Policy brief ini disusun dengan mendapatkan masukan dari Seri Webinar Ekosistem Ekonomi Digital II dengan beberapa pemangku kepentingan kebijakan tata kelola data dan ekonomi digital di Indonesia yang diselenggarakan oleh CSIS Indonesia, disamping berbagai kajian yang telah dilakukan sebelumnya. Diskusi publik tersebut dihadiri oleh perwakilan dari pemerintah, yaitu Kementerian Komunikasi dan Informatika, Bank Indonesia, Badan Pusat Statistik, perwakilan dari organisasi dan pelaku usaha ekonomi digital. Policy brief ini bertujuan untuk memberikan ulasan terkait diskusi serta memberikan rekomendasi kebijakan terkait dengan tata kelola data yang melindungi pengguna serta mendukung pengembangan inovasi dalam ekonomi digital.

CSIS Policy Brief
Department of Economics

Implikasi Kerangka Regulasi Tata Kelola Data Terhadap Ekonomi Digital di Indonesia

Yose Rizal Damuri & Dandy Rafitrandi
Departemen Ekonomi CSIS Indonesia

Digitalisasi dan globalisasi merupakan *enabler* dalam perdagangan internasional dan investasi yang menyebabkan akselerasi ekonomi digital beberapa dekade terakhir. Arus data elektronik yang bersumber dari interaksi antar manusia khususnya dalam ekonomi meningkat tajam dari 100 *gigabytes* setiap harinya pada tahun 1992 menjadi 150.000 *gigabytes* per detik pada tahun 2022 nanti.[1] Hal ini juga sejalan dengan konsumsi *mobile data* per bulan secara global yang meningkat sekitar 10 kali lipat dalam lima tahun terakhir sehingga rata-rata setiap *smartphone* menggunakan 9,4 *gigabytes* setiap bulan.[2]

[1] Digital Economy Report Value Creation And Capture: Implications For Developing Countries (2019). UNCTAD Digital Economy
[2] https://datareportal.com/reports/digital-2021-global-overview-report

Oleh sebab itu, banyak negara mengeluarkan kerangka regulasi terkait dengan *data governance* atau tata kelola data, termasuk Indonesia. Permasalahan yang mengemuka adalah bagaimana tata kelola data tersebut dapat memberikan jaminan perlindungan terhadap para pengguna, tetapi di satu sisi lain juga dapat mendukung perkembangan ekonomi dan inovasi yang mengandalkan penggunaan dan analisa data secara intensif.

Policy brief ini akan membahas beberapa isu yang terkait dengan tata kelola data khususnya perlindungan dan pembagian data dalam konteks pengembangan ekonomi digital di Indonesia. Pada bagian pertama akan dibahas terkait dengan data dan jenisnya serta dinamika antara pemangku kepentingan tata kelola data yaitu pengguna, sektor privat, dalam hal ini platform penyedia jasa digital, serta pemerintah. Selanjutnya, diskusi mengenai isu-isu penting dalam tata kelola data khususnya regulasi-regulasi yang terkait dengan ekonomi digital akan dijelaskan pada bagian kedua. Lalu di bagian ketiga, pembahasan akan fokus terhadap pembagian data dan potensi implikasi dalam pengembangan ekonomi digital di Indonesia dengan beberapa studi kasus negara-negara lain. Kesimpulan dan rekomendasi kebijakan akan didiskusikan pada bagian terkakhir.

Tata Kelola Data dan Pemangku Kepentingan

Seperti yang diketahui, pemanfaatan data elektronik merupakan salah satu elemen penting dalam ekonomi digital. Data merupakan *enabler* dari *multi-side markets* yang menjadi karakteristik utama dari platform digital seperti *e-commerce* dan *ride sharing*. Data menjadi aset yang sangat bernilai khususnya bagi perusahaan yang mengadopsi pengambilan keputusan bisnis berdasarkan data dengan peningkatan output dan produktivitas sebesar 5-6%.[3] Data bukan hanya menjadi asset yang berguna bagi dunia usaha, tetapi juga sangat berguna dari sisi pemerintahan.

Berbagai hal tersebut membuat lalu lintas antara berbagai pemangku kepentingan menjadi hal yang tidak dapat dihindarkan. Lalu lintas data ini sering disebut sebagai *data sharing*. Data yang dikumpulkan oleh satu penyelenggara platform digital akan dapat dikombinasikan dengan data dari penyelenggara lain untuk mendapatkan hasil analisa yang lebih akurat. Analisa terhadap data yang dikumpulkan oleh platform digital juga dapat digunakan untuk keperluan perumusan kebijakan dan implementasi regulasi, maupun kepentingan nasional lainnya, sehingga pemerintahpun mempunyai kepentingan untuk mendapatkan akses terhadap data tersebut.

Tetapi di sisi lain, penggunaan data yang dikumpulkan oleh platform digital harus juga dibarengi dengan komitmen untuk menjamin pelindungan bagi para penggunanya, yang menjadi sumber dari data tersebut. Di sisi lain, keamanan data menjadi hal yang semakin penting untuk mencegah *data breach* yang menjadi lebih sering. Perlindungan terhadap kepentingan pengguna menjadi sangat krusial terkait dengan masifnya pertukaran data tersebut. Ini bukan hanya menjadi kepentingan dari pengguna, tetapi mempengaruhi perkembangan ekonomi digital ke depannya. Dengan terjaminnya perlindungan terhadap data mereka, pengguna platform digital juga akan lebih

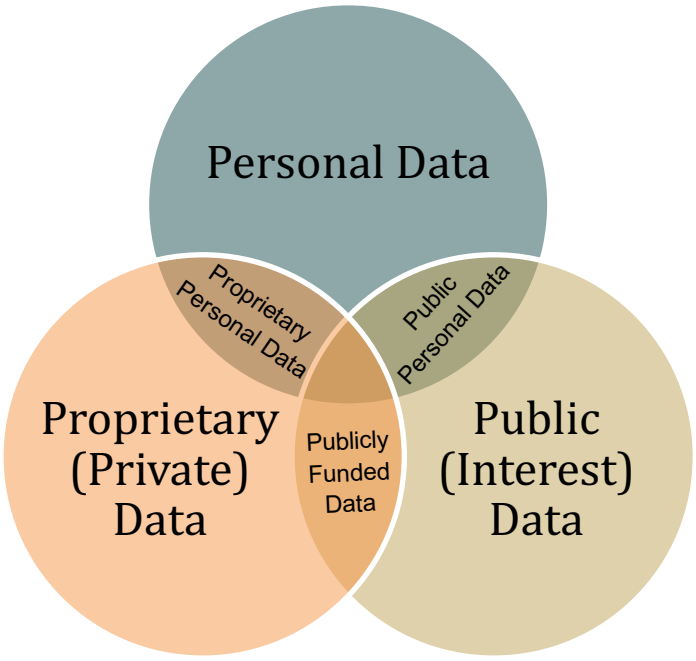
[3] Brynjolfsson, Erik and Hitt, Lorin M. and Kim, Heekyung Hellen, Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance? (April 22, 2011). Available at SSRN: https://ssrn.com/abstract=1819486 or http://dx.doi.org/10.2139/ssrn.1819486

memberikan kepercayaan terhadap teknologi dan jasa yang digunakan, yang pada akhirnya mendorong inovasi dan perkembangan lebih lanjut.

Namun demikian, untuk menemukan keseimbangan antara perlindungan data pribadi dan juga mendukung perkembangan dan inovasi ekonomi digital bukanlah hal yang mudah. Sering sekali dapat terjadi bahwa penggunaan data mempunyai potensi untuk merugikan pengguna. Untuk itu diperlukan tata kelola data yang dapat memenuhi kepentingan berbagai pihak secara seimbang, akuntabel, transparan, dan dapat dilaksanakan dengan baik.

Menurut *Organisation for Economic Co-operation and Development* (OECD)[4], data dapat dibagi menjadi beberapa jenis. Pertama, data pribadi yang meliputi data terkait identifikasi atau dapat diidentifikasi terhadap individu sehingga merupakan ranah privasi. Kedua, data *proprietary* atau yang dilindungi oleh hak kekayaan intelektual seperti hak cipta dan rahasia dagang. Yang terakhir, data publik yang merupakan data yang tidak dilindungi oleh hak kekayaan intelektual dan hak lainnya sehingga dapat diakses dan digunakan kembali secara bebas termasuk data untuk kepentingan publik. Dengan akselerasi arus dan penggunaan data di masa depan, ruang lingkup antara jenis-jenis data diatas akan semakin pudar. Hal ini yang akan menjadi tantangan bagi pengambil kebijakan untuk kerangka regulasi yang tepat.

Figur 1. Ruang Lingkup Data



Sumber: OECD (2019)

Dengan semakin meningkatnya risiko keamanan data baik pengguna data, pemerintah dan dunia usaha memiliki aspirasi terhadap isu tata kelola data. Hal ini harus disadari oleh pemerintah untuk menciptakan keseimbangan antara keuntungan dan risiko yang ditimbulkan dari tata kelola data. Pemerintah memiliki tujuan untuk melindungi keamanan data pengguna melalui kebijakan.

[4] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en

Namun disisi lain, pemerintah juga memiliki kepentingan untuk menggunakan data secara lebih optimal khususnya dalam rangka mendukung proses pengambilan kebijakan berdasarkan data sehingga meningkatkan kualitas pelayanan publik. Pemerintah juga memiliki kepentingan untuk melindungi data negara yang bersifat rahasia dan strategis.

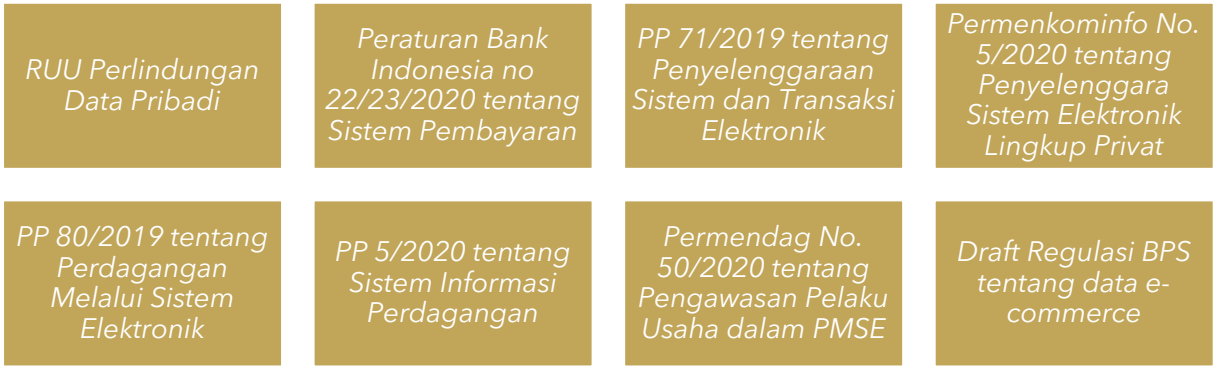
Dari sisi pengguna, isu penting tata kelola data terkait dengan bagaimana data mereka dikumpulkan, diproses dan digunakan. Hal ini terkait dengan adanya ancaman terkait dengan penyalahgunaan data pribadi yang dapat merugikan di masa depan. Selain itu, kepercayaan terhadap penyedia jasa digital dan pemerintah dalam hal tata kelola data juga masih perlu ditingkatkan. Dunia usaha juga memiliki kekhawatiran akan regulasi data yang terlalu restriktif sehingga mengancam inovasi. Regulasi data yang restriktif juga berpotensi meningkatkan biaya kepatuhan sehingga membuat berdampak negatif terhadap iklim investasi terutama dalam sektor ekonomi digital.

Dengan semakin intensifnya pertukaran data antara berbagai pihak, perlu adanya tata kelola data yang lebih baik dari mulai pengumpulan dan pengolahan data, pengaturan *data sharing*, akses ke data khususnya bagi pemerintah sebagai regulator serta perlindungan data pengguna. Hal ini harus terefleksikan dengan adanya kerangka regulasi yang berlaku sama kepada semua pihak serta menjunjung prinsip dan mekanisme yang setara. Bagian selanjutnya akan membahas lebih dalam terkait dengan kerangka regulasi tata kelola data di Indonesia serta beberapa diskusi spesifik untuk masing-masing regulasi.

Isu Dalam Kebijakan Tata Kelola Data di Indonesia

Tata kelola data atau *data governance* sebenarnya memiliki definisi yang cukup luas namun fokus yang akan dibahas pada policy brief ini adalah kebijakan dan regulasi yang terkait dengan *data protection* (perlindungan data) dan *data sharing* (pembagian data). Figur 2 di bawah berusaha memberikan gambaran sederhana mengenai kerangka regulasi yang terkait dalam tata kelola data di Indonesia.

Figur 2. Regulasi Terkait Perlindungan dan Pembagian Data di Indonesia



Sumber: Penulis

Salah satu contoh regulasi dalam perlindungan dan pembagian data adalah Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan RUU Perlindungan Data Pribadi (PDP). Regulasi ini tentunya diharapkan dapat melindungi dan

menjamin hak dasar warga negara terkait dengan pelindungan diri pribadi serta menjamin masyarakat untuk mendapatkan pelayanan dari pemerintah dan pelaku usaha, dan organisasi/institusi lainnya. Selain itu, regulasi ini juga mewajibkan pemberian akses terhadap sistem elektronik dan data elektronik untuk keperluan monitoring dan pengawasan. Hal ini berpotensi meningkatkan beban biaya kepatuhan (terutama bagi pelaku usaha rintisan/start-up digital) dan potensi kurangnya kepercayaan dari pengguna, seperti yang diharapkan pengguna. Masih belum jelasnya mekanisme perlindungan dan *data sharing* serta masih lemahnya koordinasi antar instansi pemerintah serta ketidakjelasan implementasi masih menjadi tantangan utama bagi pemerintah. Dampaknya antara lain menimbulkan kerancuan khususnya bagi para pelaku usaha serta investor potensial dalam ekonomi digital. Terkait dengan RUU PDP, aturan yang mewajibkan persetujuan eksplisit untuk semua jenis pemrosesan data dapat menimbulkan risiko ancaman siber karena subjek data perlu membagikan informasi mereka dalam berbagai tahap. Selain itu, mewajibkan pengontrol data untuk verifikasi dapat menimbulkan risiko keamanan karena subjek data perlu membagikan data pribadi mereka secara teratur dan itu bisa membebani sektor usaha.

Selain itu, PP No. 80 Tahun 2019 juga telah diterbitkan khusus mengatur tentang Perdagangan Melalui Sistem Elektronik (PMSE). Badan Pusat Statistik (BPS) merupakan lembaga yang diberikan wewenang dalam melakukan pendataan khususnya terkait dengan data perdagangan elektronik. Tata kelola *data sharing* di lingkup perdagangan juga diatur lebih lanjut dalam PP No. 5/ 2020 tentang Sistem Informasi Perdagangan yang mencakup pasal-pasal terkait jenis data perdagangan, kewenangan Menteri Perdagangan untuk meminta data kepada pelaku usaha dan kementerian/ lembaga lainnya. Dari kedua regulasi ini, beberapa isu yang masih mengemuka antara lain terkait dengan ruang lingkup data dan mekanisme data sharing antar K/L yang masih kurang jelas. Hal ini akan menjadi faktor krusial dalam menjaga integritas, transparansi serta keamanan dalam tata kelola data di Indonesia. Terkait dengan adanya kemungkinan untuk terjadi *data leakage/failure*, regulasi turunan nantinya diharapkan dapat memiliki standard yang jelas dalam penanganan hal ini.

Terkait dengan sistem pembayaran yang merupakan aspek yang terintegrasi dalam ekonomi digital, Bank Indonesia memiliki Blueprint Sistem Pembayaran Indonesia (BSPI) 2025 yang bertujuan untuk mereformasi pengaturan sistem pembayaran di Indonesia. Beberapa strategi dan inisiatif misalnya tentang pengembangan infrastruktur data yang bersifat publik dan menjamin keterbukaan akses dan proteksi data pribadi konsumen. Tentunya data-data ini akan digunakan untuk kepentingan nasional khususnya mendukung transformasi digital di Indonesia. Namun demikian, menemukan keseimbangan antara inovasi, perlindungan konsumen serta integritas tata kelola data bukanlah persoalan yang mudah.

Dapat disimpulkan dari isu-isu yang mengemuka, konsekuensi terhadap diberlakukannya regulasi-regulasi diatas harus menjadi perhatian para pemangku kepentingan. Pertama, belum adanya mekanisme perlindungan data yang terstandardisasi diantara K/L akan meningkatkan potensi adanya tumpang tindih pembuatan kebijakan dan implementasi terkait tata kelola data. Perhatian pemerintah yang semakin besar terhadap peranan data dalam pengambilan kebijakan juga harus diartikan sebagai semakin mendesaknya peningkatan kapasitas pemerintah dalam mengolola data sesuai dengan mekanisme dan standard yang baik. Bukan hanya diartikan sebagai mengumpulkan data dari sektor usaha.

Kedua, pemerintah juga harus menyadari bahwa sektor usaha memiliki tanggung jawab kepada pengguna/pemilik data sehingga *data sharing* hanya dimungkinkan untuk data-data yang bersifat agregat. Data dengan tingkatan yang lebih khusus akan meningkatkan kemungkinan penyalahgunaan apabila dipindahtangankan dengan format yang berbeda-beda, landasan hukum yang kurang jelas hingga tidak disertai dengan mekanisme data sharing yang baik.

Ketiga, regulasi yang restriktif berpotensi meningkatkan biaya kepatuhan bagi sektor usaha sehingga berdampak negatif terhadap iklim usaha di sektor ekonomi digital. Apalagi jika regulasi-regulasi ini memiliki prinsip-prinsip yang berbedag dengan *best practices* di negara-negara lain.

Terakhir, beberapa poin yang patut digarisbawahi terkait dengan *regulatory framework* perlindungan dan pembagian data secara umum antara lain:

- Regulasi perlindungan dan pembagian data harus berlaku untuk semua pemangku kepentingan tanpa pengecualian. Semua pihak harus menjunjung prinsip dan mekanisme yang setara dan sesuai dengan regulasi yang berlaku untuk semua pihak termasuk pemerintah. Contohnya dalam kerangka regulasi sekarang, belum ada mekanisme yang berlaku apabila terjadi penyalahgunaan atau kebocoran data pribadi dari sisi pemerintah

- Ketidaksetaraan dan pengecualian berpotensi untuk menimbulkan penyalahgunaan wewenang. Tanggung jawab dan kewajiban yang sama bagi semua pemangku kepentingan dalam mematuhi prosedur dan mekanisme pengambilan, pemrosesan hingga pembagian data merupakan aspek yang penting dalam membentuk kerangka regulasi yang seimbang dan mendukung iklim ekonomi digital di Indonesia.

- Koordinasi antar K/L merupakan faktor yang krusial dalam menjaga integritas, transparansi serta keamanan dalam tata kelola data di Indonesia. Terkait dengan adanya kemungkinan untuk terjadi data leakage/failure, regulasi turunan nantinya diharapkan dapat memiliki standard yang jelas dalam penanganan hal ini.

- *Regulatory framework* terkait dengan prosedur perlindungan dan pembagian data pada akhirnya harus memperhatikan prinsip-prinsip hukum dan hak asasi manusia. Berkaca dengan praktik di negara lain, peraturan terkait dengan hal ini biasanya dibahas ditingkat UU dengan mengikutsetakan partisipasi publik seperti *Electronic Communications Privacy Act* (ECPA) di Amerika Serikat yang telah berkali-kali direvisi

Belajar dari Pengalaman Berbagai Negara

Beberapa regulasi terkait dengan pembagian data akan dibahas sebagai studi kasus antara lain Uni Eropa, Singapura dan Australia.

General Data Protection Regulation (GDPR) – Uni Eropa

Persyaratan GDPR berlaku untuk setiap negara anggota Uni Eropa, yang bertujuan untuk menciptakan perlindungan yang lebih konsisten atas data konsumen dan pribadi di seluruh negara UE. Beberapa privasi utama dan persyaratan perlindungan data dalam GDPR yaitu memerlukan persetujuan subjek untuk pemrosesan data, menganonimkan data yang dikumpulkan untuk melindungi privasi, memberikan pemberitahuan pelanggaran data, menangani transfer data lintas batas dengan aman dan mewajibkan perusahaan tertentu untuk menunjuk petugas perlindungan data untuk mengawasi kepatuhan GDPR.

Dibandingkan dengan GDPR, RUU PDP Indonesia menyertakan beberapa ketentuan yang lebih ketat. Misalnya, RUU PDP menetapkan jangka waktu yang sangat singkat bagi pengontrol data untuk menanggapi permintaan pemilik data dalam 72 jam dan harus memberikan pemberitahuan pelanggaran dalam 72 jam. Sebaliknya, GDPR memungkinkan pengontrol data untuk menanggapi permintaan pemilik data dalam waktu satu bulan. Ini juga mensyaratkan bahwa pengontrol data memberikan pemberitahuan pelanggaran dalam 72 jam tetapi jika pemberitahuan tidak dibuat dalam 72 jam, pengontrol harus memberikan alasan penundaan.

GDPR mengamanatkan kerja sama antara pengontrol data dan prosesor dengan otoritas pengawas dalam kondisi yang ketat. GDPR juga melarang pengontrol untuk "memproses" data pribadi kecuali salah satu dari enam situasi, atau tujuan yang diizinkan, berlaku. Sebelum membagikan data pribadi dengan lembaga pemerintah, pengontrol harus menentukan tujuan yang diizinkan yang berlaku, seperti persetujuan subjek data, jika diperlukan untuk melindungi kepentingan vital seseorang, dan jika perlu untuk pelaksanaan tugas yang dilakukan di kepentingan umum.

Adapun kerangka regulasi Indonesia seperti Permenkominfo No. 5/2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat mengatur secara luas akses otoritas ke sistem dan data perusahaan, yang tidak selaras dengan standar internasional yang ditetapkan oleh GDPR.

GDPR dipandang sebagai regulasi model untuk tata kelola data. Ini menetapkan standar perlindungan data yang juga pasti meningkatkan biaya kepatuhan untuk perusahaan digital yang beroperasi di UE. Meski perusahaan kini memiliki lebih banyak standar yang harus dipatuhi, umumnya GDPR dipandang positif karena juga memberikan jaminan dan perlindungan data pribadi yang sebelumnya tidak ada. Setelah dua tahun diimplementasikan, GDPR membawa dampak positif dan negatif terhadap ekonomi digital.

Dampak positifnya adalah memberikan standar baru perlindungan data pribadi bagi warga negara, meningkatkan kepercayaan pengguna, dan dengan demikian mendorong lebih banyak orang untuk menggunakan layanan digital. Standard ini juga banyak dijadikan *benchmark* bagi negara-negara lain dalam mengatur kerangka regulasi tata kelola data. Sebaliknya, GDPR dinilai berpotensi mempersulit proses kepatuhan dan meningkatkan biaya operasi (terutama untuk perusahaan baru), menghadirkan rintangan bagi arus informasi yang bebas.

2018 Public Sector Governance Act – Singapura

Menurut Undang-Undang tersebut, ketika arahan *data sharing* diberikan, badan sektor publik Singapura dan pejabat mereka berwenang untuk berbagi informasi di bawah kendali badan tersebut dengan badan sektor publik Singapura lainnya sejauh diizinkan oleh arahan berbagi data. Agensi terpusat telah dibentuk untuk memastikan bahwa data mentah dianonimkan dengan benar sebelum dirilis ke agensi terkait.

Petugas sektor publik yang membagikan data pribadi warga Singapura tanpa izin dapat didenda hingga $5.000, penjara hingga dua tahun, atau keduanya. Hal yang sama berlaku untuk mereka yang menggunakan data untuk keuntungan diri mereka sendiri atau mengidentifikasi ulang data yang dianonimkan tanpa otorisasi. Proses pidana masih dapat dilembagakan bahkan setelah dia meninggalkan layanan badan sektor publik Singapura. Kerangka peraturan Indonesia belum memasukkan sanksi apa pun bagi pejabat sektor publik yang menggunakan informasi secara tidak benar, mengungkapkan informasi tanpa otorisasi apa pun ataupun terbukti lalai dalam proses pembagian data. Penting bagi pembuat kebijakan untuk memasukkan sanksi tersebut untuk mencegah bahaya moral di masa depan.

Lain halnya dengan GDPR, *Public Sector Governance Act* mengatur *data sharing* di antara lembaga pemerintah di Singapura. Hal ini memberikan panduan bagi pengambil kebijakan di Singapura ketika mereka menerima, berbagi, dan mengungkapkan data kepada pihak-pihak yang terkait. Namun peraturan ini memberikan jaminan bagi perusahaan karena menetapkan standar tindakan perlindungan data di antara lembaga pemerintah. Secara keseluruhan, peraturan ini mendukung penggunaan data dan pembagian data yang bertanggung jawab di antara lembaga pemerintah, yang pada gilirannya akan mendukung tata kelola data yang baik di sektor ekonomi digital Singapura.

Adapun dampak positif dari Undang-undang ini adalah memberikan standar baru perlindungan data pribadi untuk pejabat publik dan kantor ketika mereka berbagi data, memberikan jaminan bagi perusahaan jika terjadi kebocoran tanggal dan berbagi data tanpa izin. Namun di sisi lain, peraturan ini sangat bergantung pada kompetensi tinggi pejabat pemerintah yang berwenang untuk mengelola data, sedangkan hal ini akan menjadi tantangan jika kebijakan serupa diterapkan di Indonesia.

Privacy Act and Data Sharing Principles – Australia

Untuk menanggapi meningkatnya kebutuhan Pemerintah untuk berbagi data antar kementerian dan dengan sektor swasta, Pemerintah Australia mengembangkan pedoman tentang prinsip-prinsip berbagi data yang bertujuan untuk memberikan panduan yang jelas kepada lembaga-lembaga pemerintah Australia ketika mereka melakukan *data sharing* kepada pihak lain. Misalnya, sebelum meminta dan membagikan data, instansi pemerintah di Australia harus melalui proses *self assesment* terkait apakah permintaan data tersebut sesuai dengan data yang digunakan dan mendapatkan persetujuan dari pemilik data. Panduan *data sharing* juga memberikan pertanyaan kepada pembuat kebijakan pemerintah yang harus mereka jawab untuk memastikan keselarasan antara permintaan dan penggunaan data yang diminta.

Meskipun memiliki Undang-Undang Privasi sejak 1998, privasi data tetap menjadi masalah besar di Australia. Orang-orang sangat prihatin dan tidak mengetahui tentang tujuan pengumpulan

dan penggunaan data mereka oleh Pemerintah dan sektor swasta. Panggilan telah dilakukan untuk merevisi undang-undang untuk meningkatkan perlindungan pada keamanan data pribadi. Namun, satu pendekatan positif yang telah diadopsi oleh Australia adalah pembentukan *the Office of the Australian Information Commissioner* (OAIC) sebagai badan pengawas tunggal yang bertanggung jawab atas perlindungan data secara keseluruhan di Australia.

Prinsip berbagi data juga sebagian besar disambut secara positif oleh sektor swasta dan publik karena menjadi standar bagi lembaga pemerintah di Australia saat meminta data dan berbagi data. Misalnya, prinsip berbagi data menyarankan penjaga data (mereka yang memiliki/memiliki data) untuk memiliki perjanjian berbagi data dengan pihak ketiga (mereka yang menerima data), dan ini berlaku untuk sektor swasta dan publik. Secara keseluruhan ini adalah praktik yang lebih baik untuk mendukung pertumbuhan ekonomi digital, dibandingkan dengan yang kita miliki di Indonesia.

Penutup: Menuju Tata Kelola Data yang Lebih Baik

Faktor kepercayaan antar pemangku kepentingan adalah salah satu hal yang paling penting untuk membangun kerangka kebijakan dalam tata kelola data. Prinsip perlindungan data perlu diperjelas dan berlaku untuk semua pihak, bukan hanya untuk dunia usaha. Hal ini termasuk standard dan mekanisme untuk menghindari kebocoran dan penyalahgunaan data, tidak terkecuali bagi lembaga pemerintah. Regulasi yang berlaku harus berlaku kepada semua pihak dengan pengecualian yang minimum contohnya seperti GDPR. Pada prinsipnya, tata kelola data yang baik seharusnya dapat memberikan fasilitasi atas penggunaan data yang bertanggung jawab oleh semua pihak yang pada akhirnya dapat meningkatkan kepercayaan antar pemangku kepentingan.

Terdapat tren yang konsisten di seluruh institusi pemerintah untuk menuntut pelaku *e-commerce* berbagi data dan/atau informasi. Namun, tren ini tidak diikuti oleh komitmen perlindungan data yang kuat karena sebagian besar peraturan tersebut hanya menuntut perusahaan untuk berbagi data tanpa penjelasan yang tepat dan rinci tentang langkah-langkah perlindungan data. Terlepas dari tren yang konsisten, terdapat kurangnya koordinasi antar kementerian terkait bagaimana perusahaan diharapkan untuk berbagi data.

Kurangnya koordinasi antar kementerian juga terlihat dari perbedaan jenis data yang dibutuhkan dari perusahaan, perbedaan mekanisme pembagian data, ruang lingkup, tujuan, dan koordinator pemerintah. Persyaratan ini mengakibatkan tingginya biaya kepatuhan dan potensi kurangnya kepercayaan dari pengguna, karena pengguna mengharapkan sektor swasta akan dapat melindungi datanya dan tidak membagikan kepada pihak ketiga lainnya termasuk pemerintah.

Terakhir, isu tata kelola data merupakan isu global yang masih memliki banyak tantangan. Untuk itu, konvergensi regulasi dan kerja sama regulasi internasional merupakan hal yang harus didorong dalam rangka mewujudkan regulasi yang mendukung perkembangan ekonomi digital. Contohnya dalam isu data privasi antara lain OECD *Guidelines on the Protection of Privacy Transborder Flows of Personal Data*, GDPR serta APEC *Cross-Border Privacy Rule*. Prinsip-prinsip yang terkandung dalam *regulatory framework* diatas dapat menjadi pedoman bagi pengambil kebijakan di Indonesia untuk dapat memberikan perlindungan yang efektif dan menghindari hambatan-hambatan informasi yang tidak perlu. Dengan regulasi yang lebih selaras dengan praktik internasional dan

iklim ekonomi digital yang mendukung, perdagangan digital Indonesia dapat mencapai 172 miliar USD pada tahun 2030 atau meningkat delapan kali lipat dibandingkan data tahun 2020.[5]

[5] Hinrich Foundation, 2019, "The Digital Komodo Dragon: How Indonesia Can Capture the Digital Trade Opportunity at Home and Abroad." Available via the Internet: https://www.alphabeta.com/wp-content/uploads/2019/02/digitrade_indo_eng_1-pgview.pdf