between 20% and 30%. This rapid development is fueled by 175.4 million internet users (in January 2020) who are increasingly drawn by the efficiency and convenience of e-commerce, online travel bookings, ride-hailing apps, and digital payment. This, in turn, feeds growing investor confidence in the digital sector (We are Social & Hootsuite, 2020; Davis et al., 2019, p.10, 18). The Covid-19 pandemic has accelerated this trend even further. Statistics Indonesia (2020) reported a 42% increase in e-commerce transactions in April 2020 in a socio-demographic survey on Covid-19 impact.

In 2020, the President of Indonesia tasked his cabinet with prioritizing the digital economy's potential for economic growth (Ministry of Finance, 2020). Since the digital economy covers a broad range of business models, in the Center for International Private Enterprise (CIPE) and New Markets Lab developed the *Digital Economy Enabling Environment Guide: Key Areas of Dialogue for Business and Policymakers*, Kulhmann et al. (2018) suggest four key areas to support the development of an enabling environment for inclusive digital economy policy: consumer protection, data privacy, cybersecurity, and e-payment.

"In 2020, the President of Indonesia tasked his cabinet with prioritizing the digital economy's potential for economic growth."

[1] Based on GDP in 2019, processed from a database available at https://data.aseanstats.org/indicator/AST.STC.TBL.5. The top three countries are Indonesia, Thailand, and the Philippines with 35.4%, 17.2% and 11.9% of the value respectively.
[2] There are 86 digital financial companies, 158 fintech lending companies, 51 e-payment companies, six e-signature companies, and 329 e-commerce member companies registered with the Financial Service Authority, the central Bank, the Ministry of Communication and Informatics, and the Indonesian E-commerce Association (idEA) as of August 2020 (OJK, 2020a; OJK, 2020b; BI, 2020; MOCI, 2020a; idEA, 2020).
[3] Daily deals are e-commerce companies that offer discount vouchers valid within a certain time period.
[4] Directory is a platform providing links related to specific information, for example product prices.

This framework of four key policy areas for the digital economy is more extensive and comprehensive than other approaches. For example, Lovelock (2018) suggests targeting the sharing economy, data protection, and cybersecurity, while the Commission for the Supervision of Business Competition or *Komisi Pengawas Persaingan Usaha* (2017) only highlights consumer protection and data protection. The following analysis will apply the four key policy areas approach of the Digital Economy Guide.

Each policy area tackles different, but related issues in the digital economy. At times they overlap, impacting the nation's digital economy. Digital consumer protection safeguards individuals and enterprises from rights violations during electronic transactions (Kulhmann et al., 2018, p.7; Aprilianti, 2020). Data privacy for both consumers and companies aims at protecting individuals' right to privacy. Cybersecurity safeguards information technology and computers from intrusions. E-payments are defined as digitized payment services that facilitate bank and non-bank payments, whether through conventional credit and debit cards or an e-wallet provided by non-bank intermediaries, more popularly known as financial technology (fintech) providers.

"An underlying issue is the need for the government to maintain safety in the digital ecosystem while providing a regulatory framework conducive to innovation."

An underlying issue is the need for the government to maintain safety in the digital ecosystem while providing a regulatory framework conducive to innovation (Rumata & Sastrosubroto, 2020, p.7–9). Regulating the digital economy is especially challenging because of its fast-changing and technical nature, which often results in policies that cannot keep up with or accommodate innovation (Beaumier et al., 2020; OECD, 2019; Bukht & Heeks, 2018, p.9–10). An effective, agile regulatory approach that overcomes this challenge is crucial.

THREE REGULATORY APPROACHES IN THE DIGITAL ECONOMY

Broadly speaking, there are three degrees of responsibility sharing between the industry and the state in the regulatory process: state-controlled, self-regulation, and co-regulation (Latzer et al., 2013; Johns, 2015; Finck, 2017). Each approach has benefits and risks, especially in the digital economy.

The traditional state-controlled model, sometimes referred to as command-and-control or top-down regulation, implies regulation by the state and enforcement through legal rules backed by criminal sanction (Finck, 2017, p.6; Latzer et al., 2013; Johns, 2015, p.3). In this approach, the state imposes policy with a rigid mechanism of one-way monitoring by the government of businesses. The state oversees all aspects of the policy cycle by determining the dos and don'ts for the industry with limited or no input from non-state actors such as associations, business, civil society, and academia (Finck, 2017, p.8).

The state-controlled approach treats the government as though it has all the relevant knowledge about the industry (Finck, 2017, p. 8), but in reality this approach suffers from the near-certainty that reliance on the state's capacity to anticipate and oversee all possibilities will lead to information deficits (Latzer et al., 2013; Finck, 2017, p. 7). Even in more stable and established markets, governments can find it challenging to anticipate all of the relevant scenarios that should inform their regulations. In the digital economy, it is impossible. Rules that fail to anticipate innovations can outlaw them before they can be realized, even if it was not the intention of the offending rule. Rules that are not completely informed may also impose high compliance costs or be difficult or impossible to enforce (Finck, 2017, p. 7).

"The state-controlled approach treats the government as though it has all the relevant knowledge about the industry, but in reality this approach suffers from the near-certainty that reliance on the state's capacity to anticipate and oversee all possibilities will lead to information deficits."

Vietnam's data protection regulation provides a perfect example of the consequences of a state-controlled approach. This regulation was passed without much consultation with the private sector. It mandated data localization and local branch offices, which pose unnecessary barriers to doing businesses. Data localization raises the cost of hosting data by 30–60% and a local branch office will involve, at least, renting physical space, hiring local staff, and securing permits. This regulation was criticized by the Vietnamese public (Cooper & Le, 2018, p. 16; Leviathan Security Group, 2015, p.9–10).

The polar opposite of state-controlled regulation is self-regulation. Under self-regulation, the rules under which an industry operates are developed and enforced by the industry actors themselves (Latzer et al., 2013; Johns, 2015, p.3, Finck, 2017, p.8). The rules may be developed individually or jointly by groups or associations. A common misconception about self-regulation is that it is merely 'self-help' efforts from the industry and 'do-nothing' policy from the state. Even in self-regulation, the state remains involved through the creation of mechanisms that give businesses independence to govern their industry to achieve higher efficiency (Latzer et

al., 2013; Finck, 2017). For example, the state can establish a regulatory framework that allows businesses to develop their own code of conduct on technical issues such as data privacy and leave the detailed provisions to the businesses' responsibility (Johns, 2015, p.3).

> Self-regulation, however, may also open the door to negligence of public interest and anticompetitive business practices, especially when self-regulation is undertaken by large, established players but covers the actions of small and medium enterprises.

Unlike state-controlled regulation, self-regulation tends to be extremely flexible because the businesses affected can make the changes to the rules as necessary to allow innovation or be flexible about implementation to account for burdensome or unrealistic goals. Self-regulation is also much cheaper for the state, which does not need to worry about rule-making, monitoring, or enforcement (Latzer et al., 2013, and Finck, 2017, p.13). Self-regulation, however, may also open the door to negligence of public interest and anticompetitive business practices, especially when self-regulation is undertaken by large, established players but covers the actions of small and medium enterprises (Latzer et al., 2013).

Japan's consumer protection strategy is an example of successful self-regulation within the digital economy. The country's industry-driven regulatory regime is shaped by businesses in cooperation with consumer alliance groups (Lee & Nakaide, 2018). It is supported and guided by the government, which defines the scope and nature of permissible conduct, encourages competition, and sets standards and market segmentation (Lee & Nakaide, 2018). As a result, Japanese consumers are protected by exacting standards of quality.

Co-regulation provides a middle path between state-control and self-regulation. It distributes responsibilities between state and non-state actors. Non-state actors include groups such as companies, industry associations, experts, and civil society. Co-regulation relies on collaboration in the creation, adoption, application, enforcement, and evolution of policies and regulations (Latzer et al. 2013, Finck 2017, p.15; Torfing et al. 2016, p.8; Hirsch, 2010, p.441). It aims to ensure that no single institution controls the entire regulatory process (Latzers et al., 2013; Finck, 2017, p.13).

> Co-regulation provides a middle path between state-control and self-regulation. It distributes responsibilities between state and non-state actors.

In practice, co-regulation is more than a one-time intervention of seeking non-government input during policy creation. Rather, co-regulation is the result of continuous feedback, making it an experimental, mutual, and adaptive process (Finck, 2017, p.18, Torfing et al., 2016, p. 8). The constant dialogue and adaptive environment differentiate co-regulation from other approaches. Implementation and policy enforcement are delegated in whole or in part by the government to the private sector based on mutually agreed upon standards and ongoing dialogue (Finck, 2017, p.24).

Co-regulation has several advantages that make it suitable for the digital economy (Finck 2017; Johns, 2015). First, co-regulation addresses problems of asymmetric or incomplete information

held by governmental and non-governmental actors (Finck, 2017; Johns, 2015). The state lacks the data necessary to establish and maintain an innovation-supporting regulatory climate that also safeguards the public interest (Finck 2017, p.19).

Second, co-regulation can provide a mechanism for dialogue for flexible adaptation to legislative solutions in the new and fast-changing digital economy. Technological changes can happen instantly, requiring immediate changes to business models. While it makes their jobs more challenging, regulators must adapt to sustain and facilitate this innovation.

Lastly, co-regulation facilitates regulatory enforcement when the government delegates enforcement efforts to businesses and both share regulatory responsibilities. The government can, for instance, limit its efforts to setting general rules while leaving the detailed code of conduct to the platforms and/or their associations (Finck, 2017, p.12). It has been observed in the sharing-economy that this may also increase tax compliance rates (Finck, 2017, p.17-18). In Portugal and France, the vacation rental online marketplace Airbnb collected tourist tax payments for the government at much lower costs than when the state had tried to levy them directly.

> “Co-regulation can contribute to more informed decision-making, more efficient and effective regulatory enforcement, and continuous review and assessment of the regulatory process.”

Overall, co-regulation can contribute to more informed decision-making, more efficient and effective regulatory enforcement, and continuous review and assessment of the regulatory process (Finck, 2017, p.29).

Torfing et al. (2016, p.14–15) have identified disadvantages of co-regulation. It can be costly to accommodate continuous interaction. When navigating the different perspectives of involved actors, the process may also introduce the risk of biased participation because groups with more resources, time and energy to participate tend to be better represented and included in dialogue compared to smaller groups with less resources. Latzer et al. (2013, p.385) added that it is difficult to evaluate the performance of co-regulation and to establish causality between co-regulation and the outcome of the reform.

Despite its shortcomings, the potential benefits of co-regulation outweigh its risks. An evaluation conducted by IFC in 30 Asian, African, and European countries found that PPD enabled 400 specific policy reforms in over 50 areas, resulting in USD 400 million in private sector savings (Bettcher et al., 2015, p.3)[5]. Meanwhile, Singapore was successful in using the regulatory sandbox approach in the areas of fintech and personal data protection. It allowed Singapore to quickly respond to corporate innovations and to facilitate the growth of its economy. Singapore remains a regional enabler for digital economic growth, hosting the highest number of headquarters of e-commerce and fintech unicorns in Southeast Asia (Google et al., 2020, p.32).

[5] IFC (2009, p.50-68) commissioned a study in over 50 distinct areas within the business enabling environment, such as taxation system, infrastructure, ICT, and regulatory environment. Annex I of the study mentions specific reforms related to the implementation of a public-private dialogue.

A. Public-Private Dialogue

There are several tools that the government can use to make co-regulation work. Public and private engagement and dialogue are crucial for the success of co-regulation (Torfing et al., 2016, p.11). Public-private dialogue is an instrument for maintaining the effective flow of information (see also Box 2), that should be established before agreeing on the shared responsibility which is the final aim of co-regulation.

> Public-private dialogue is an instrument for maintaining the effective flow of information, that should be established before agreeing on the shared responsibility which is the final aim of co-regulation.

Box 2.
Public-Private Dialogue (PPD) in Co-regulation

Effective communication between state and business is necessary for the success of co-regulation. PPD mechanisms provide a structured, participatory, and inclusive dialogue or series of consultations between the government and the private sector (Kuhlman et al., 2018; Freeman, 2000, p.20–26; OECD, 2007).
PPD has potential benefits such as (Herzberg & Wright, 2013):

- Facilitating reforms, creating momentum, and accelerating the reform process which helps improve investment and development climate;
- Promoting better design of policy reforms through comprehensive problem diagnosis;
- Promoting easier policy reform implementation;
- Promoting transparency and good governance;
- Promoting mutual trust and understanding between public and private sectors;
- Providing governments with a sounding board that can improve the quality of policy-making and enforcement.

PPD also has proven to deliver better results of policy reforms, as PPD provides an opportunity to establish inclusive, participatory, and evidence-based policymaking, increase legitimacy, and consider feedback (Bettcher et al., 2015, p.3).

To some extent, the legal basis for a formalized PPD mechanism exists in the Indonesian Law No. 12/2011 on the Formation of Laws and Regulations, which states in Article 96 that the public has a legitimate right to provide input during the regulatory drafting process. However, guaranteeing this right has not been uniformly or effectively implemented across institutions. As UNDP (2017, p.41) notes, the prevalence and quality of government-led PPDs in Indonesia is still lacking.

In other countries, establishing PPD to increase stakeholders' participation in the policy making and policy enforcement processes for the digital economy has proven successful. The United States

Computer Emergency Readiness Team (CERT) within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency engaged in detailed public-private dialogue sessions to investigate cyber-attacks. Together with Microsoft CERT successfully combated the Waledac botnet virus (Kaijankoski, 2015, p.38) benefitting Microsoft users worldwide. PPD was also implemented when the EU Commission involved a broad range of industry associations, academics, and companies in formulating its policy recommendations for the sharing economy, (Finck, 2017, p.25). The included an online feedback form that allowed EU citizens to express their views at any time.

B. Regulatory Sandbox

Another tool in the co-regulation approach is the establishment of a regulatory sandbox (see Box 3) to create space for innovation and experimentation. This policy option has been implemented in more than 60 jurisdictions, including in Singapore (Jenik & Duff, 2020).

"Another tool in the co-regulation approach is the establishment of a regulatory sandbox to create space for innovation and experimentation."

The Singaporean Personal Data Protection Commission (PDPC) has followed the regulatory sandbox approach in revising the Personal Data Protection Act. According to an official report, PDPC promotes policy co-creation and an industry-supportive framework (PDPC, 2019). The collaboration included policy prototyping to identify areas where policy interventions are needed and to outline policies that respond quickly to advancements in technology and innovation in business models. A private sector committee spent approximately four months formulating policy proposals that were fed into the public consultations by the PDPC (PDPC, 2019). Singaporean experiences with the sandbox approach can inform the process of Indonesian policymaking.

Singapore's regulatory sandbox approach also allows financial institutions and fintech players to test new products and services, while remaining under the oversight of the Monetary Authority of Singapore (MAS). The MAS relaxes specific legal and regulatory requirements for the duration of the sandbox.

As a result of this process, Singapore adopts new technology and drives innovation more rapidly, compared to other Southeast Asian countries. In one instance, Singapore pioneered the early adoption of a unified Quick Response (QR) code technology, which combines multiple QR codes for single payment. Singapore extended the regulatory sandbox approach to test possible changes in the Personal Data Protection Act in 2018 (Denham, 2019).

Box 3.
Regulatory Sandbox as Innovation-Enhancing Tool for Co-regulation

A regulatory sandbox is a policy innovation space for businesses to engage in ideation, iteration, and experimentation within temporary, flexible regulatory or legal frameworks for specific companies (Egan, 2020, p.12–13; Jenik & Duff, 2020). The concept has been promoted since 2012 in the communications sector, specifically television broadcasting. It was found suitable for the digital economy by Johns (2015, p.4) since the regulatory sandbox provides an experimental space and opportunity to co-improve both regulation/standards and business models before they are used on a larger scale. In the digital economy, the regulatory sandbox is commonly used in the fintech industry, but its use can expand to other areas.

With PPD and the regulatory sandbox options, co-regulation can be a suitable policy approach to regulating the digital economy. It can accommodate rapid changes of digital innovation while safeguarding public interests (Finck, 2017, p.19; Johns, 2015).

The next sections outline specific Indonesian policy challenges for the digital economy and how co-regulation can contribute to possible policy solutions.

INDONESIA'S CURRENT REGULATORY FRAMEWORK AND CHALLENGES OF THE DIGITAL ECONOMY

It is difficult to pinpoint when the digital economy first emerged in Indonesia. Even the term 'digital economy' was only coined in 1995 as e-commerce emerged (Johns, 2015). The Directorate of Banking Research and Arrangement at the central bank (Bank Indonesia, 2002, p.38) suggests it began with the introduction of internet banking by a private bank in 1999. Others suggest that it did not exist until 2010 when the first digital start-up was successfully established (Rumata & Sastrosubroto, 2020, p.4). The government began actively issuing regulations meant to govern the digital economy after 2010 when the rapid growth of local e-commerce and ride-hailing startups began disrupting conventional businesses (Nandini, 2019).

As of December 2020, the Indonesian digital economy is regulated by at least 14 government entities, shown in Table 1. While coordination efforts between these entities exist under the National Development Planning Agency (Bappenas) and the Coordinating Ministry of Economic Affairs (CMEA), this has not resulted in comprehensive or coherent policies. For example, despite this coordinating body, the E-commerce Roadmap 2017–2019 was discontinued without any replacement, and the release of the National Cyber Security Strategy has been delayed.

"As of December 2020, the Indonesian digital economy is regulated by at least 14 government entities."

Table 1.
Indonesian Governmental Entities on the Digital Economy

Ministries	Non-ministerial Entities
1. Ministry of Trade (MOT)	8. The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN)
2. Ministry of Communication and Informatics (MOCI)	9. The National Consumer Protection Agency (*Badan Perlindungan Konsumen Nasional* or BPKN)
3. Ministry of Finance (MOF)	10. National Development Planning Agency (Bappenas)
4. Ministry of Home Affairs (MOHA)	11. Financial Services Authority (*Otoritas Jasa Keuangan* or OJK)
5. Ministry of Defense (MOD)	12. Indonesian National Police
6. Ministry of Justice and Human Rights (MOJHR)	13. Bank Indonesia
7. Coordinating Ministry of Economic Affairs (CMEA)	14. The House of Representatives (*Dewan Perwakilan Rakyat* or DPR)

Source: Author's compilation

> There are over 60 laws and regulations governing the four key policy areas in Indonesia's digital economy, and even more ministerial regulations.

The number of regulations affecting the digital economy has increased with the growth of the digital economy. There are over 60 laws and regulations governing the four key policy areas in Indonesia's digital economy, and even more ministerial regulations, such as the Ministry of Transportation Regulation No. 118/2019 on Special Rental Transportation, which regulates popular on-demand transportation platforms. Despite the large number of laws and regulations, some areas remain unregulated, specifically in the areas of data privacy and cybersecurity.

The fragmented institutional and regulatory landscape has brought challenges in each of the following four key policy areas affecting the digital economy.

> Despite the large number of laws and regulations, some areas remain unregulated, specifically in the areas of data privacy and cybersecurity.

A. Consumer Protection

An effective regulatory framework for consumer protection is important not just for consumers, but also for the growth of e-commerce businesses. Between January 2019–May 2020 there were 5,826 cases of online fraud reported to the Indonesian National Police (Directorate of Cyber Crime, n.d.). Many Indonesian consumers do not trust online shopping. More than half of Indonesians associate online shopping with fraud (56%) and more than a third believe that product quality is not reliable (34%) or that payment is not safe or convenient (35%) (Damuri et al., 2017). Effective consumer protection regulations protect consumers and help them feel more comfortable conducting online transactions, supporting the growth of e-commerce businesses.

Consumer protection in Indonesia is regulated under Law No. 8/1999 on Consumer Protection, which will be referred to as General Consumer Protection Law (GCPL). At the time the law was passed, e-commerce was still nascent in Indonesia. Although some GCPL provisions are applicable to e-commerce—such as the right to safety in consuming goods and services—specific digital consumer rights protections remain insufficient, namely digital contracting, consumer-to-consumer transactions, online dispute resolution, and digital products transactions (Aprilianti, 2020, p.23). The course of action and complaint mechanisms available for consumers also remain limited and underutilized (Aprilianti, 2020, p.10).

To fill the regulatory gap between offline and online consumer protection, regulators enacted Government Regulation No. 80/2019 on E-Commerce (E-Commerce Regulation) derived from the Law No. 7/2014 on Trade (Trade Law)[6]. The E-Commerce Regulation covers unique consumer protection issues in e-commerce, such as data collection, electronic advertising, confirmation of electronic transactions, secured electronic payments, shipping, exchange and cancelation procedures, and dispute settlement in electronic trade (Aprilianti, 2020, p.14).

[6] Digital contracting in articles 50–57, borderless dispute resolution in articles 72–75, and digital products transactions in articles 67–68. As for digital non-tangible products and/or services, it imposes a tax regulated through the Ministry of Finance Regulation No. 48.PMK.03/2020 on Procedures to Appoint Collector, Collection as well as Reporting of Value-Added Tax (VAT) on Taxable Non-Tangible Products and/or Services.

The drafting process of the E-commerce Regulation included consultations with private sector players from companies and associations, which indicates that some measure of PPD was already being applied (Interview 3, 5, 9, 11, 12). However, the PPD was limited to more established businesses, resulting in the absence in the regulation of some consumer-to-consumer business models such as online auctions and dropshipping[7].

"The drafting process of the E-commerce Regulation included consultations with private sector players from companies and associations, which indicates that some measure of PPD was already being applied."

The E-Commerce Regulation also introduced licensing requirements for online sellers in order to support consumer protection. This provision is further detailed in MOT Regulation No. 50/2020 on the Provisions of Business Licensing, Advertising, Development and Supervision of Businesses in Trading through Electronic Systems. This regulation was drafted in consultation with industry associations and their members (Interview 2, 3, 5, 9, 11, 13), including some level of PPD. However, the resulting regulation follows a state-controlled approach. Should online sellers fail to obtain a license, the Ministry will give a written warning letter that can be escalated into blacklisting the enterprise or blocking it from selling through online platforms over a course of six months.

The licensing requirement can be problematic since 96% of micro-, small-, and medium-sized businesses in Indonesia are still informal (ILO, 2019, p.33–34; Taufik, 2017, p.371–372). Licenses may become a barrier for micro- and small-sized businesses to access the online market as many of them perceive the licensing process to be too complicated, not beneficial, and too expensive. The rigid state-controlled licensing regulation may discourage businesses from entering the e-commerce market.

"The absence of provisions for some business models and the rigid licensing requirements demonstrate how difficult it is for the Ministry of Trade to protect online consumers without harming industry development.

The absence of provisions for some business models and the rigid licensing requirements demonstrate how difficult it is for the Ministry of Trade to protect online consumers without harming industry development. MOT Regulation No. 50/2020 considers the private sector a group suitable for mentoring and supervision instead of a potentially integral part of the policy enforcement process.

B. Data Privacy

An unprecedented amount of data is created and circulated, nationally and internationally, in the digital economy. Data privacy is important not only for personal privacy, but also for national security. Unfortunately, data privacy enforcement in Indonesia is weak.

[7] Dropshipping is an online retail business model in which the retailer acts as a broker between customers and wholesalers, manufacturers, or other retailers. Dropshippers take the orders from customers but do not hold the items ordered in inventory. Instead, they make an order on the customer's behalf from another merchant or a manufacturer.

> There is no specific regulation targeting personal data privacy in Indonesia. The issue is regulated through at least 32 different laws and regulations

There is no specific regulation targeting personal data privacy in Indonesia. The issue is regulated through at least 32 different laws and regulations, most prominently in Law No. 19/2016 on Electronic Information and Transactions (EIT Law) but also by sector-specific regulations such as the E-Commerce Regulation, regulations on banking, telecommunications, health, population administration, and electronic systems operators (Aprilianti, 2020, p. 15; Simpson & Sotto, 2020). The government also issued Government Regulation No. 82/2012 on the Implementation of Electronic System and Transaction (GR 82/2012), and electronic systems providers were required to comply with GR 82/2012 by 14 October 2017. MOCI Regulation No. 20/2016 on Personal Data Protection in the Electronic System further operationalized the EIT Law.

The EIT Law and MOCI Regulation No. 20/2016 adopted several general principles from the European Union General Data Protection Regulation (GDPR), which sets a global standard of reference for other countries (Kuhlman et al., 2018; Simpson & Sotto, 2020).[8] However, GR 82/2012 and MOCI Regulation No. 20/2016 also contain provisions that are potentially burdensome to the industry, such as data localization. Based on Government Regulation No. 71/2019 on Implementation of Electronic System and Transaction (GR 71/2019), exceptions can be made to data localization requirements if the technology is not available domestically based on the assessment of an expert committee.

Data localization creates a burden for foreign companies that wish to set up business in Indonesia. Vietnam's experience, outlined in the previous section, demonstrates that data localization can raise the cost of hosting data by up to 60%. Data localization also creates a dilemma for businesses from other countries with clearer and better-enforced data privacy policies, since it requires them to store their data in Indonesia where regulations and standards are less well-developed and the data may be less safe.

Underdeveloped data privacy regulations go hand-in-hand with enforcement problems. Gandhi et al. (2018) suggests that industry players do not follow personal data privacy provisions. For example, ridesharing applications fail to encrypt data storage in spite of the requirements in MOCI Regulation No. 20/2016.

MOCI has been preparing a Personal Data Protection (PDP) Bill since 2014 (Karunian, 2020). It is listed in the 2020 National Legislative Program, meaning it is supposed to be passed in the

> MOCI has been preparing a Personal Data Protection (PDP) Bill since 2014.

[8] However, it falls short of recognizing important concepts such as data controller, data processor, sensitive personal data, dedicated data protection officers, privacy by design, and automatic processing (Simpson & Sotto, 2020). Even the definition of "strategic electronic data" that must be protected also remains unclear, which leaves it open to interpretation and makes enforcement problematic.

mentioned year. However, as of December 2020, the bill is still being discussed in parliament. MOCI, businesses, associations, and independent experts (Uddarojat, 2020; Interview 1, 3, 6, 12) claim that business views have been included in the bill's deliberation process and content. So far, at least three dialogues have been conducted between the parliament (DPR RI), academics, and business associations such as the Indonesian E-commerce Association (idEA), the Indonesian Financial Technology Association (AFTECH), the PDP Advocacy Coalition, and four others[9] (Rizkinaswara, 2020b; Interview 6; DPR RI, 2020). The government is engaged in some level of PPD, at least during the legislative drafting process. The industry appears hopeful that stakeholder views will be accommodated in the law when it is finally passed (Interview 1, 3, 5, 7, 12).

> The government is engaged in some level of PPD, at least during the legislative drafting process.

The draft bill[10] follows European GDPR provisions (Interview 1, 3, 6, 12). It clearly defines and classifies personal data into two categories: general and specific, and it provides examples for each. Cross-border data transfers are allowed with a minimum level of protection for data subjects, but there is no article requiring internal controls. Data privacy officers[11] must only reside on Indonesian territory if the business involves large-scale data processing. The PDP bill explicitly encourages associations to establish guidelines on data privacy while setting a minimum level of protection expected. This suggests a minimum level of co-regulation between the government and the private sector.

C. Cybersecurity

Cyberattack cases have been growing more common in Indonesia. From January to April 2020, BSSN (2020a) found 88,414,296 cyberattacks, made up of 56% trojan activities and 43% information collection cases. The number of cases peaked in March 2020 with 3,344,470 attacks, when the Covid-19 pandemic forced people to start working from home. These attacks can harm consumers, industry, as well as government.

> Indonesia is ranked 41st among 193 countries in the Global Cybersecurity Index (GCI)

Indonesia is ranked 41st among 193 countries in the Global Cybersecurity Index (GCI) (International Telecommunication Union, 2019, p.58). The GCI is an international index measuring countries' commitment to cybersecurity based on legal, technical, organizational, capacity building, and cooperation aspects. Compared to other Southeast Asian countries, Indonesia ranks lower than Singapore, Malaysia, and Thailand.

> Compared to other Southeast Asian countries, Indonesia ranks lower than Singapore, Malaysia, and Thailand.

[9] The records of the business associations can be accessed on the official parliamentary website.
[10] September 2019 version is available at https://aptika.kominfo.go.id/wp-content/uploads/2019/09/RUU-PDP..pdf
[11] The officers have at least four responsibilities as explained in Article 45: (1) advising personal data controller or processor on the PDP Law; (2) monitoring and ensuring the Law's compliance; (3) advising on PDP impact assessment and monitoring the performance of personal data controller and processor; and (4) coordinating and acting as a contact person for problems related to PDP, this include conducting consultation on PDP risks mitigation. There is no detail on what is considered large-scale volume of transactions or firm size. More details on the officers will be included in a Government Regulation which will act as the implementing regulation for the PDP Law as suggested by Article 46 point (3) in the Bill.

Between May and August 2020 alone, personal data of customers of two e-commerce marketplaces and a credit company were stolen, affecting data 15 million (Rizkinaswara, 2020a), 1.2 million (MOCI, 2020b), and 800,000 (Annur, 2020) users respectively. Hackers sold the data on online platforms, which potentially results in identity theft and fraud. From January 2019 to May 2020, 182 cases of identity/data theft were reported to the Indonesian National Police (Directorate of Cyber Crime, n.d.). Risks associated with the growing number of online transactions indicates the urgency of effective regulation and enforcement to strengthen cybersecurity.

Despite the increasing threat to cybersecurity, there is no dedicated law regulating cybersecurity in Indonesia. Cybersecurity is mainly regulated in the EIT Law and GR82/2012. However, the provisions remain limited, as the EIT Law covers only cybercrimes in the form of information and document interception, while GR82/2012 covers only electronic transaction-related cybercrimes such as malicious codes or viruses.

Cybersecurity provisions also exist under ministerial regulations such as MOCI Regulation No. 20/2016 and Joint MOCI Regulation No. 26/2015 and MOJHR Regulation No. 14/2015 on the Implementation of Closing Down Content and/or a User's Rights to Access over Copyright Infringement and/or Related Rights in an Electronic System. Both regulations have an even narrower focus as they are derived from GR82/2012. MOCI Regulation No. 20/2016 focuses on the illegal utilization of personal data while the joint regulation covers only digital intellectual property theft. Sectoral regulations further complicate the landscape. In financial services, for example, OJK acts as the cybersecurity regulator through its Regulation No. 13/POJK.02/2018 on Digital Financial Innovation in Financial Service.

This complex regulatory landscape is plagued by fragmented authorities spread across different institutions. This leads to discretionary enforcement (Interview 6, 8, 9, 16), where government officials choose whether to punish the violation of a law on a case-by-case basis rather than according to transparent, knowable rules, opening the door to corruption.

"Many business practitioners, academics, and policymakers believe the bill should not impose additional burdens to businesses and, instead, focus on establishing coordination mechanisms among institutions, implementing a multi-stakeholders approach through its drafting process."

Ongoing cyberattacks illustrate the need for an effective cybersecurity law. In mid-2019, the DPR published a draft[12] Cybersecurity and Cyber Resilience Bill (*Rancangan Undang-undang Keamanan dan Ketahanan Siber* or RUU KKS), which aims to create an overarching cybersecurity regulation. The bill was widely criticized by businesses because it contains cumbersome provisions (Interview 8, 16, 17). Among these are: mandatory human resources competency certification issued by the BSSN and empowering the agency to monitor "destructive and negative contents and electronic applications". This monitoring power is as strong as the authority granted to the MOCI in the EIT Law. Many business practitioners, academics, and policymakers believe the bill should not impose additional burdens to businesses and, instead, focus on establishing coordination mechanisms among institutions, implementing a multi-stakeholders approach through its drafting process (Interview 6, 8, 12, 14, 16, 17). The bill must also align with a National Cyber Security Strategy, which was in the drafting process in October 2020 (Interview 14, 16).

[12] May 2019 version is available at http://institute.id/wp-content/uploads/2019/09/RUU-Keamanan-dan-Ketahanan-Siber.pdf

The bill provoked an online petition opposing it[13], signed by over 6,000 people. The petition highlighted insufficient public consultations, since the draft was only released to the public in the month when it was supposed to be passed. Juniarto (2019), business players, and experts (Interviews 7, 8, 15, and 16) criticized the bill for consulting only selected academics in its drafting; a claim also made by the petition. Even related institutions such as MOCI, Bappenas, and the Indonesia Computer Emergency Response Team (ID-CERT)—an independent technical coordination team handling internet network incidents in Indonesia—were not involved in the discussion (Interview 6, 15, 16). The bill has since been dropped from the 2020 Legislative Agenda (*Program Legislatif Nasional* or Prolegnas) of the Parliament.

D. E-Payments

While Cash-On-Demand still dominates payment methods in e-commerce, making up almost 84% of payments, the e-payment sector in Indonesia is growing and innovative; between 2018 and 2020, electronic money transfers grew by 307% to IDR 47.2 trillion (USD 3.31 billion) (Statistics Indonesia, 2019; East Ventures, 2020 p. 35). This growth needs to be accompanied by a regulatory framework that supports innovation while maintaining payment safety.

The two main government entities responsible for regulating e-payment in Indonesia are the central bank (BI) and the Financial Services Authority (OJK). BI is responsible for maintaining the smooth operation of the payment system, which includes bank and non-bank e-payments. To achieve an integrated e-payment system, BI mapped the regulatory framework in Indonesia Payment Systems Blueprint 2025. The Blueprint sets out the policy context, the 2025 vision, and the roadmap of e-payment, including stakeholder involvement (BI, 2019; Interview 10).

Since e-payment is a form of financial technology or fintech, the regulations fall under the OJK and were tested in a regulatory sandbox, specifically OJK Regulation No. 77/2016 and No. 13/2018. OJK allowed fintech and e-payment services to operate under its supervision without a permit for a maximum of one year after registration (with a possible extension for six months). At the end of this period, the fintech business may be approved or asked to alter their business to fit the criteria, such as suitability assessment on the business's risk and safety management based on OJK Regulation No. 13/2018 (Prime Consultancy, 2020, p.11). Frequent discussions occur between businesses, associations, and regulators during the regulatory sandbox period.

BI and OJK are considered receptive to new technologies and open for collaboration with the private sector (Interview 1, 2, 5, 9). Regular meetings to discuss technology issues between digital companies and government (represented by BI and OJK) are usually initiated by associations, such as AFTECH and Indonesian Payment System Association (Asosiasi Sistem Pembayaran Indonesia or ASPI) (AFTECH, 2020a; AFTECH, 2020b; AFTECH, 2020c; ASPI, 2018; ASPI, 2020; Interview 3, 9, 10). These associations act as a bridge between the regulators and businesses,

[13] The petition can be accessed at https://www.change.org/p/dewan-perwakilan-rakyat-tolak-ruu-kks-ruu-kks-bermasalah

especially to provide inputs for the fintech policy-making process (Prime Consultancy, 2020, p.12). Co-regulation is also embodied in the recognition by OJK of the codes of conduct drafted by the associations (Prime Consultancy, 2020, p.12; Yuniarti & Rasyid, 2020, p.4; Hidajat, 2019, p.280).

"As the independent institution responsible for regulating, overseeing, examining and investigating financial services, OJK has successfully carried out co-regulation practices in the fintech sector by explicitly involving the associations under its regulation."

As the independent institution responsible for regulating, overseeing, examining and investigating financial services, OJK has successfully carried out co-regulation practices in the fintech sector by explicitly involving the associations under its regulation. AFPI and AFTECH are formally acknowledged by OJK Regulation 77/2016 and 13/2018 as associations with the authority to manage business permits.

The comprehensive regulatory framework through the e-payment blueprint, regulatory sandbox, and co-regulation with the industry provides insights on the flexibility needed to balance business growth with safeguarding the public. These three mechanisms oversaw increasing e-payment transaction volume in Indonesia, which grew almost threefold from 2017 to 2020 (Statista, 2020b).

Despite a regulatory environment conducive to e-payments, problems remain when online consumers use e-payment for transactions (J. P. Morgan, 2019; Singh et al., 2013, p. 28). Unsafe e-payment transactions covering carding (credit card fraud) and the theft of payment data are popular, since credit cards are the dominant payment method when shopping online in Indonesia. Bank transfers and digital wallets are the second and third most important payment methods (J. P. Morgan, 2019). Singh et al. (2013, p.28) highlighted Indonesia among twelve countries that are prone to carding.

IMPROVING THE REGULATORY FRAMEWORK FOR THE INDONESIAN DIGITAL ECONOMY

Regulating the digital economy is complex because of the rapid pace of innovative transformation that gives rise to new products, services, and business models. Balancing consumer protection, government intervention, and business growth calls for increased collaboration, inclusion, and compliance. Involving businesses in regulatory design and implementation is critical to ensure protection without undermining growth in the digital economy.

While the policy-making process in some areas of Indonesia's digital economy has begun to incorporate co-regulation, especially through PPD and regulatory sandboxes, challenges remain for the regulatory framework. PPD as it is being employed leaves new business models out of the conversation, regulations continue to create undue burdens for the private sector, and enforcement and compliance are both lacking. Improvements are necessary to strengthen the regulatory framework governing Indonesia's digital economy, starting with a legislative commitment that binds policy-makers to the PPD process (Herzberg & Wright 2006, p.21–22).

Co-regulation would help bring about these improvements, beginning with an agreement between regulators and firms that they have a mutual interest in promoting innovation while ensuring reliable business practices that protect users (Johns, 2015, p.3–5; Cannon & Chung, 2014; MOCI, 2020c; BSSN, 2020b; Interview 1, 2, 3, 5, 6, 7).

Co-regulation provides an opportunity for continuous, transparent collaboration between public and private actors that can address the challenges outlined above. Government entities with relevant authority in the four key policy areas should use their authority to gather information from businesses and set minimum general standards while leaving technicalities to the businesses. They should also share responsibility for policy enforcement and monitor policy implementation to ensure that it balances public and private interests. Finally, to make co-regulation sustainable, an evaluation mechanism needs to be created (Latzer et al., 2013, p. 385) that establishes avenues for continuous improvement of the co-regulation approach.

Three key reforms are suggested to bolster co-regulation in the Indonesian digital economy: integrate an effective public-private dialogue into the policy-making process, establish a flexible mechanism with shared responsibilities on both sides, and continuously monitor and evaluate the co-regulation process.

“Three key reforms are suggested to bolster co-regulation in the Indonesian digital economy: integrate an effective public-private dialogue into the policy-making process, establish a flexible mechanism with shared responsibilities on both sides, and continuously monitor and evaluate the co-regulation process.”

A. Improving Public-Private Dialogue

As mentioned above, citizens' rights to give verbal or written input into the drafting of regulations is protected by Law No. 12/2011. Input is provided through public hearings, official visits to the regulators, information sessions, seminars, workshops, and/or discussions (Interview 3, 5, 9,

10, 11, 16). While this law already serves as the legal basis for PPD, it does not yet capture the principles of effective PPD. According to this law, the drafting process for every regulation should be accessible to the public, but it does not specify what constitutes effective dialogue, a continuous channel for extending input, or what happens if the government fails to provide these tools to facilitate feedback. This last point is key: a failed PPD process should have legal consequences. For example, regulations that fail to provide a functional PPD process or a monitoring framework could be rendered void.

Lessons learned from the public perception of deliberations for the EIT Law as closed and the shortcomings that caused public opposition to and the cancellation of advancement for the Cybersecurity and Cyber Resilience Bill should inform the creation of general principles for effective public-private dialogue.

Twelve principles to ensure that a public-private dialogue is effective, outlined in Box 4, should guide future revisions of Law No. 12/2011.

Box 4.
Principles of Effective PPD in the Digital Economy Policy-making Process

Herzberg & Wright (2013, p.19) present 12 general principles for conducting PPD:

1. Assessing the optimal mandate (formal or legal mandate) and relationship with existing institutions (Sen, 2015);
2. Deciding who should participate under a flexible, balanced structure (Sen, 2015);
3. Identifying the right champions from both public and private sectors (Sen, 2015), and helping them to push for reforms;
4. Engaging the right facilitator;
5. Choosing and reaching target outputs;
6. Devising a communications and outreach strategy;
7. Elaborating a monitoring and evaluation framework;
8. Considering the potential for dialogue on a sub-national level, try to involve micro-, small- and medium-enterprises (SMEs), and other local stakeholders (Sen, 2015);
9. Focusing on a specific topic in each dialogue, and linking it to a broader framework;
10. Linking sector-specific and locally conducted PPD to cross-border and international PPD sessions;
11. Recognizing the specificities and potential of dialogue in post-conflict or crisis environments; and
12. Involving stakeholders of international development projects in locally coordinated PPD sessions based on the initiative of local partners and beneficiaries.

Herzberg and Wright formulated these principles for international development projects, but they also provide a useful guide for PPD in the digital economy.

As the Coordinating Ministry for Economic Affairs (CMEA) maps the regulations and institutions that regulate the digital economy, a continuous dialogue on sharing response prevents overlapping regulations that inflate compliance risks and costs. For example, both the EIT Law and the E-Commerce Regulation stipulate what kinds of data can be collected and how they can be stored and processed in electronic transactions (Aprilianti, 2020, p.13–14). Continuous dialogue should also reduce potential for corruption created by discretionary enforcement (Surianta, 2020, p.5).

Inclusivity within the dialogue is an important factor (Torfing et al., 2016, p.14–15). Indonesian e-commerce associations that are involved in the policy dialogue largely represent medium-sized and big companies. An inclusive PPD can help address exclusion problems and the problems that stem from them, such as overly burdensome online licensing requirements that act as barriers to entry. PPD can also address the information asymmetry on new e-commerce models, like auctions and dropshipping. Through including new business models in the PPD, the government can be better informed on the latest development in the digital economy and be better prepared to respond.

“An inclusive PPD can help address exclusion problems and the problems that stem from them, such as overly burdensome online licensing requirements that act as barriers to entry.”

Including representatives from SMEs, big corporations, academia, civil society organizations, and even the media adds different perspectives to the process, which should improve outcomes. Relevant stakeholders need to be able to voice their interests and the disproportional influence of large companies needs to be countered and avoided if possible (Finck, 2017, p.19; Torfing et al., 2016, p.10). This is why the principles of an effective PPD (Box 4) include representing SMEs in the process.

The process of an effective dialogue requires time. To allow for an inclusive and robust discussion, regulators should consider and stipulate a dialogue period for any draft legislation being proposed.

Indonesian Law No. 12/2011 on the Formation of Laws and Regulations needs to be extended beyond external input to the legislative process to reaffirming the legal role of PPD in the policy-making process. The law should be revised to invalidate regulations for which dialogue was not carried out effectively during drafting and to require effective dialogue to involve multiple stakeholders within a reasonable timeframe. Ideally, this should include digital tools to enable online contributions by stakeholders.

“Indonesian Law No. 12/2011 on the Formation of Laws and Regulations needs to be extended beyond external input to the legislative process to reaffirming the legal role of PPD in the policy-making process.”

Non-governmental actors were invited to contribute during the drafting of the Personal Data Protection (PDP) Bill and provided room for amendments (Interview 1, 7). It is expected that this PPD effort will make the enforcement easier because businesses were involved and generally informed in the drafting process. However, more dialogue is needed to clarify ambiguous

specifications regarding personal data in the PDP Bill and the Population Administration Law.

Ideally, legislators should apply digital tools to accommodate broad public input towards potential legislation as suggested by Herzberg & Sisombat (2016, p.19–20) and ParlAmericas (n.d., p.10–11). This allows SMEs and even the general public to participate in the dialogue. It also helps to maintain the dialogue during a public health crisis like the Covid-19 pandemic. Document repositories and online consultation portals applied in other countries can serve as references. For instance, in Canada legislators have held e-consultations with their constituents (ParlAmericas, n.d., p.33–37).

The Indonesian parliament has embarked on the Open Parliament Indonesia National Action Plan 2018–2020[14]. The plan includes a dedicated website and a mobile phone application with up-to-date information on legislative efforts that are underway in order to facilitate public participation. The mobile application was supposed to be launched in September 2020 but there was no update as of December 2020.

By providing a legal definition of what is considered an effective dialogue, the revised law would demonstrate the government's commitment to incorporating non-governmental voices into the legislative process, including those from business, academia and civil society.

B. Improving the Regulatory Sandbox

After ensuring an effective dialogue, a flexible regulatory framework is necessary to allow for an innovative business climate (Finck, 2015, p. 20–21). A regulatory sandbox helps determine the scope of responsibility and the level of flexibility. It allows both regulators and businesses to test run regulatory provisions before they become a formal part of the regulatory framework. The experience of Singapore, which uses a regulatory sandbox approach and adopts new technology and innovation rapidly compared to other Southeast Asian countries, can offer lessons for Indonesia.

> A regulatory sandbox helps determine the scope of responsibility and the level of flexibility. It allows both regulators and businesses to test run regulatory provisions before they become a formal part of the regulatory framework.

Because 14 government entities are involved in regulating Indonesia's digital economy, the regulatory framework is not only rigid—multiple entities must make changes to comprehensively address a problem—but complex and with unclear, overlapping responsibilities. Changes in software application and process technologies happen more quickly than policy-makers can adapt regulation. In digital consumer protection, The GCPL, EIT Law and the E-commerce Regulation all cannot accommodate new online business models like dropshipping.

Complex regulation also leads to enforcement problems. To address this, co-regulation clearly distributes responsibility between government entities and non-governmental actors and establishes sanctions for rule violation. The draft PDP Bill stipulates data privacy provisions but also calls on associations to establish technical guidelines for expected protection levels.

[14] The plan is available at http://www.dpr.go.id/doksetjen/dokumen/-Rencana-Aksi-NAP-Open-Parliament-Indonesia-2018-2020-1553660195.pdf

Responsibility should also be shared with business players in the areas of consumer protection and cybersecurity. Formally shared responsibility between the government and the private sector in the Cybersecurity and Cyber Resilience Bill, currently being deliberated, has been demanded by stakeholders from MOCI, BSSN, academia, and businesses (Interview 6, 8, 12, 14, 16, 17).

C. Improving Evaluation

Finally, establishing monitoring and evaluation mechanisms that involve the private sector once regulations are in force (*ex-post*) are required both to improve co-regulation and to make policy process sustainable and iterative.

There is no ideal evaluation model for co-regulation, which is still in its infancy (Latzer et al., 2013, p.391). Evaluating co-regulation is difficult in part because it is hard to establish a causal relationship between policy outcomes and the PPD and co-regulation process (Herzberg & Sisombat, 2016, p.19–20). To address this difficulty and seek a better evaluation process, monitoring and evaluation should include periodic, on-the-record, and transparent reviews by stakeholders (Herzberg & Wright, 2013, p.24). Perhaps fittingly, co-regulation and PPD can help address the very problems that plague their evaluation.

“Establishing monitoring and evaluation mechanisms that involve the private sector once regulations are in force (*ex-post*) are required both to improve co-regulation and to make policy process sustainable and iterative.”

D. Concluding Remarks

Indonesia's digital economy has experienced the fastest growth among Southeast Asian countries in 2019. The following year, the Covid-19 pandemic accelerated digitalization and caused a higher rate of adoption which expands economic opportunities for many Indonesians. This trend carries a huge potential for economic recovery and even economic growth. However, current regulatory deficiencies in the digital economy may stifle this potential. To create an enabling environment that will realize the expected growth, an inclusive digital economy policy is needed in the key areas of consumer protection, data privacy, cybersecurity, and e-payments.

When it comes to the regulatory process, co-regulation is the most promising approach for designing and enforcing a safe, inclusive, and adaptive policy in those four key areas amid the rapidly changing digital economy landscape. If Indonesia can successfully improve its regulatory landscape through effective co-regulation, it will not only create a safer environment for consumers, it will also facilitate the growth of existing businesses as well as encourage more business players especially micro-, small-, and medium- enterprises to enter the digital economy.

“When it comes to the regulatory process, co-regulation is the most promising approach for designing and enforcing a safe, inclusive, and adaptive policy in those four key areas amid the rapidly changing digital economy landscape.”

REFERENCES

AFTECH, see Asosiasi Fintech Indonesia or the Indonesian Fintech Association

Annur, C.M. (2020). *1,2 Juta Data Pengguna Bhinneka Dikabarkan Diretas. Kata Data*. https://katadata.co.id/agungjatmiko/digital/5eb8c77dc127b/12-juta-data-pengguna-bhinneka-dikabarkan-diretas

Aprilianti, I. (2020). Protecting People: Promoting Digital Consumer Rights. *CIPS Policy Paper No. 27*. https://www.cips-indonesia.org/digital-consumer-rights-pp27

Asosiasi Fintech Indonesia. (2020a). *AFTECH Power Breakfast.* https://fintech.id/news-detail/AFTECH%20CMO%20Power%20Breakfast

Asosiasi Fintech Indonesia. (2020b). *Indonesia Fintech Summit & Expo*. https://fintech.id/ifse

Asosiasi Fintech Indonesia. (2020c). *Fintech Corner*. https://drive.google.com/file/d/1kr79TqUOl9GqTLRZil6aJVUqh54mleMb/view

Asosiasi Sistem Pembayaran Indonesia. (2018). *Kegiatan ASPI - 2018*. https://www.aspi-indonesia.or.id/laporan-kegiatan

Asosiasi Sistem Pembayaran Indonesia. (2020). *Kick-Off Meeting Pembentukan WG Nasional Open API.* https://www.aspi-indonesia.or.id/berita/kickoff-meeting-pembentukan-wg-nasional-open-api

ASPI, see Asosiasi Sistem Pembayaran Indonesia or the Indonesian Payment System Association

Bank Indonesia. (2002). Internet Banking di Indonesia. *Buletin Ekonomi Moneter dan Perbankan Bank Indonesia,* 5(1).

Bank Indonesia. (2019). *Indonesia Payment Systems Blueprint 2025*. https://www.bi.go.id/en/publikasi/sistem-pembayaran/riset/Pages/Blueprint-Sistem-Pembayaran-Indonesia-2025.aspx

Bank Indonesia. (2020). *Daftar Penyelenggara Uang Elektronik yang Telah Memperoleh Izin dari Bank Indonesia Per 27 Mei 2020*. https://www.bi.go.id/id/sistem-pembayaran/informasi-perizinan/uang-elektronik/penyelenggara-berizin/Contents/Default.aspx

Beaumier, G., Kalomeni, K., Campbell-Verduyn, M., Lenglet, M., Natile, S., Papin, M., Rodima-Taylor, D., Silve, A. and Zhang, F. (2020). Global Regulations for a Digital Economy: Between New and Old Challenges. *Glob Policy, 11*: 515-522. https://doi.org/10.1111/1758-5899.12823

Bettcher, K. E., Herzberg, B., & Nadgrodkiewicz, A. (2015). *Public-private dialogue: the key to good governance and development.* Center for International Private Enterprise & World Bank Group. http://www. cipe. org/publications/detail/publi c-private-dialogue-key-good-governance-and-development.

BI, see Bank Indonesia

BSSN, see the National Cyber and Crypto Agency

Cannon, B., & Chung, H. (2014). *A framework for designing co-regulation models well-adapted to technology-facilitated sharing economies*. Santa Clara Computer & High Tech. LJ, 31, 23.

Cooper, G. & Le, H. (2018). *Vietnam's New Cybersecurity Law: A Headache in the Making?* Duane Morriss. https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf

Damuri, Y.R., Negara, S.D., & Azali, K. (2017). *Indonesia's E-Commerce: A New Engine of Growth?* [Presentation]. Symposium on E-Commerce, ASEAN Economic Integration, and Competition Policy & Law. https://asean-competition.org/research/uploads/admin-f88de83727/files/blogs/23092018/batch2/Indonesia%20

Country%20Study_Damuri%20Negara%20Azali.pdf

Davis, S., Saini, S., Sipahimalani, R., Hoppe, F., Lee, W., Girona, IM., Choi, C., Smittinet, W. (2019). *e-Conomy SEA 2019: Swipe up and to the right: Southeast Asia's $100 billion internet economy*. Google, Temasek & Bain Mobile, Consumer Insight. https://www.thinkwithgoogle.com/intl/en-apac/tools-resources/research-studies/e-conomy-sea-2019-swipe-up-and-to-the-right-southeast-asias-100-billion-internet-economy/

Denham, E. (2019). *Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice*. Information Policy Center. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection__constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf

Dewan Perwakilan Rakyat Republik Indonesia (The Indonesian House of Representative (2020). RUU tentang Perlindungan Data Pribadi (*Personal Data Protection Bill*). http://www.dpr.go.id/uu/detail/id/353

Directorate of Banking Research and Arrangement at the Central Bank of Indonesia, see Bank Indonesia

Directorate of Cyber Crime (n.d.). *Statistik Laporan*. Patroli Siber. https://patrolisiber.id/statistic

DPR RI, see Dewan Perwakilan Rakyat Republik Indonesia

East Ventures. (2020). East Ventures Digital Competitiveness Index 2020. *Insight Report*. https:// east-ventures-reports.s3-ap-southeast-1.amazonaws.com/EV-DCI-2020-ENG.pdf

Egan, E. (2020). *Charting A Way Forward, Communicating About Privacy: Towards People-Centered and Accountable Design*. Facebook. https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf

Finck, M. (2017). Digital Regulation: Designing a Supranational Legal Framework for the Platforms Economy. *LSE Law, Society and Economy Working Papers,* 15/2017.

Freeman, J. (2000). The Private Role in Public Governance. *New York University Law Review*, 75(101),1-109.

Gandhi, A., Sucahyo, Y. G., & Ruldeviyani, Y. (2018, July). *Investigating the protection of customers' personal data in the ridesharing applications: A desk research in Indonesia*. In 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 118-121). IEEE.

Google, Temasek, & Bain. (2020). *E-Conomy SEA 2020 At full velocity: Resilient and racing ahead*. https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf

Heeks, R. & Bukht, R. *Digital Economy Policy in Developing Countries* (2018, February). DIODE Working Paper no. 6, 2018, Available at SSRN: https://ssrn.com/abstract=3540027 or http://dx.doi.org/10.2139/ssrn.3540027

Herzberg, B., & Wright, A. (2006). *The PDD handbook: a toolkit for business environment reformers (No. 39115, pp. 1-208).* The World Bank.

Herzberg, B. & Wright, A. (2013). *The PPD Handbook: A Toolkit for Business Environment Reformers*. Public Private Dialogue. http://www.publicprivatedialogue.org/tools/PPDhandbook.pdf

Herzberg, B., & Sisombat, L. (2016). State of Play—Public-Private Dialogue. World Bank.

Hidajat, T. (2019). *Unethical practices peer-to-peer lending in Indonesia*. Journal of Financial Crime. Available at https://www.emerald.com/insight/content/doi/10.1108/JFC-02-2019-0028/full/html?skipTracking=true

Hirsch, D. D. (2010). *The Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation.* Seattle UL Rev., 34, 439.

idEA, see Indonesian E-Commerce Association

IFC, see International Finance Corporation

ILO, see International Labour Organization.

Indonesian E-Commerce Association. (2020). *Direktori Keanggotaan*. https://www.idea.or.id/direktori-member

International Finance Corporation (April 2009). *Review of World Bank Group Support to Structured Public-Private Dialogue for Private and Financial Sector Development*. http://www.publicprivatedialogue.org/workshop%202009/Review%20of%20World%20Bank%20Group%20Support%20to%20PPD%20-%20April%202009.pdf

International Labour Organization. (2019). *Financing Small Businesses in Indonesia.* https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-jakarta/documents/publication/wcms_695134.pdf

International Telecommunications Union (2019). *Global Cybersecurity Index 2018*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Jenik, I. & Duff, S. (2020). *How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers.* Consultative Group to Assist the Poor/The World Bank. https://www.cgap.org/sites/default/files/publications/2020_09_Technical_Guide_How_To_Build_Regulatory_Sandbox.pdf

Johns, N. (2015). Regulating the Digital Economy. *Observer Research Foundation, 6(2).*

J.P. Morgan. (2019). *E-commerce Payments Trends: Indonesia. Indonesia e-commerce insights*. https://www.jpmorgan.com/merchant-services/insights/reports/indonesia

Juniarto, D (2019). Statement on social media Twitter @damarjuniarto and @safenetvoice on 25th September. https://twitter.com/DamarJuniarto/status/1176860066823065601?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1176860657624346624%7Ctwgr%5E&ref_url=https%3A%2F%2Finetdetik.com%2Fsecurity%2Fd-4723195%2Fkontroversi-ruu-keamanan-siber-dikuliti-ini-poin-pentingnya

Kaijankoski, E. A. (2015). *Cybersecurity information sharing between public private sector agencies*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA. https://core.ac.uk/download/pdf/36737334.pdf

Karunian, A.Y. (2020). *Kawal Pembahasan RUU Pelindungan Data Pribadi, Koalisi Advokasi RUU PDP serahkan usulan DIM Alternatif kepada DPR RI*. Elsam. https://elsam.or.id/kawal-pembahasan-ruu-pelindungan-data-pribadi-koalisi-advokasi-ruu-pdp-serahkan-usulan-dim-alternatif-kepada-dpr-ri/

Komisi Pengawas Persaingan Usaha (2017). *The Digital Economy in Indonesia. In cooperation with Australia Indonesia Partnership for Economic Governance*. http://eng.kppu.go.id/wp-content/uploads/REPORT_Digital_Economy_27-December-2017-FINAL.docx.pdf

Kulhmann, K., Glaub, M., Wang, M., Tomar, L. (Ed). (2018). *Digital Economy Enabling Environment Guide: Key Areas of Dialogue for Business and Policymakers.* CIPE Guides and Tools. https://www.cipe.org/resources/digital-economy-enabling-environment-guide-key-areas-of-dialogue-for-business-and-policymakers/

Latzer, M., Just, N., & Saurwein, F. (2013). *Self-and co-regulation.* Routledge handbook of media law, 373. https://www.researchgate.net/publication/260793886_Self-_and_co-regulation_Evidence_legitimacy_and_governance_choice

Lee, H., Nakaide, S. (2018). Financial Consumer Protection in Japan. *An International Comparison of Financial Consumer Protection*. T.-J. Chen (ed.). https://doi.org/10.1007/978-981-10-8441-6_9

Leviathan Security Group. (2015). *Quantifying the Cost of Forced Localisation*. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

Lovelock, P. (2018). *Framing Policies for the Digital Economy: Towards Policy Frameworks in the Asia-Pacific.* UNDP Global Centre for Public Service Excellence. https://www.undp.org/content/undp/en/home/librarypage/capacity-building/global-centre-for-public-service-excellence/DigitalEconomy.html

Manyika, J., Lund, S., Singer, M., White, O., Berry, C. (2016) *How digital finance could boost growth in emerging*

economies. McKinsey. https://www.mckinsey.com/featured-insights/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies#

Ministry of Communications and Informatics. (2020a). *Penyelenggara Sertifikasi Elektronik*. https://tte.kominfo.go.id/

Ministry of Communications and Informatics. (2020b). *Ratusan Ribu Data Bocor, Kominfo Minta Kreditplus Buka Suara*. https://aptika.kominfo.go.id/2020/08/ratusan-ribu-data-bocor-kominfo-minta-kreditplus-buka-suara/

Ministry of Communications and Informatics. (2020c). *Startup Studio Indonesia, Komitmen Kominfo Fasilitasi Startup untuk Akselerasi Bisnisnya.* https://aptika.kominfo.go.id/2020/08/startup-studio-indonesia-komitmen-kominfo-fasilitasi-startup-untuk-akselerasi-bisnisnya/

Ministry of Finance (2020) *Presiden: Indonesia Tidak Boleh Tertinggal Kemajuan Ekonomi Digital*. https://www.kemenkeu.go.id/publikasi/berita/presiden-indonesia-tidak-boleh-tertinggal-kemajuan-ekonomi-digital/

MOCI, see Ministry of Communications and Informatics

Nandini, A.F. (2019). *Kebijakan Deregulasi untuk Startup Digital Indonesia*. Kominfo. https://jdih.kominfo.go.id/monografi_hukum/monografi/unduh/3.

National Cyber and Crypto Agency. (2020a). *Rekap Serangan Siber (Januari – April 2020)*. Badan Siber dan Sandi Negara. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

National Cyber and Crypto Agency. (2020b). *BSSN Ajak Kolaborasi Seluruh Sektor Industri Digital pada Pekan Industri 4.0 Yogyakarta*. Badan Siber dan Sandi Negara. https://bssn.go.id/bssn-ajak-kolaborasi-seluruh-sektor-industri-digital-pada-pekan-industri-4-0-yogyakarta/

OECD, see Organisation for Economic Co-operation and Development

OJK, see Otoritas Jasa Keuangan

Organisation for Economic Co-operation and Development. (2007). *Public-Private Dialogue in Developing Countries: Opportunities, Risks, and Pre-Conditions*. https://www.oecd.org/dev/39517753.pdf

Organisation for Economic Co-operation and Development. (2015). *Addressing the Tax Challenges of the Digital Economy.* OECD/G20 Base Erosion and Profit Shifting Project. https://www.oecd-ilibrary.org/docserver/9789264241046-en.pdf?expires=1594712019&id=id&accname=guest&checksum=6444D20F31B1777C9815383E985F8D82

Organisation for Economic Co-operation and Development. (2019). *Regulatory effectiveness in the era of digitalisation*. https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

Otoritas Jasa Keuangan. (2020a). *Grup Inovasi Keuangan Digital Otoritas Jasa Keuangan: Daftar Penyelenggara Inovasi Keuangan Digital Per Juni 2020*. https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/-Penyelenggara-IKD-dengan-Status-Tercatat-di-OJK-per-Juni-2020.aspx

Otoritas Jasa Keuangan. (2020b). *Perkembangan Fintech Lending (Pendanaan Gotong Royong Online)*. https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/default.aspx

ParlAmericas (n.d.). *Citizen Participation in The Legislative Process*. https://parlamericas.org/uploads/documents/Toolkit_Citizen%20Participation%20in%20the%20Legislative%20Process.pdf

PDPC, see Singapore Personal Data Protection Commission

Prime Consultancy. (2020). *Financial Technology in Indonesia*. 2020 Report. Retrieved from: https://drive.google.com/file/d/1F3QiqRDxLEfLidbiSul8yMgns2ZJ0NrP/view

Rillo, A. (2018). Understanding the Digital Economy: *What Is It and How Can It Transform Asia? News and Events of*

Asian Development Bank. Asian Development Bank. https://www.adb.org/news/events/understanding-digital-economy-what-it-and-how-can-it-transform-asia

Rizkinaswara, L. (2020a). *Ada Indikasi Kebocoran Data, Kominfo Minta Tokopedia Lakukan Tiga Hal Ini.* Aptika Kominfo. https://aptika.kominfo.go.id/2020/05/ada-indikasi-kebocoran-data-kominfo-minta-tokopedia-lakukan-tiga-hal-ini/

Rizkinaswara, L. (2020b). *DPR telah Adakan Rapat Dengar Pendapat Umum terkait RUU PDP*. Aptika Kominfo. https://aptika.kominfo.go.id/2020/07/dpr-telah-adakan-rapat-denger-pendapat-umum-terkait-ruu-pdp/

Rosyidi, M. I. (2019, June). *Indonesian Online Travel Agencies: Profiling the services, employment, and users*. In 3rd International Seminar on Tourism (ISOT 2018). Atlantis Press.

Rumata, V. M., & Sastrosubroto, A. S. (2020). *The Paradox of Indonesian Digital Economy Development.* In E-Business. IntechOpen.

Schueth, S. & Simorangkir, I. (2018). *Financial Inclusion Insights Indonesia. Finclusion*. http://finclusion.org/uploads/file/fii-indonesia-2018-2019-final-report(1).pdf

Sen, K. (2015). State-business Relations: Topic Guide. Birmingham, UK: GSDRC, University of Birmingham.

Simpson, A.P. & Sotto, L.J. (2020). Data Protection & Privacy 2020. Law Business Research Ltd. https://aksetlaw.com/content/uploads/2019/09/Data-Protection-Privacy-2020.pdf

Singapore Personal Data Protection Commission. (2019). *Re-imagining Trust Governance and Private Law Rules.* Mr. Yeong Zee Kin, Deputy Commissioner's public speech at Singapore Management University, 5 December 2019. https://www.pdpc.gov.sg/news-and-events/press-room/2019/12/keynote-speech-by-deputy-commissioner-at-ai-and-commercial-law-on-thu-5-dec-2019-at-smu

Singh, P., Supriya, N., & Joshna, M. S. (2013). Issues and challenges of electronic payment systems. *International Journal for Research in Management and Pharmacy, 2*(9), 25-30.

Statista (2020). *Digital Payments Indonesia*. https://www.statista.com/outlook/296/120/digital-payments/indonesia

Statistics Indonesia. (2019). Statistik E-commerce 2019 [*E-commerce Statistics*]. Badan Pusat Statistik. Catalog 8101004. https://www.bps.go.id/publication/2019/12/18/fd1e96b05342e479a83917c6/ statistik-e-commerce-2019.html.

Statistics Indonesia (2020). *Belanja Online Menjadi Pilihan [Digital image]*. https://covid-19.bps.go.id/home/infografis.

Surianta, A. (2020). *Indonesia in Post COVID-19 Global Value Chain Restructuring*. Center for International Private Enterprise: Asia's Path Forward. https://www.cipe.org/wp-content/uploads/2020/08/Andree-Surianta.pdf

Taufik, A. I. (2017). Evaluasi Regulasi dalam Menciptakan Kemudahan Berusaha bagi UMKM. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 6*(3), 369-386.

Torfing, J., Sørensen, E., & Røiseland, A. (2019). Transforming the public sector into an arena for co-creation: Barriers, drivers, benefits, and ways forward. *Administration & Society, 51*(5), 795-825.

Uddarojat, R. (2020). Social media statement representing idEA on July 2020. https://www.linkedin.com/posts/rofi-uddarojat-5413abb0_its-an-important-milestone-to-advise-the-activity-6685885632214110208-ly5U/

UNDP, see United Nations Development Programme

United Nations Development Programme. (2017). *Indonesia: Financing the Future with an Integrated National Framework. UNDP's Regional Bureau for Asia and the Pacific.* https://www.undp.org/42content/dam/rbap/docs/dg/dev-effectiveness/RBAP-DG-2018-Development-Finance-Assessment-Snapshot-Indonesia.pdf

We Are Social & Hootsuite. (2020). *Digital 2020: Indonesia*. Data Reportal. https://datareportal.com/reports/digital-2020-indonesia

Women's World Banking (2018). *Ten years later: what has digital technology done for women's financial inclusion?* https://www.womensworldbanking.org/insights-and-impact/ten-years-later-digital-technology-done-womens-financial-inclusion/

Yuniarti, S., & Rasyid, A. (2020, March). *Consumer Protection in Lending Fintech Transaction in Indonesia: Opportunities and Challenges.* In Journal of Physics: Conference Series (Vol. 1477, p. 052016).

Interviews

Interview 1 – A digital economy consultant and expert (2020, June 5). Personal communication.

Interview 2 – A vice president for government affairs at a marketplace (2020, June 8). Personal communication.

Interview 3 – An executive director at an independent council on policy and regulatory reform (2020, June 8). Personal communication.

Interview 4 – A director/head of department at the Financial Services Authority (*Otoritas Jasa Keuangan* or OJK) (2020, June 9). Personal communication.

Interview 5 – A public policy and government affairs team at a technology company (2020, June 11). Personal communication.

Interview 6 – A deputy director at MOCI (2020, June 15). Personal communication.

Interview 7 – A public policy manager at a technology company (2020, June 9). Personal communication.

Interview 8 – A lecturer and an academic who writes academic script the Cybersecurity and Cyber Resilience Bill (2020, June 17). Personal communication.

Interview 9 – A director at a financial technology company (2020, June 17). Personal communication.

Interview 10 – Department of Payment System at the central bank (*Bank Indonesia* or BI) (2020, June 26). Written interview.

Interview 11 – A public policy manager at a digital economy association (2020, June 19). Personal communication.

Interview 12 – A public policy and government relations team at a marketplace (2020, July 2). Written interview.

Interview 13 – Ministry of Trade (MOT) (2020, June 29). Personal communication.

Interview 14 – The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN) (2020, June 26). Personal communication.

Interview 15 – The Indonesia Computer Emergency Response Team (2020, June 22). Personal communication.

Interview 16 – Directorate Defense and Security at the National Development Planning Agency (2020, June 24). Personal communication.

Interview 17 – An IT Security professional at a marketplace (2020, June 24). Personal communication.

ABOUT THE AUTHORS

Ira Aprilianti is an Analyst at MicroSave. She was previously a Researcher at CIPS who uses both qualitative and quantitative research methods to support evidence-based policy-making and policy impact evaluation in economic and trade policy. She received her Bachelor of Economics (Hons) from Universitas Jenderal Soedirman, Purwokerto, and her Master of International and Development Economics from the Australian National University. Previously, she provided analysis on trade data, market briefs, and trade policies for the Embassy of the Republic of Indonesia in Australia, under the Trade Attaché.

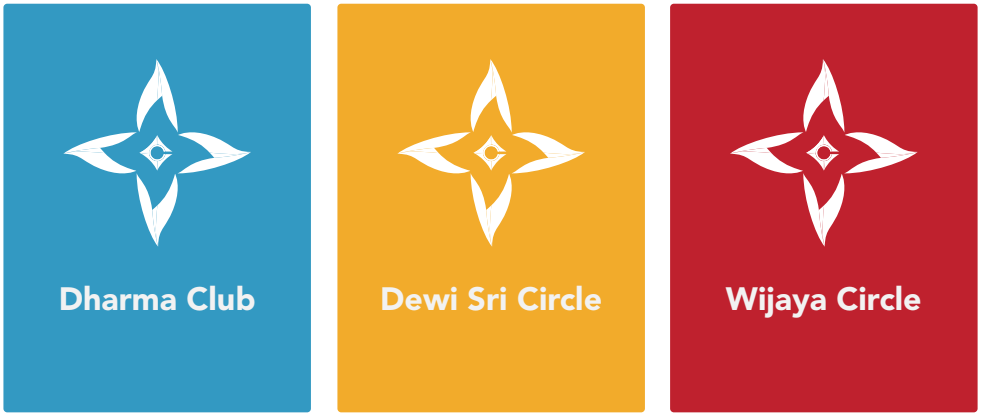
Siti Alifah Dina is a Researcher at the CIPS. Her research focuses on themes of poverty and labour force. Prior to joining CIPS, she was a consultant on social development sector for the World Bank Jakarta Office and a senior program officer at the Japan International Cooperation Agency Indonesia Office. She obtained her BSc from Bandung Institute of Technology in Urban and Regional Planning and MA from International Institute of Social Studies The Hague, in Development Studies with specialisation in Poverty.

JOIN OUR SUPPORTERS CIRCLES

Through our Supporters Circles, you, alongside hundreds of others, enable us to conduct our policy research and advocacy work to bring greater prosperity to millions in Indonesia.

Those in our Supporters Circles get the opportunity to engage in the work of CIPS on a deeper level. Supporters enjoy:

- Invitation to CIPS' annual Gala Dinner
- Exclusive Supporters-only briefings by CIPS leadership
- Priority booking at CIPS-hosted events
- Personal (Monthly/Quarterly) Supporters-only update emails and videos
- Free hard copy of any CIPS publication upon request



For more info, please contact anthea.haryoko@cips-indonesia.org.

Scan to join


Rp

ABOUT THE CENTER FOR INDONESIAN POLICY STUDIES

Center for Indonesian Policy Studies (CIPS) is a strictly non-partisan and non-profit think tank providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allows Indonesia to prosper. We are financially supported by donors and philanthropists who appreciate the independence of our analysis.

KEY FOCUS AREAS:

Food Security & Agriculture: To enable low-income Indonesian consumers to access more affordable and quality staple food items, CIPS advocates for policies that break down the barriers for the private sector to openly operate in the food and agriculture sector.

Education Policy: The future of Indonesia's human capital need to be prepared with skills and knowledge relevant to the 21st century. CIPS advocates for policies that drive a climate of healthy competition amongst education providers. Such competition will drive providers to constantly strive to innovate and improve education quality for the children and parents they serve. In particular, CIPS focuses on the improvement of operational and financial sustainability of low-cost private schools who serve the poor.

Community Livelihood: CIPS believes that strong communities provide a nurturing environment for individuals and their families. They must have the rights and capacities to own and manage their local resources and to ensure healthy and sound living conditions for the development and prosperity of the community.

www.cips-indonesia.org

facebook.com/cips.indonesia

@cips_id

@cips_id

Center for Indonesian Policy Studies

Center for Indonesian Policy Studies

Jalan Terogong Raya No. 6B
Cilandak, Jakarta Selatan 12430
Indonesia