KONRAD ADENAUER STIFTUNG

Tata Kelola Data di Indonesia dan India

Sebuah Studi Komparasi

Disusun oleh Institute of South Asian Studies, National University of Singapore dan Center for Digital Society, Universitas Gadjah Mada

www.kas.de

Tata Kelola Data di Indonesia dan India

Tata Kelola Data di Indonesia dan India

Sebuah Studi Komparasi

**Disusun oleh Institute of South Asian Studies,
National University of Singapore dan
Center for Digital Society, Universitas Gadjah Mada**

**Untuk Konrad Adenauer Stiftung, Rule of Law
Programme Asia, Singapura.**

Maret 2021

KONRAD ADENAUER STIFTUNG

CfDS CENTER FOR DIGITAL SOCIETY

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

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

ISBN 978-981-18-1797-7

Kredit gambar

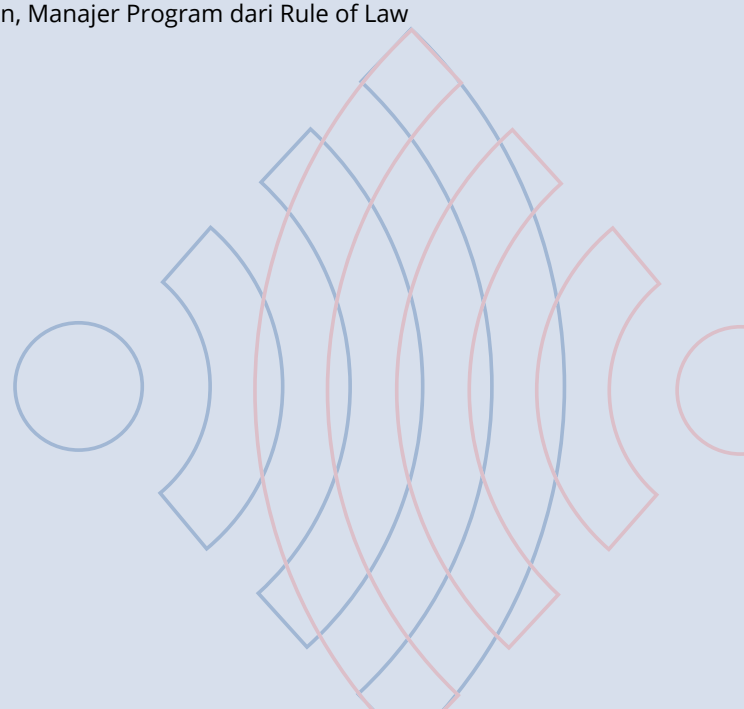
Sampul: gambar biner didesain oleh starline / Freepik
Halaman 7: ikon bank dan ikon tas uang didesain oleh Kreativkolors / Freepik
Halaman 7, 11dan 33: ikon internet dan ikon telepon didesain oleh rawpixel.com / Freepik
Halaman 35: ikon klik didesain oleh rawpixel.com / Freepik
Halaman 36: gambar belanja didesain oleh Katemangostar / Freepik
Halaman 79: gambar beberapa server oleh Cskiran pada Wikipedia

Tentang Konrad Adenauer Stiftung (KAS)

Konrad Adenauer Stiftung (KAS) merupakan sebuah yayasan politik Republik Federal Jerman yang telah, selama lebih dari 50 tahun, berkomitmen untuk memajukan demokrasi dan kerja sama internasional. Didirikan pada tahun 1964, yayasan ini diberikan nama kanselir pertama Republik Federal Jerman, Konrad Adenauer. KAS menawarkan berbagai aktivitas politik dan sosial, mengadakan penelitian, memberikan beasiswa kepada pelajar dan mendukung serta mendorong pemahaman internasional dan pengembangan ekonomi. The Rule of Law Programme merupakan program KAS di seluruh dunia dengan kantor regional di Asia, Eropa, Amerika Latin, Afrika Sub-Sahara dan Timur Tengah / Afrika Utara. The Rule of Law Programme Asia, yang berbasis di Singapura, berdedikasi untuk bekerja sama dengan mitra Asia menuju pengembangan supremasi hukum di wilayah tersebut. Program ini memulai digitalisasi untuk mengamati perkembangan regional terkait munculnya media baru dan teknologi canggih. Salah satu bidang fokus khusus adalah untuk mengeksplorasi interaksi antara teknologi, masyarakat dan peran hukum.

Pimpinan Proyek dari KAS:

- Stefan Samse, Direktur dari Rule of Law Programme Asia
- Aishwarya Natarajan, Manajer Program dari Rule of Law Programme Asia



Tentang Institute of South Asian Studies, National University of Singapore

Institute of South Asian Studies (ISAS) didirikan pada Juli 2004 sebagai institusi penelitian otonom di National University of Singapore (NUS). ISAS didedikasikan untuk penelitian tentang Asia Selatan kontemporer. Lembaga ini berusaha mempromosikan pemahaman dari wilayah vital dunia ini dan menyampaikan pengetahuan dan wawasan mengenai hal tersebut kepada pembuat kebijakan, komunitas bisnis, akademisi dan masyarakat sipil, di Singapura dan sekitarnya.

Kontributor dari ISAS:
- Karthik Nachiappan
- Ronojoy Sen

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

Center for Digital Society (CfDS) merupakan pusat penelitian di bawah Fakultas Ilmu Sosial dan Politik, Universitas Gadjah Mada. Lembaga ini didirikan oleh perkembangan dan dinamika kehidupan sosial politik kontemporer di dunia yang ditandai dengan pengaruh teknologi informasi. Untuk itu diperlukan pendekatan baru dalam mengelola dan memahami fenomena masyarakat digital. Riset dan aktivitas kami terutama didukung oleh semboyan terkemuka, yaitu produktif, inovatif dan berpengaruh.

Kontributor dari CfDS:
- Mulya Amri
- Dewa Ayu Diah Angendari
- Anisa Pratita Kirana Mantovani
- Janitra Haryanto
- Raka Wicaksana

Ringkasan Eksekutif

Laporan kebijakan ini merangkum bagaimana India dan Indonesia berusaha meregulasi data. Ekonomi digital yang berkembang di kedua negara telah menciptakan tuntutan pengembangan kerangka hukum untuk mengatur data – bagaimana data dikumpulkan, diproses, disimpan dan dibagikan. Aturan yang mengatur data akan secara signifikan memengaruhi arah perkembangan dan pertumbuhan ekonomi digital India dan Indonesia. Pemerintah kedua negara harus mampu mengelola data secara baik mengingat ada ratusan juta warga yang terhubung secara daring.

Politik seputar regulasi data meresahkan di kedua negara. India tergesa-gesa membuat kerangka kebijakan dan hukum baru untuk mengelola data yang membahas seputar apa itu data, bagaimana organisasi seharusnya menangani data dan bagaimana pemerintah harus mengatur kesenjangan ini. Selama ini, Indonesia telah mengatur data dengan cara tambal sulam peraturan sektoral yang dikeluarkan lembaga secara terpisah. Gambaran yang terfragmentasi ini akan segera memberi jalan bagi undang-undang baru yang komprehensif mengenai perlindungan data pribadi. Setelah beroperasi, kewenangan undang-undang di kedua negara kemungkinan besar akan mendalam dan begitu juga dengan dampaknya terhadap privasi dan hak warga negara, peran negara dalam mengatur data dan tren inovasi digital di India dan Indonesia.

Di kedua negara, rancangan undang-undang telah dipengaruhi oleh kerangka European Union's General

Data Protection Regulation (GDPR), pendekatan perlindungan data yang berpusat pada pengguna yang diilhami oleh gagasan persetujuan dan akuntabilitas. Gagasan pengaturan data yang berpusat pada pengguna ini diimbangi dengan preferensi pendekatan statistik terhadap regulasi data di kedua negara yang menggaris bawahi kedaulatan dengan mengorbankan privasi. Tantangan kritisnya adalah untuk melihat bagaimana undang-undang data yang baru di kedua negara akan menyeimbangkan dua tujuan yang tidak dapat disatukan ini.

Tantangan utama lainnya terkait dengan penerapan dan penegakan hukum data setelah diberlakukan. Ketentuan hukum ini mengharuskan regulator baru untuk mengelola dan mengawasi masalah di bawah pengiriman data yang sedang berkembang. Namun, pertanyaannya tetap mengenai kemandirian regulator data di masa depan dan kemampuan mereka dalam melakukan penilaian dan menengahi konflik. Hal ini berdasar pada adanya berbagai kepentingan publik dan pribadi. Terdapat juga pertanyaan mengenai koordinasi dan kapasitas – akankah perusahaan dan organisasi publik memiliki staf khusus untuk mengelola pertanyaan tentang data dan bertanggung jawab untuk penyesuaian? Kedua negara harus mengelola dan mengatasi defisit kelembagaan yang diharapkan setelah undang-undang data mereka diberlakukan dan pembuat peraturan sudah dibuat. Terakhir, politik seputar data di kedua negara akan mempersulit regulasi dan penegakan yang efektif – aktivis privasi dan organisasi masyarakat sipil terkait kemungkinan besar akan menekan pemerintah untuk memberlakukan hukum yang kuat guna menyeimbangkan privasi dan akuntabilitas tanpa mengorbankan prioritas ini di altar kontrol negara.

Daftar Isi

Pendahuluan

India dan Indonesia adalah dua kekuatan Asia yang juga merupakan negara demokrasi besar dan padat penduduk. Baik India maupun Indonesia merupakan negara berkembang yang kebijakannya memiliki efek sistemik yang cukup besar. Kedua negara ini memiliki ekonomi yang dinamis dengan perusahaan digital yang berkembang pesat mengisi lanskap industri mereka. Penggunaan dan penetrasi internet meningkat dan mendorong inovasi pada sektor digital India dan Indonesia. Dalam waktu dekat, kedua negara akan mengalami lonjakan ekonomi digital. Lonjakan ini akan menjadi sumber investasi transnasional yang penting dan berfungsi sebagai bagian sentral ekonomi saat pandemi yang mengubah struktur ekonomi global digital. Meskipun sektor digital dan ekonomi berkembang, masa depan India dan Indonesia bergantung pada undang-undang yang diadopsi untuk mengatur inovasi digital dan transaksi digital lintas batas. Aturan yang mengatur keamanan siber dan kecerdasan buatan bergantung pada faktor fundamental yang mendorong inovasi digital dan perdagangan, yakni data. Cara kedua negara mengatur data akan menunjukkan intensi dan prioritas terhadap mitra eksternal yang ingin berinvestasi pada ekonomi mereka. Perusahaan domestik juga perlu mengetahui pengelolaan yang dilakukan negara karena mereka membutuhkan kejelasan lebih lanjut ketika mengembangkan produk dan layanan digital untuk pasar global.

Laporan ini mencatat dan mengungkap bagaimana India dan Indonesia berupaya mengatur data. Tekanan

yang didorong oleh ekonomi digital yang berkembang pesat telah memaksa pembuat kebijakan dan para regulator untuk merancang aturan yang koheren dan komprehensif untuk mengumpulkan, mengelola, menyimpan dan memproses data pribadi. Data pribadi merujuk pada informasi individu yang dapat diidentifikasi serta diberikan kepada berbagai layanan dan perusahaan untuk berkomunikasi dan kebutuhan perdagangan daring. Peningkatan penggunaan internet, pertumbuhan penetrasi internet dan peningkatan pada kepemilikan *platform* dan perangkat seluler telah memecahkan catatan penggunaan data di India dan Indonesia. Ratusan juta orang di kedua negara mengelola kehidupan mereka secara daring. Secara tidak langsung, mereka memberikan sedikit demi sedikit informasi tentang kehidupan sehari-hari mereka ke layanan dan perusahaan daring untuk kenyamanan dan penggunaan yang lebih besar. Peningkatan catatan penggunaan data belum dipenuhi oleh aturan domestik yang secara efektif mengatur kondisi dan batasan yang harus dipatuhi oleh perusahaan ini saat mengumpulkan informasi pribadi.

Tekanan untuk membuat undang-undang perlindungan data baru di kedua negara berbeda-beda. Di India, permintaan untuk membuat kerangka baru untuk mengelola data pribadi berasal dari diskusi hak atas privasi, yang muncul dari investasi pemerintah untuk menciptakan identitas digital bagi semua warga negara India. India menanggapi dengan mempercayakan rumusan RUU baru kepada komite ahli yang menilai data cukup berharga secara ekonomi untuk menjamin disimpan seluruhnya di India, meskipun beberapa dari ketentuan ini telah dilonggarkan. Di Indonesia, tuntutan untuk melindungi data diakibatkan oleh beberapa pelanggaran data yang menyebabkan perusahaan membahayakan data pribadi. Kesenjangan keamanan telah memengaruhi dorongan untuk undang-undang perlindungan data yang menyeluruh di Indonesia.

Peraturan yang ada di India dan Indonesia saat ini masih jauh dari harapan. Hal ini membuat para pembuat kebijakan peka untuk meninjau aturan saat ini yang mengatur pengumpulan dan pengelolaan data

pribadi. Undang-undang sektoral mendominasi kedua yurisdiksi tetapi efektivitasnya terbatas. Sebagian besar terjadi karena fragmentasi di Indonesia dan penegakan hukum yang kurang di India. Pembuatan kerangka perlindungan data baru telah didorong oleh kebutuhan mendesak untuk meningkatkan dan menggantikan aturan pengumpulan data yang ada saat ini. Pertimbangan internasional juga dilibatkan dalam hal ini. Kerangka General Data Protection Regulation (GDPR) Uni Eropa telah berfungsi sebagai sebuah pedoman bagi perumus data legislasi di India dan Indonesia. Tanpa aturan global yang jelas mengenai data, GDPR telah diandalkan selama penyusunan aspek-aspek tertentu dari kedua rancangan undang-undang tersebut. Privasi sangat penting. Begitu pula persetujuan pribadi yang harus dihormati oleh perusahaan yang mengumpulkan data. Hak-hak pengguna memengaruhi kedua undang-undang tersebut.

Meskipun begitu, terdapat penekanan yang kuat pada perlindungan data untuk membantu tujuan negara, sebuah faktor penting yang terwujud dalam kedok "kedaulatan data" atau data yang juga menjadi milik negara. Ke depannya, dorongan yang melindungi privasi dan hak pengguna individu harus diimbangi dengan kepentingan negara yang selaras dengan pengumpulan data untuk penggunaan umum. Menyeimbangkan kebutuhan publik dan pribadi – kepentingan negara dan para pengguna – serta prioritas perusahaan teknologi domestik dan asing akan menyulitkan India dan Indonesia. Kedua negara berusaha keras untuk memberlakukan undang-undang perlindungan data untuk mengatur data pribadi. Beban politik ini harus ditanggung oleh lembaga untuk mengatur data yang akan dibuat (India) atau diberi sanksi (Indonesia). Tantangan institusional mungkin masih mengganggu penerapan kedua undang-undang ini setelah mereka menerima persetujuan.

Laporan ini menjelaskan dan menganalisis bagaimana India dan Indonesia telah berusaha mengelola data, berfokus pada faktor dan pelaku politik dan kelembagaan. Bagian pertama mengungkap upaya India untuk mengelola data dengan berfokus pada RUU Perlindungan Data Pribadi (PDP) yang dirancang oleh komite

terpilih pada Juli 2018 dan setelah itu direvisi. Bagian kedua berfokus pada upaya Indonesia serta pembahasan mengenai berbagai peraturan dan tekanan yang menyebabkan diskusi seputar undang-undang perlindungan data baru di Indonesia. Bagian ketiga membandingkan dan membedakan pengalaman kedua negara untuk menarik beberapa kesimpulan luas terkait regulasi data di Asia. Kesimpulan tersebut menggambarkan beberapa tantangan dan peluang yang terbentang di depan bagi kedua negara di sepanjang jalur ini.

India – Tata Kelola Data

Pendahuluan

Ketika pemerintah India meresmikan Kebijakan *E-Commerce* Nasional (*National E-Commerce Policy*) pada Februari 2019 silam, diskusi mengenai pengaturan data kemudian berkembang. Saat ini data disebut sebagai "minyak" baru di India. Kondisi ini membuat para pemimpin politik dan bisnis menyerukan agar data ditempatkan di bawah kendali kedaulatan demi mendukung pembangunan India. Pernyataan semacam itu dibuat oleh pejabat India di luar negeri dan di dalam komite parlemen, serta tercermin dalam aturan yang mengatur berbagai aspek data di dalam negeri, terutama draf RUU Perlindungan Data Pribadi 2018 dan 2019.

Beberapa tahun terakhir telah terlihat beberapa intervensi kebijakan pada tata kelola data oleh berbagai kementerian dan departemen pemerintah India. Meskipun dihubungkan oleh visi "kedaulatan data" bersama dan kebutuhan menggunakan data untuk mengejar pembangunan dan memberdayakan komunitas yang rentan, tampaknya terdapat beberapa hal yang tidak konsisten serta celah dalam kebijakan ini.

Langkah kebijakan signifikan pertama pada pelokalan data dimulai dengan pemberitahuan dari Reserve Bank of India (RBI) pada April 2018. Pelokalan ini memaksa penyimpanan dan pemrosesan semua data pembayaran di India. WhatsApp, Google Pay, MasterCard dan beberapa perusahaan asing memprioritaskan kepatu-

han terhadap arahan ini untuk mempertahankan posisi mereka di sektor pembayaran yang berkembang pesat di India. Arahan RBI diikuti oleh beberapa pemberitahuan yang mewajibkan berbagai bentuk lokalisasi data di berbagai industri. Beberapa industri tersebut termasuk pelayanan kesehatan, *e-commerce* dan asuransi. Aturan yang paling luas adalah draf RUU Perlindungan Data Pribadi Agustus 2018. RUU tersebut berisi ketentuan *mirroring* yang mengamanatkan salinan semua data pribadi disimpan di India. Aturan tersebut juga memiliki ketentuan yang membatasi transfer lintas batas untuk semua data yang ditetapkan pemerintah sebagai "data pribadi penting".

Komite Srikrishna merupakan lembaga yang membuat Rancangan Undang-Undang (RUU) perlindungan data untuk pertama kalinya. Mereka menyebutkan dua alasan menonjol yang membenarkan tindakan ini dalam laporan yang menyertainya. Pertama adalah proses panjang lebar yang harus dilalui oleh lembaga penegak hukum India untuk mengakses data yang disimpan dalam yurisdiksi asing. Otoritas India telah mengenali masalah ini sebagai hambatan yang signifikan untuk melakukan investigasi kriminal. Kedua, pelokalan data dapat memungkinkan perusahaan India menggunakan alat pengambilan keputusan berdasarkan data untuk mengakses dan menggunakan data untuk keuntungan ekonomi mereka. Meski begitu, masih banyak proses pengaturan data India yang perlu dipertanggungjawabkan.

Bagian ini akan bertujuan untuk memberikan konteks seputar diskusi perumusan undang-undang pengaturan data di India. Diskusi ini akan menggarisbawahi para pelaku utama dan konseptualisasi data yang mereka miliki serta memeriksa bagaimana preferensi dan persepsi ini telah memengaruhi undang-undang perlindungan data pribadi India.

Ekonomi Digital India

Pemerintah India telah mendorong transformasi digital India. India adalah penjaga dan pengelola Aadhaar,

sebuah program identitas biometrik digital unggulan India yang mendaftarkan 1,2 miliar warga India. India tetap menjadi satu-satunya negara yang telah memberikan identitas yang dapat diverifikasi secara digital berbasis biometrik kepada sebagian besar penduduk dewasanya. Identitas ini memungkinkan warga negara terlibat dan berpartisipasi dalam ekonomi digital yang berkembang pesat. Dengan identifikasi yang aman dan terverifikasi, warga negara India dapat melakukan transaksi tanpa dokumen pendukung tambahan. Dalam putusan baru-baru ini, Mahkamah Agung India mengagungkan signifikansi Aadhaar sebagai "simbol penting ekonomi digital India" yang membuka banyak jalan untuk interaksi pribadi dan komersial.

Aadhaar telah muncul sebagai instrumen penting yang digunakan pemerintah untuk menyalurkan subsidi dan tunjangan dengan memotong antarmuka (*interface*) manusia. Dengan Undang-Undang Aadhaar, pemerintah India telah melembagakan transfer subsidi digital untuk memastikan warga negara India tidak kehilangan haknya. Aadhaar telah menjadi komponen kunci dari beberapa program kesejahteraan kritis, termasuk Undang-Undang Jaminan Pekerjaan Pedesaan Nasional Mahatma Gandhi (*Mahatma Gandhi National Rural Employment Guarantee Act*, MNREGA) yang menyediakan lapangan kerja publik dan Sistem Distribusi Publik (*Public Distribution System*, PDS).

Pemerintah Modi telah menggunakan Aadhaar untuk mempromosikan inklusi keuangan melalui program Jan Dhan Yojana yang membuat rekening bank untuk warga negara India. Sejak 2014 hingga 2018, sekitar 500 juta rekening bank ditautkan ke Aadhaar. Tautan ini memungkinkan pemerintah untuk mentransfer pembayaran kesejahteraan secara langsung[1]. Pemerintah telah meningkatkan akses keuangan melalui program Jan Dham (JAM), di mana 85% warga negara India memiliki rekening bank. Rekening bank ini memperluas akses

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

keuangan ke warga India yang tidak memiliki rekening bank. Hal ini terjadi ketika rekening bank digunakan bersama dengan 1.2 miliar *database* Aadhaar, 1.1 miliar pengguna telepon seluler dan 600 juta pengguna internet. Mengaitkan rekening bank ke Aadhaar melalui standar verifikasi yang kuat memungkinkan pemerintah membasmi kejahatan seperti pencucian uang dan pendanaan teroris.

500
juta rekening bank terhubung ke Aadhaar (2014 – 2018)

85%
masyarakat India saat ini memiliki rekening bank

AADHAAR

600
juta pengguna internet

1.1
miliar pengguna telepon seluler

Lembaga pajak barang dan jasa (Good and Services Tax, GST) telah merampingkan pembayaran pajak bisnis sehingga seluruh transaksi ada dalam satu *platform* digital. Pemerintah memasukkan lebih dari 10 juta bisnis ke dalam *platform* dan inisiatif tersebut masih bertindak sebagai pendorong bagi perusahaan untuk memindahkan operasi mereka secara daring[2]. Pemerintah India juga telah mendirikan pasar elektronik di mana perusahaan besar dan kecil dapat bersaing untuk mendapatkan kontrak pemerintahan dan pemerintah bisa mendapatkan layanan mereka. Empat puluh dua persen transaksi dalam pasar ini melibatkan usaha kecil dan menengah. Saat ini sedang dilakukan upaya untuk

[2] ibid

mendatangkan lebih banyak usaha rintisan, produsen skala kecil dan pelaku pasar lainnya. Portal ini dirancang untuk menghilangkan antarmuka manusia sekaligus meningkatkan cakupan dan akses. Penghilangan antarmuka (*interface*) tersebut dapat memberikan hak istimewa atau bias pada pelaku tertentu.

India telah mendorong digitalisasi dengan meluncurkan inisiatif untuk mendorong adopsi alat dan *platform* digital. Inisiatif Digital india – yang diperkenalkan pada tahun 2015 – bertujuan untuk menjembatani dan memperbaiki kesenjangan digital dalam masyarakat dan mengubah ekonomi India menjadi ekonomi pengetahuan yang diberdayakan secara digital[3]. Digital India melibatkan tiga komponen utama, yaitu: menciptakan infrastruktur digital yang dapat diakses, menyediakan layanan secara digital dan mempromosikan literasi digital di antara warga negara[4]. Pada tahun 2025, inisiatif ini diharapkan dapat berkontribusi antara USD550 miliar hingga USD1 triliun untuk PDB India[5].

Investasi publik di bidang digital telah memadati investasi swasta untuk menelurkan ekonomi digital yang berkembang pesat. Nilai sektor digital inti India – seperti Teknologi Informasi (TI), layanan komunikasi dan manufaktur elektronik – memiliki nilai sekitar 7% dari PDB India pada 2017-2018 atau hampir USD200 miliar[6]. Pada tahun 2025, nilai potensial sektor inti ini diperkirakan menjadi USD435 miliar atau mencapai dua kali lipat dari nilainya saat ini[7]. Meskipun sebelumnya tidak dianggap sebagai bagian dari ekonomi digital India,

---

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

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

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

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

[7] ibid

sektor-sektor seperti pertanian, pendidikan, layanan keuangan, layanan kesehatan dan ritel menjadi bagian dari ekonomi digital karena mereka perlahan-lahan mengalami digitalisasi[8].

Terlepas dari kebijakan dan langkah yang diambil, pola digitalisasi yang tidak merata terjadi di berbagai sektor. Sektor seperti Teknologi Informasi dan Komunikasi (TIK), layanan profesional dan layanan kesehatan, dengan perusahaan yang lebih digital, terwakili di kuartil terbawah dari adopsi digital. Pada saat bersamaan, beberapa perusahaan kuartil teratas berasal dari sektor-sektor seperti transportasi dan konstruksi[9]. Kesenjangan antara perusahaan kecil dan besar dapat dijembatani karena perusahaan kecil lebih cepat dalam mengadopsi teknologi digital, media sosial dan sistem konferensi video. Laju digitalisasi yang cepat juga memungkinkan negara berpenghasilan rendah tumbuh lebih cepat daripada negara berpenghasilan tinggi dalam hal langganan internet[10]. Antara tahun 2014 dan 2018, tujuh dari sepuluh negara bagian dengan tingkat pertumbuhan internet tertinggi memiliki PDB lebih rendah dibandingkan rata-rata nasional[11]. Namun demikian, lintasan pertumbuhan ekonomi digital India belum mencapai puncaknya. Langganan internet baru dimiliki oleh kurang dari setengah populasi[12]. Hal ini dikarenakan hampir 90% transaksi ritel masih berbasis uang tunai.

Beberapa pemain kunci seperti Airtel, Reliance Jio, Vodafonedan Idea telah mengadopsi strategi penetapan harga yang menarik. Strategi ini bertujuan untuk

[8] ibid

[9] ibid

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

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

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

memberi insentif kepada pelanggan India sehingga pelanggan akan membeli produk dan teknologi mereka di sektor telekomunikasi[13]. Penurunan drastis pada harga data seluler memungkinkan perusahaan telekomunikasi memangkas harga dan memperluas basis pelanggan mereka[14]. Sebagai ekonomi digital yang bertumbuh paling cepat secara global, India telah menjadi sangat menarik bagi raksasa teknologi global. Telah terjadi peningkatan kemitraan antara perusahaan India dan raksasa teknologi global seperti kolaborasi Jio-Facebook dan kemitraan Jio-Google terbaru[15].

Meskipun ekonomi digital India menempati urutan terakhir di antara 17 ekonomi digital dengan kemajuan paling besar dalam hal adopsi digital, India menempati peringkat kedua dalam pertumbuhan adopsi digital, yaitu sebesar 90% sejak tahun 2014[16]. Munculnya ekonomi digital yang berkembang dapat dikaitkan dengan investasi berkelanjutan yang dilakukan pada dua dekade yang lalu terkait TIK yang telah mendorong perusahaan telekomunikasi untuk berinvestasi – yang selanjutnya didorong oleh digitalisasi yang cepat dan semakin banyaknya masyarakat yang menggunakan alat digital dalam aktivitasnya sehari-hari. Pertumbuhan ekonomi digital india yang pesat ini telah memaksa perusahaan teknologi global untuk memperdalam komitmen mereka ke India secara individu dan melalui mitra domestik. Persaingan antara perusahaan teknologi dalam dan luar negeri juga berpusat pada masukan utama yang mendorong transformasi digital India – data.

---

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

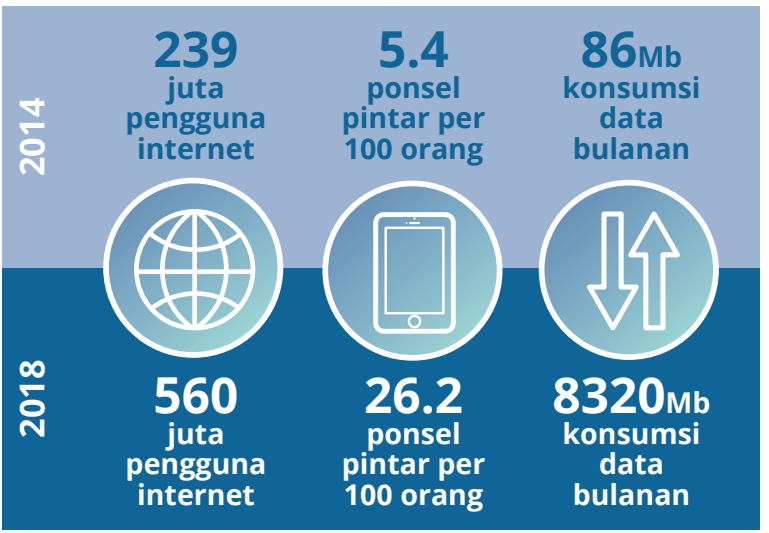
[14] ibid

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

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

Data

Digitalisasi yang cepat memiliki efek bertingkat pada input atau unit produksi yang mendorong interaksi digital – data. Tingkat penggunaan internet yang membeludak dan penetrasi digital telah mengakibatkan jatuhnya biaya data seluler sekaligus meningkatkan penggunaannya. India adalah pasar dengan pertumbuhan konsumen digital tercepat di dunia sekaligus pasar terbesar kedua dalam langganan internet dan pengguna pesan instan secara global[17]. Hanya dalam waktu empat tahun (sejak 2014 hingga 2018), penggunaan data meningkat secara eksponensial. Data menunjukkan terdapat 239 juta pengguna internet, 5.4 ponsel pintar per 100 orang dan konsumsi data bulanan per koneksi sebesar 86Mb pada tahun 2014 silam. Pada tahun 2018, semua angka ini meningkat secara eksponensial dengan perbandingan mencapai 560 juta pengguna internet 26.2 ponsel pintar per 100 orang dan konsumsi data bulanan telah meningkat ratusan kali hingga mencapai angka rata-rata 8320Mb[18].



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

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

Pada tahun 2018, pengguna ponsel di India rata-rata mengonsumsi 8.3Gb data per bulan. Sebagai perbandingan, tingkat rata-rata konsumsi di China mencapai 5.5Gb. Sementara itu di negara digital maju, tingkat rata-rata konsumsi mencapai 8 hingga 8.5Gb[19]. Konsumsi data internet bulanan di India naik menjadi 12Gb pada tahun 2019 dengan perkiraan bahwa angka ini akan meningkat menjadi 25Gb pada tahun 2025[20]. Lonjakan baru-baru ini terutama disebabkan oleh penurunan harga data lainnya. Pada tahun 2014, harga data bulanan (per 1 Gb sebagai persentase dari PDB bulanan) adalah 6.1% dan harga ini turun menjadi 0.1% pada tahun 2018[21], menyusul disrupsi besar-besaran yang disebabkan masuknya Reliance Jio ke pasar pada tahun 2016[22]. Faktor lain yang mendorong peningkatan konsumsi data ini termasuk ponsel pintar yang terjangkau. Faktor harga ponsel yang terjangkau ini meningkatkan jumlah pengguna internet seluler terutama di daerah pedesaan. Dampak lainnya adalah mengubah cara warga negara India mengonsumsi media dan budaya yang telah menjadi lebih berorientasi pada video. Kondisi ini lantas menimbulkan peningkatan penggunaan data[23]. Pertumbuhan konsumsi data India belum mencapai puncaknya – konsumsi data seluler per orang tumbuh pada tingkat 152% per tahun[24].

---

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

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

[21] ibid

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

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

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

Meningkatnya penggunaan data memunculkan kekhawatiran atas hilangnya privasi individu. Potensi hilangnya privasi individu ini bisa terjadi karena para pengguna memberikan informasi pribadi kepada perusahaan telekomunikasi, *platform* dan berbagai layanan saat mereka terlibat secara daring. Dalam laporan UNCTAD (*United Nations Conferece on Trade and Development*), sembilan puluh persen pengguna internet India mengungkapkan kekhawatiran mereka terkait privasi[25]. Masalah privasi ini mencakup proses pengumpulan, penyimpanan dan penggunaan data. Pemerintah India dipaksa untuk mengatur data melalui undang-undang. Salah satu komponen penting akan melibatkan pemerintah dan berbagai aktor untuk memilih apa yang mereka anggap sebagai data. Selain itu, mereka juga harus mengetahui bagaimana data itu akan dikelola dengan mempertimbangkan kepentingan yang saling bersaing. Kepentingan ini termasuk kebutuhan untuk mengontrol data guna memajukan potensi ekonomi dalam ekonomi digital yang berkembang.

Konseptualisasi Data

Penggunaan data yang sangat tinggi dan kekhawatiran mengenai pengelolaan data menunjukkan persepsi yang berbeda atas data pribadi di India. Perbedaan persepsi tersebut tergantung pada siapa yang Anda tanyai dan minat mereka masing-masing.

Dengan bangkitnya ekonomi "data", semakin banyak masyarakat yang menggunakan perangkat pribadi untuk bertransaksi dan berkomunikasi dengan entitas yang berbeda. Akibatnya, timbullah masalah terkait privasi dan kepemilikan informasi pribadi yang dikumpulkan, diproses dan disimpan untuk berbagai tujuan. Jadi, pada satu sisi terdapat perasaan bahwa publik India khawatir tentang penyimpanan dan penggunaan data dan bagaimana data mereka dapat disalahgunakan. Akan tetapi publik juga tidak dapat

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

menahan diri untuk mengurangi penggunaannya karena kenyamanan dan kebiasaan yang berubah[26]. Tampaknya ada keinginan yang berkembang di antara masyarakat untuk terlibat dalam cara transaksional dengan entitas yang mengumpulkan dan berbagi data mereka. Warga India juga semakin merangkul aspek budaya ekonomi digital dan hal ini menyebabkan konsumsi media besar-besaran pada perangkat pribadi – sebuah tren yang dipercepat oleh COVID-19.

Meskipun begitu, terdapat bukti bahwa perhatian publik atas informasi dan data pribadi meningkat. Survei yang dilakukan menunjukkan kecemasan mengenai bagaimana data pribadi masyarakat ditangani secara langsung oleh entitas yang mengumpulkan data (termasuk negara) dan secara tidak langsung setelah data dibagi dan diberikan ke perusahaan yang menggunakannya untuk tujuan kebijaksanaan[27]. Masyarakat India menjadi lebih sadar bahwa informasi pribadi diambil, diubah ukurannya dan dibagikan dengan cara yang merugikan kepentingan mereka. Sebuah kesadaran mulai muncul bahwa proses mengumpulkan dan menyimpan informasi pribadi melalui perangkat berpotensi menyebabkan depersonalisasi. Lebih lanjut, hal ini dapat mengakibatkan tidak hanya hilangnya privasi tetapi juga "rasa diri" (*a sense of the self*). Kondisi ini yang kemudian mendorong beberapa tekanan politik seputar regulasi data[28]. Masyarakat – beberapa dari segmen termiskin – mempertanyakan apakah informasi pribadi mereka dapat dilihat sebagai informasi independen oleh mereka sendiri atau dapat dilindungi dan dimiliki tanpa persetujuan atau keterlibatan mereka. Peningkatan penggunaan berbagai aplikasi dan layanan terjadi di bawah berbagai kampanye yang diprakarsai oleh pemerintah Modi untuk mendigitalkan India. Pemerintah Modi telah mengembangkan platform asli dan asing yang menawarkan berbagai layanan kepada masyarakat India.

---

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

[27] Wawancara dengan analis politik, Carnegie India, 12 Juli 2020.

[28] ibid

Sektor swasta India memiliki kepentingan dalam penerapan aturan yang kuat yang mencakup data saat mereka menangani informasi pelanggan. Hingga saat ini, sebagian besar perusahaan India percaya bahwa data yang mereka kumpulkan adalah milik mereka dan bukan milik pengguna yang datanya mereka kumpulkan[29]. Data pengguna ini mereka anggap sebagai informasi yang dapat mereka gunakan untuk menambah kapasitas analitik, menyempurnakan produk dan layanan yang ada dan merancang aplikasi yang lebih baru untuk penggunaan publik dan pribadi. Diskusi seputar RUU perlindungan data India telah mengubah pandangan tersebut dan memaksa perusahaan India untuk memikirkan kembali peran, pendekatan dan kebijakan mereka terkait data pribadi yang mereka kumpulkan. Perubahan tersebut terkait dengan status pemilik langsung dan pemegang fidusia (*fiduciaries*) yang memiliki rangkaian tanggung jawab berbeda[30].

Konon, ada tekanan balik dari teknologi dan industri besar. Penyedia layanan telekomunikasi seperti Reliance Jio sangat mendorong pemerintah India untuk memberlakukan persyaratan ketat pada perusahaan asing dan domestik untuk menyimpan dan memproses data di India, atau dikenal sebagai lokalisasi data[31]. Sebagian besar perusahaan teknologi kecil dan menengah (terutama perusahaan baru atau rintisan) memiliki kepentingan mengenai undang-undang yang membahas mengenai pengelolaan data. Hal ini karena lingkungan peraturan yang tidak pasti akan mempersulit operasi bisnis mereka. Saat perusahaan dan bisnis di luar ruang teknologi berubah menjadi digital, akan ada tekanan yang meningkat terkait pengelolaan data secara hati-hati dan tidak mengeksploitasi informasi pribadi pelanggan tanpa pedoman internal.

Melimpahnya data telah menimbulkan kekhawatiran mengenai privasi dan kepemilikan data. Hal ini telah

[29] Wawancara dengan mantan pegawai MEITY, 23 Juli 2020.

[30] Wawancara dengan pegawai Think Tank, 13 Juli 2020.

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

memaksa negara bagian India untuk campur tangan. Tampaknya ada pemahaman bahwa pemerintah India dapat berbuat lebih banyak untuk melindungi data pribadi. Dari perspektif negara bagian India, data dikonseptualisasikan sebagai alat yang dapat membantu birokrat dan pembuat kebijakan untuk merancang kebijakan, menyalurkan kesejahteraan dan subsidi, menyetel ulang insentif dan menyediakan berbagai layanan[32]. Perlindungan data membantu pembuat kebijakan India memperkuat infrastruktur digital publik seperti Aadhaar serta membantu aparat penyusun India yang mendorong innovator dan wirausahawan untuk mengembangkan aplikasi untuk penggunaan publik. Sehingga, data diperlukan untuk memfasilitasi hasil ini[33]. Data, baik merupakan data pribadi maupun anonim, membantu penyusunan kebijakan bertarget. Pada akhirnya, kebijakan ini menghilangkan inefisiensi yang merugikan negara bagian India selama beberapa dekade. Perspektif ahli statistik lainnya memandang data sebagai hal penting untuk melindungi kehidupan masyarakat dari ancaman dunia maya, termasuk kejahatan dunia maya (kejahatan siber). Seperti yang diketahui, adanya potensi kejahatan siber menuntut perlindungan dan aksesibilitas pada data pribadi masyarakat. Persepsi ini bersinggungan dengan pendekatan regulasi yang ada yang kerap tidak mengatur atau menegakkan ketentuan perlindungan data pribadi.

Pengaturan Data

IT Act 2000

Meskipun belum ada undang-undang perlindungan data khusus yang diberlakukan oleh India, kerangka kerja yang ada yang mengatur data pribadi adalah Undang-Undang Teknologi Informasi (*Information*

[32] Wawancara dengan mantan pegawai MEITY, 23 Juli 2020.

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

Technology Act / IT Act, 2000). Berdasarkan Bagian 43A, undang-undang ini berisikan peraturan mengenai praktik dan prosedur keamanan saat menangani informasi pribadi[34]. IT Act telah diubah pada tahun 2008 dengan tambahan undang-undang turunan yang berhubungan dengan data. Tambahan undang-undang tersebut dikenal sebagai Aturan Prosedur dan Praktik Keamanan yang Wajar (*Reasonable Security Practices and Procedures Rules,* RSPP) dan berfungsi untuk melindungi data pribadi yang sensitif[35]. Undang-undang tersebut tidak secara proaktif menegakkan aturan terkait pengumpulan dan perlindungan data, akan tetapi memperbolehkan masyarakat untuk mengklaim kompensasi jika perusahaan melanggar aturan RSPP. Bagian 72 dan 72A dari IT Act menjatuhkan hukuman pidana jika pejabat pemerintah atau penyedia layanan mengungkapkan informasi pribadi tanpa persetujuan pribadi atau jika dilakukan untuk menyebabkan kerugian yang tidak semestinya[36]. Aturan privasi yang dikeluarkan pemerintah diterapkan secara bertahap dan hanya berlaku jika RSPP tidak memungkinkan.

Namun, berbagai pertanyaan telah lama muncul terkait validitas hukum RSPP karena tidak ada undang-undang hukum independen yang memaksa organisasi dan perusahaan untuk melindungi data. Hal ini semakin jelas bahwa IT Act belum cukup ditegakkan sehingga memicu regulator lain untuk membuat aturan mereka sendiri agar dapat mengelola kesenjangan yang terjadi. Sektor lain tidak bergantung pada RSPP tetapi telah memilih untuk menyusun aturan sektoral yang mengatur data. Reserve Bank of India telah mengeluarkan surat edaran dan pemberitahuan yang mewajibkan bank dan lembaga keuangan lainnya untuk menjaga data pelang-

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

[35] ibid

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

gan. Meskipun demikian, penting untuk diingat bahwa bank-bank di India selalu diatur secara ketat. Beberapa aturan baru yang harus dipatuhi oleh bank terkait keamanan siber lebih berasal dari keinginan untuk mengelolanya dengan cermat daripada pertimbangan terkait perlindungan data[37]. Badan pengatur lain seperti *Telecom Regulatory Authority of India* (TRAI) dan *Securities and Exchange Board of India* (SEBI) memiliki aturan khusus yang mengatur data tetapi jarang menegakkannya secara efektif. India juga mengandalkan dua alat tambahan yang melacak arus informasi – Sistem Pemantauan Pusat (*Central Monitoring System*, CMS). Sistem ini memberi pejabat pemerintah akses cepat ke lalu lintas internet yang mengalir melalui jaringan tertentu dan Analisis Lalu Lintas Jaringan (*Networks Traffic Analysis*, NETRA), yang menganalisis lalu lintas internet melalui istilah seperti "membunuh" ("*kill*") atau "bom" ("*bomb*")[38].

[37] ibid

[38] CMS diumumkan melalui siaran pers pada tahun 2009 dan NETRA pada tahun 2014. Lihat Biro Informasi Pers, Sistem Terpusat untuk Memantau Komunikasi, 26 November 2009, http://pib.nic.in/newsite/.

Laporan Komite Srikrishna dan RUU Perlindungan Data Pribadi 2018

Dorongan untuk menyusun undang-undang perlindungan data tumbuh dari keputusan Mahkamah Agung India yang menegaskan hak konstitusional atas privasi. Pertanyaan apakah masyarakat India memiliki hak dasar atas privasi muncul dari tantangan konstitusional terhadap Aadhaar pada tahun 2012. Pemerintah bersikeras bahwa Konstitusi India tidak menjamin hak atas privasi. Pertanyaan yang diajukan ke sembilan hakim yang harus memutuskan apakah hak ini ada secara konstitusional. Pada 24 Agustus 2017, Sidang mengenai *Justice KS Puttaswamy* melawan *Union of India* menyatakan bahwa privasi adalah hak fundamental berdasarkan Bagian III dari Konstitusi India yang mencantumkan hak-hak dasar warga negara India – yang mencakup hak yang terkait dengan kesetaraan, kebebasan berbicara dan berekspresi, kebebasan bergerak dan lain-lain[39]. Di bawah konstitusi, hak-hak fundamental ini tidak dapat dicabut oleh hukum. Semua aturan dan tindakan eksekutif tidak boleh melanggarnya. Tidak seperti hak fundamental lainnya, hak atas privasi sebagaimana ditafsirkan oleh putusan Puttaswamy bukanlah hak mutlak tetapi tunduk pada tes dan tolok ukur khusus dan pertimbangan yang bersaing seperti kepentingan negara dan warganya[40]. Pendapat pluralitas yang dikarang oleh Hakim Chandrachud berpendapat bahwa hak atas privasi tidak terlepas dari kebebasan konstitusional lainnya tetapi merupakan aspek esensial dari martabat manusia dan "hak alami yang tidak dapat dicabut"[41]. Menurutnya, Chandrachud mengaitkan hak privasi dengan pertumbuhan ekonomi digital, mengacu pada risiko yang dihadapi masyarakat saat bertransaksi secara digital, termasuk bahaya pengumpulan data dan risiko kehilangan data, serta menggarisbawahi perlunya hukum perlindungan data yang komprehensif[42].

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

[40] ibid

[41] ibid

[42] ibid

Sementara Puttaswamy didengar, pemerintah India membentuk komite ahli yang diketuai oleh Hakim BN Srikrishna (Komite Srikrishna) untuk meninjau aturan dan norma perlindungan data yang ada di India dan merekomendasikan jalan untuk menggantikannya. Laporan menunjukkan bahwa kinerja dan pertimbangan komite, terutama mengenai RUU tersebut, memanfaatkan bantuan Vidhi Center for Legal Policy, sebuah wadah pemikir yang melakukan penelitian dan menyusun RUU[43]. Setelah musyawarah, komite merilis "Lembar Putih tentang Perlindungan Data" ("*White Paper on Data Protection*") pada tahun 2017 dan "RUU Perlindungan Data Pribadi 2018" dengan ketentuan membangun kerangka perlindungan data yang komprehensif untuk India[44]. Rancangan undang-undang berupaya melindungi hak dan otonomi individu terkait data pribadi, menetapkan norma eksplisit mengenai pemrosesan data oleh entitas yang mengumpulkan data pribadi dan membentuk badan yang akan mengatur pemrosesan data. RUU tersebut juga secara terbuka mengakui bahaya yang ditimbulkan oleh ekonomi yang berkembang pesat bagi masyarakat India dan berupaya membuat aturan yang memperbaharui Undang-undang TI (IT Act) yang ada.

RUU awal terdiri dari aturan yang mengatur penanganan data pribadi oleh pemerintah, perusahaan swasta dan organisasi ("pemegang fidusia data") baik yang berbasis di India maupun di luar negeri. Pemrosesan hanya diperbolehkan setelah persetujuan individu diberikan. Agar persetujuan menjadi valid maka persetujuan tersebut harus diberikan secara bebas, spesifik, bebas dari jargon dan dapat ditarik kembali[45].

RUU tersebut juga menjelaskan secara gamblang persetujuan yang harus dipenuhi organisasi yang mengo-

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

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

[45] ibid

lah data sensitif; warga dan konsumen, atau "pemilik data", memiliki hak mengenai data mereka dan mereka dapat meminta pihak yang menyimpan dan mengolahnya atau "penanggung jawab data", untuk menjaga atau menjamin informasi pribadi mereka[46].

Para pemegang fidusia ini memiliki kewajiban khusus saat memproses dan mengelola data pribadi yang mencakup pemberian pemberitahuan dan kejelasan tentang sifat dan tujuan pemrosesan data. Kewajiban berlaku untuk perusahaan swasta dan pemerintah dan mengharuskan mereka memproses data dengan "cara yang adil dan wajar" yang "menghormati privasi individu". RUU 2018 juga membatasi potensi penyalahgunaan dengan menghitung kondisi di mana data harus diproses dan serangkaian tuntutan yang memenuhi persyaratan tersebut.

RUU 2018 juga menyerukan pembentukan Otoritas Perlindungan Data (*Data Protection Authority*, DPA) untuk mengawasi dan mengatur data dan penanganannya antara "data prinsipal" dan "pemegang fidusia data"[47]. DPA ditempatkan dengan tanggung jawab penyelidikan dan pengawasan yang vital dan kewenangan untuk menjatuhkan hukuman dan sanksi pada entitas yang melanggar aturan. Meskipun demikian, pertanyaan seputar otonomi badan tersebut muncul karena sebagian besar regulator akan diterjunkan dari pemerintah[48].

Terakhir, bagian paling kontroversial dari RUU tersebut adalah ketentuan untuk mewajibkan satu salinan data pribadi untuk disimpan di dalam wilayah India guna memastikan pejabat penegak hukum India memiliki akses ke data tersebut; ketentuan ini kemudian dikenal sebagai "pelokalan data"[49]. Jenis data pribadi tertentu (seperti data pribadi penting dengan informasi sensitif) harus disimpan hanya di India. Meskipun RUU tersebut memberikan pengecualian untuk pemrosesan data

[46] ibid

[47] ibid

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

[49] ibid

pribadi dan hak data prinsipal jika datanya digunakan untuk tujuan keamanan nasional, pemrosesan tersebut harus dilakukan secara proporsional dan hanya jika diperlukan. Perlindungan yang memadai juga ditambahkan ke dalam RUU untuk mencegah pengawasan massal.

Tidak mengherankan, perusahaan teknologi India yang cukup besar – Reliance, Paytmdan PhonePe – sudah memiliki pusat data di India atau dapat membayar datanya untuk disimpan di pusat data lokal[50]. Perusahaan besar China – Alibaba dan Xilinx – telah mengambil sikap prolokalisasi. Mungkin karena mereka memiliki pusat data yang disiapkan di India. Namun, langkah menuju pelokalan data ini ditentang keras oleh beberapa perusahaan teknologi Amerika Serikat. Wakil Presiden Kebijakan Publik Facebook, Nick Clegg dan CEO Google, Sundar Pichai, bersama dengan kelompok lobi seperti *US-India Strategic Partnership Forum* (USISPF), *US-India Business Council* (USIBC)dan *National Association of Software and Service Companies* (NASSCOM), melakukan beberapa perjalanan ke India untuk menekankan pesan tersebut[51].

Pelobian oleh industri dan bekerja sama dengan upaya pemerintah AS disebabkan karena lokalisasi data menjadi bagian yang semakin penting dari agenda dalam agenda diskusi perdagangan bilateral. Faktanya, Menteri Luar Negeri Mike Pompeo, dilaporkan mempertimbangkan pembatasan jumlah visa H1B yang diberikan kepada warga negara India apabila ketentuan lokalisasi tidak dilonggarkan. Presiden Trump sendiri membuat pernyataan publik yang secara eksplisit mengecam lokalisasi data di KTT G20 Osaka[52]. Lobi oleh pejabat pemerintah AS dan negara barat serta industri teknologi nampaknya berhasil. Ketika Menteri TI Ravi Shankar Prasad mengeluarkan versi revisi dari RUU

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

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

[52] ibid

tersebut pada Desember 2019, ketentuan *mirroring* tersebut hilang.

RUU Perlindungan Data Pribadi 2019

Pengulangan pertama dari RUU Perlindungan Data Pribadi India melemah selama hampir 18 bulan sebelum pejabat India merilis versi terbaru dari rancangan undang-undang pada Desember 2019. Versi revisi tersebut menawarkan perlindungan individu yang kuat terkait pemrosesan data oleh perusahaan. Meski demikian, terdapat perbedaan yang tampak jelas, terutama terkait dengan pengecualian pemerintah dari undang-undang pertama yang memberikan ruang lingkup luas kepada pemerintah untuk mengumpulkan data warga negara tanpa batasan. Ketentuan kontroversial yang mewajibkan penyimpanan salinan semua data pribadi di India, atau pelokalan data, telah dilonggarkan, dengan menerapkan pelokalan hanya pada data pribadi yang sensitif dan kritis, yang definisinya juga telah diklarifikasi.

Terdapat lebih banyak kejelasan mengenai kategorisasi data di bawah versi baru RUU – data dapat diklasifikasikan sebagai data pribadi, data non-pribadi, data pribadi sensitif, atau data pribadi penting.

Data non-pribadi hanyalah data yang dianonimkan[53]. Data pribadi, di bawah Undang-undang TI (IT Act), yang disebut sebagai "informasi pribadi", merupakan informasi apa pun yang terkait dengan orang-perorangan baik secara langsung maupun tidak, dalam kombinasi dengan informasi lain yang tersedia atau kemungkinan besar akan tersedia mampu mengidentifikasi orang. RUU PDP melengkapi ini dengan kesimpulan apa pun yang diambil dari data tersebut untuk pembuatan profil

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

(*profiling*)[54]. Data pribadi yang sensitif mencakup kata sandi; data keuangan, seperti rekening bank dan detil alat pembayaran; data kesehatan, yang memuat catatan dan riwayat baik kondisi fisiologis maupun mental; orientasi seksual; dan informasi biometrik[55]. RUU tersebut meluaskan dengan memasukkan data genetik, status transgender, status interseks, kasta atau sukudan keyakinan agama dan politik atau afiliasi[56]. Jenis data lain yang diusulkan oleh RUU ini adalah data pribadi penting, yang definisinya memungkinkan pemerintah untuk memutuskan tanpa membatasi kewenangan untuk melakukannya. RUU tersebut juga secara ketat melokalisasi data ini, dengan memberikan pengecualian hanya untuk transfer ke negara atau organisasi yang dianggap mampu memberikan perlindungan dan transfer yang melindungi kepentingan vital[57].

Persetujuan, dalam konteks pengumpulan data di India, yang terutama telah didefinisikan oleh RUU Perlindungan Data Pribadi 2019 ("RUU 2019") yang baru saja diusulkan, dikritik karena bisa dimanfaatkan oleh perusahaan swasta untuk menghindari tanggung jawab atas kerugian. Masalahnya terletak pada pengurangan persetujuan RUU 2019 terhadap konsep yang berfokus pada menghindari tanggung jawab atas kerugian alih-alih memastikan kepentingan warga negara terkait hak privasi pribadi mereka.[58] RUU 2019 masih mengadopsi sistem persetujuan menyeluruh, di mana tidak ada ke-

---

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

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

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

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

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

tentuan yang memerlukan "*data fiduciary*", yang mana merupakan entitas yang mengumpulkan dan memproses data individu, untuk meminta persetujuan dari prinsipal data untuk pemrosesan yang baru – hanya saja mereka "harus memberi tahu prinsip data dari operasi-operasi penting dalam pemrosesan data pribadi melalui pemberitahuan berkala" di bawah Pasal 30(2) ("prinsipal data" mengacu pada individu yang datanya sedang dikumpulkan dan diproses). Pasal ini gagal memasukkan persyaratan dalam meminta persetujuan pemrosesan data untuk tujuan selain yang dinyatakan pada saat persetujuan, sehingga menghambat transparansi penanganan data dan membuat prinsipal datanya meminta pertanggung jawaban "*fiduciary*".[59]

Salah satu rekomendasi yang muncul adalah persetujuan itu harus diminta secara bertahap, dan tujuan-tujuan dari penggunaan data harus didefinisikan secara sempit sehingga prinsipal-prinsipal datanya sepenuhnya menyadari bagaimana data mereka digunakan, terutama untuk meningkatkan layanan yang harusnya dapat dinikmati oleh para prinsipal. Meskipun mengurangi "*consent fatigue*" tetap penting, fokusnya persetujuan harus pada otonomi data utama sehubungan dengan data mereka, yang mengatakan bahwa setiap kebijakan mengenai data pribadi harus mencakup ketentuan bagi para prinsipal data untuk menarik persetujuan kapan saja tanpa ancaman konsukensi hukum, juga menyediakan para prinsipal data dengan pilihan untuk mengetahui dan menyetujui pemrosesan yang baru. Pakar-pakar hukum telah menunjukkan bahwa RUU tersebut tidak menyediakan para prinsipal data dengan ketentuan untuk memastikan jalan keluar ini.

RUU 2019 juga dikritik karena memfasilitasi kontrol pemerintah atas data tanpa memastikan prosedur *check and balances*. Secara signifikan, ketentuan yang mewajibkan pemerintah untuk membuat pemrosesan datanya menjadi "diperlukan dan proporsional" telah dihilangkan dari versi terbarunya RUU; selanjutnya, ketentuan lainnya ditambahkan, memberikan keleluasaan total kepada pemerintah untuk membebaskan agensi

[59] Ibid, 5-6.

atau departemen yang terkait dari hukum.[60] Langkah ini membuat kekosongan kebijakan terkait *surveillance* India tetap ada, yang tampaknya tidak kompatibel dengan kerangka kerja perlindungan privasi yang kuat.

Badan pemerintahan baru yang memiliki wewenang untuk membuat peraturan dan kekuatan ajudikasi yang diperlukan untuk menyelesaikan berbagai *trade-off* adalah *Data Protection Authority* ("DPA"), menurut RUU 2018. Namun, RUU 2019 membatasi wewenang institusi tersebut dengan menyerahkannya kepada pemerintah India, yaitu kemampuan untuk memberi tahu kategori data pribadi yang sensitif lainnya dan menentukan serta memberitahukan "*data fiduciary*" yang penting.[61] Perluasan kekuasaan ini dihasilkan dari RUU Tahun 2019 tentang UU DPA. RUU 2018 memiliki ketentuan yang mencakup anggota-anggota independen di komite pemerintahan DPA, khususnya para ahli dari pihak pemangku kepentingan yang dapat mewakili kepentingan non-pemerintah; RUU 2019 menggantikannya sepenuhnya, melalui pasal yang hanya mengizinkan pemerintah.[62]

RUU 2019 tidak mengizinkan adanya anggota paruh waktu di Komite DPA. Selain tidak sejalan dengan praktik undang-undang lembaga lainnya, peraturan ini juga berpotensi mengeksklusi akademisi, peneliti, praktisi, dan ahli teknis yang dapat memberi masukan untuk DPA. Para aktor utamanya, yang mana bertanggung-jawab untuk menunjuk anggota mereka sendiri, juga menimbulkan dimensi baru pada kebebasan DPA. RUU tahun 2018 mengatur bahwa Ketua Peradilan India, atau hakim Mahkamah Agung lainnya, mengepalai panitia seleksinya, sedangkan RUU 2019 mengubah peraturan ini. Implikasinya adalah panitia seleksi menjadi badan yang dipimpin oleh bagian eksekutif pemerintah, seperti Sekretaris Kabinet dan Sekretaris Penanggung Jawab Urusan Hukum dan Elektronika dan Teknologi

[60] Government of India, "The Personal Data Protection Bill", 2019, RUU No. 373 Tahun 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[61] Ibid, 5.

[62] Ibid, 21.

Informasi. DPA berpotensi menjadi kaki tangan pemerintah dan melemahkan penegakan undang-undang perlindungan data, karena memungkinkan pemerintah untuk mengabadikannya dalam lembaga regulator yang dimaksudkan untuk mengawasi pemrosesan data pribadi di sektor swasta dan agensi pemerintah.[63]

Kemudahan yang dapat dilakukan oleh pemerintah untuk membebaskan lembaga pemerintahan dari ketentuan yang telah disebutkan sebelumnya mengkompromikan tujuan RUU untuk memastikan hak individu atas privasi mereka. Tidak dapat diterapkannya RUU pada sistem *"Unique Identifier"* milik Otoritas India, misalnya, sangat memprihatinkan karena sistem tersebut menyimpan semua data Aadhaar. Hakim Srikrishna sendiri menyebut RUU 2019 "tidak konstitusional", mengklaim itu bisa mengubah India menjadi negara bagian Orwellian. Dia kemudian menganjurkan RUU baru tersebut untuk ditantang di Mahkamah Agung, haruskah itu disahkan dalam bentuknya saat ini, menunjuk bagaimana pengamanan diberlakukan dalam RUU 2018 untuk memastikan independensi DPA, dan untuk memastikan perlindungan terhadap penyalahgunaan data pemerintah secara umum, tidak ada di RUU baru tersebut. RUU yang direvisi juga tidak menjelaskan secara memadai kapan DPA akan dibuat dan seberapa cepat badan tersebut akan menegakkan aturan yang terkait dengan *timeline*. Undang-undang baru juga menghapus referensi ke *timeline* yang diuraikan dalam versi sebelumnya, memberikan wewenang penuh kepada pemerintah untuk menentukan kapan dan bagaimana hukum akan berlaku setelah dibuat.

RUU 2019 meningkatkan otoritas pemerintah melalui pengecualian bagi lembaganya untuk memproses data pribadi untuk tujuan-tujuan yang terlalu luas, di bawah Bab 3 dan 9.[64] Fungsi-fungsi negara seperti melaksanakan pembuatan kebijakan yang berlandaskan pada bukti dan pemberian layanan yang tidak memiliki definisi yang spesifik, dan pengecualiannya meninggalkan banyak ruang untuk penyalahgunaan, terutama

[63] Ibid, 21-22.

[64] Ibid, 8-9.

dalam kasus di mana pemerintah dapat mengakses informasi tanpa persetujuan yang cukup. Undang-undang yang diperbarui juga mengharapkan perusahaan dan organisasi untuk mentransfer data non-pribadi kepada pemerintah untuk membantu fungsi-fungsi umum dan perencanaan kebijakan, membuat masalah-masalah terkait perlindungan privasi dan kekayaan intelektual.[65]

Sejauh ini, ada pengakuan yang jelas di India bahwa data menciptakan nilai ekonomi, termasuk nilai-nilai publik dan sosial yang sangat besar.[66] Seperti yang telah disebutkan, India telah berada di garis depan perdebatan seputar lokalisasi data atau penyimpanan domestik dari data pribadi yang dikumpulkan di India. Lokalisasi data yang ditampilkan di RUU Perlindungan Data Pribadi India yang pertama diresmikan pada Juli 2018 oleh Komite Hakim Srikrishna, dan ditekankan di bagian iterasi kedua RUU, dirilis pada Desember 2019 dan sekarang sedang dibahas di parlemen. Di saat RUU PDP sedang dipertimbangkan lebih lanjut, panitia lain yang membahas data non-pribadi (*Non-Personal Data*/ NPD) merilis laporannya tentang apa yang Pemerintah India harus lakukan dengan NPD, yang mana implikasinya bisa lebih penting daripada RUU mengenai data pribadi itu sendiri.

Mengatur Data Non-Pribadi

Pada bulan September 2019, Kementerian Elektronika dan Teknologi Informasi India (MEITY) membentuk tim ahli untuk membahas apakah kerangka kerja tata kelola NPD diperlukan untuk menangani data-data anonim yang dihasilkan. Tim tersebut bertugas untuk membuat saran khusus kepada pemerintah tentang bagaimana

[65] Ibid, 20.

[66] Direfleksikan juga di Survei Ekonomi India 2019. Lihat Government of India, Ministry of Finance, "2019 Indian Economic Survey", https://library.iima.ac.in/public/Economic_Survey_2019_20_Vol_2.pdf.

meregulasi NPD.[67] Komite tersebut berkonsultasi dengan perwakilan dari berbagai sektor, termasuk bisnis, *think tank*, dan masyarakat sipil, untuk mengumpulkan pandangan dan ide-ide mereka. NPD, yang menjadi fokus komite tersebut, mengacu pada data yang dianonimkan atau data yang tidak mengandung informasi pribadi apa pun yang dapat diidentifikasi; pada dasarnya, ini berarti bahwa tidak ada individu dapat diidentifikasi melalui data ini.[68]

Menariknya, RUU Perlindungan Data 2019 tidak mendefinisikan data non-pribadi sebagai "segala sesuatu yang bukan data pribadi", sembari memberikan hak kepada pemerintah untuk mengakses data non-pribadi dan "data pribadi yang dianonimkan" bila dianggap cocok. Namun, dua kategori ini harus diperlakukan secara berbeda.[69] Dalam praktiknya, NPD mencakup tren-tren iklim yang dikumpulkan oleh berbagai layanan atau aplikasi cuaca atau pola lalu lintas yang dikumpulkan oleh operator angkutan umum atau layanan taksi pribadi. Pada dasarnya, panitianya harus merekomendasikan kerangka kerja dan kebijakan yang dapat diadopsi oleh pemerintah untuk memanfaatkan data yang dikumpulkan dari 1,2 miliar warga India, yang mana berbagai entitas, aktor pemerintah dan non-pemerintah seperti usaha kecil dan organisasi lain, dapat menggunakannya untuk meningkatkan kemampuan, operasi, dan layanan mereka.[70]

Kebutuhan untuk mengatur NPD berasal dari dua motivasi. Pertama, seperti data pribadi, NPD memiliki nilai ekonomi tak tertandingi yang membutuhkan regulasi untuk memastikannya digunakan untuk kemaslahatan

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

[68] Ibid.

[69] Government of India, "The Personal Data Protection Bill", 2019, RUU No. 373 Tahun 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

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

umum dan tidak disalahgunakan. Dan kedua, data-data anonim yang dikumpulkan dapat digunakan untuk tata kelola yang lebih baik. Tujuan-tujuan tersebut telah memandu pendekatan pemerintah terhadap data beberapa tahun terakhir. Pada Agustus 2017, regulator telekomunikasi India merilis makalah konsultasi yang mengagungkan nilai ekonomi data dan meningkatkan perlindungan untuk memastikan data pribadi menerima cukup pengamanan.[71] Setelah itu, NITI Aayog merilis Strategi Nasional India untuk Kecerdasan Buatan, yang menyatakan bahwa konsentrasi data di antara beberapa perusahaan teknologi telah mencegah data dapat diakses oleh seluruh ekosistem teknologi.[72] Strategi AI menyarankan bahwa data harus dibagikan secara terbuka untuk tata kelola yang baik. Dorongan ini diperkuat oleh Komite Srikrishna, yang menyusun RUU PDP India yang pertama, yang juga mendorong peningkatan perlindungan data masyarakat, meskipun sudah ada ketentuan yang membahas isu data pribadi.

Perkembangan ini mendahului pembentukan Komite NPD, dipimpin oleh mantan pendiri Infosys Kris Gopalakrishnan. Laporan Komite meminta NPD yang dibuat di India untuk dimanfaatkan oleh lembaga dan perusahaan domestik untuk menghasilkan keuntungan ekonomi.[73] Peraturan NPD yang terpisah pun direkomendasikan, yang memungkinkan berbagai aktor seperti pemerintah, bisnis, dan organisasi lain untuk meminta data anonim untuk tujuan tertentu. Hasilnya, laporan tersebut mengusulkan struktur peraturan yang akan mewajibkan *data-sharing* oleh entitas yang mengumpulkan data, serta pendaftaran mereka dengan regulator data yang baru untuk memanfaatkan data untuk penggunaan pribadi.[74] Untuk memastikan peru-

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

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

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

[74] Ibid, 40-44.

sahaan atau pemerintah menjadi tidak terlalu diprioritaskan, Komite juga mengusulkan pembentukan regulator baru, Otoritas Data Non-Pribadi, untuk mengatur bagaimana NPD digunakan dan dikerahkan. Harapan Komite adalah bahwa *data-sharing* (mengingat jumlah rekor data publik dan pribadi yang dikumpulkan) akan "memicu inovasi pada skala yang belum pernah terjadi sebelumnya".[75]

Apakah inovasi massal terjadi atau tidak, laporan Komite NPD telah meningkatkan kekhawatiran bahwa pemerintah berencana untuk membuat negara digital yang didorong oleh data. Pendekatan ini memberi sinyal kepada perusahaan teknologi Amerika dan India, yang bergantung pada data yang dikumpulkan pada *platform* mereka untuk mengoperasikan bisnis mereka, data tersebut dapat tidak ditahan dan waktunya telah tiba untuk membongkar silo data untuk kepentingan publik. Pertanyaan kuncinya ke depan adalah apakah perusahaan teknologi akan mematuhi pendekatan kebijakan ini jika undang-undang NPD dibuat, yang dapat memaksa mereka untuk memutar kembali investasi dan operasi di India. Selain itu, data anonim yang menjadi lebih mudah diakses juga dapat menciptakan risiko keamanan, terutama yang terkait dengan identifikasi. Taruhannya tinggi. India harus menyeimbangkan antara masalah privasi, risiko keamanan, dan peluang investasi karena mereka akan menentukan bagaimana data pribadi dan NPD akan diregulasi.

Kesimpulan – India

Pada 11 Desember 2019, pemerintah India memperkenalkan RUU Perlindungan Data Pribadi yang telah direvisi. Ravi Shankar Prasad, Menteri Elektronik dan Teknologi Informasi India, mengumumkan bahwa undang-undang akan dibahas di komite parlemen bersama sebelum diajukan ke majelis parlemen di bawahnya; keputusan ini menyusahkan banyak ahli dan analis

[75] Ibid, 30.

yang berpikir bahwa undang-undang akan diberikan ke Komite Tetap Teknologi Informasi untuk pemeriksaan tambahan. Sebagai hasilnya, pertanyaannya berputar-putar di seputar RUU, mengingat signifikansinya untuk perusahaan domestik dan asing yang bergerak di bidang ekonomi digital India dan kritikus yang takut RUU itu memperkuat kontrol pemerintah terhadap informasi pribadi. RUU perlindungan data yang diperbarui tidak banyak membantu mengatasi masalah terakhir, malah menambah. Ke depannya, perusahaan asing harus menyesuaikan diri dengan medan regulasi yang rumit di India seputar perlindungan data.

Mengingat digitalisasi yang cepat dan penggunaan media sosial oleh warga negara India yang meluas, ada permintaan untuk mengatur pengumpulan data di India. Dalam iterasi pertamanya, RUU PDP 2018 berusaha untuk menciptakan kerangka kerja perlindungan data yang komprehensif yang menguraikan tanggung jawab bagi warga negara, organisasi, dan perusahaan yang menyimpan informasi pribadi. Maksud asli RUU itu adalah untuk mengembangkan aturan untuk melindungi privasi individu dan mencegah penyalahgunaan data pribadi. Individu harus secara eksplisit memberikan persetujuan, terlepas dari pertanyaan seputar apakah persetujuan tersebut bermakna, sebelum data mereka dikumpulkan dan digunakan atau dimonetisasi. Perusahaan, atau "*data fiduciary*", harus mematuhi beberapa aturan saat mengumpulkan dan mengolah data. RUU sebelumnya juga mendorong pembentukan otoritas perlindungan data, atau regulator data, yang akan memantau kepatuhan peraturan terhadap pengumpulan dan perlindungan data dan memberikan sanksi bila terjadi pelanggaran. Kewenangan ini akan memiliki kekuasaan atas perusahaan teknologi dan perusahaan lintas sektor yang memperoleh informasi dari pelanggan.

Terdapat tiga masalah dalam RUU 2019 yang sudah direvisi. Pertama, undang-undang meningkatkan kekuasaan negara dan kontrol relatif terhadap hak-hak warga negara. Perundang-undangan memberikan pemerintah kekuatan yang cukup besar untuk mengumpulkan dan menahan data yang dianggap penting oleh India bagi

kedaulatan negara dan kepentingan publik yang lebih besar. Selain itu, RUU menempatkan pembatasan yang lebih sedikit pada lembaga pemerintah India, yang sudah menyimpan data sensitif warga negara India dan informasi yang dikumpulkan melalui database Aadhaar. Instansi pemerintah dibebaskan dari aturan ketat yang mengatur data atas alasan keamanan nasional atau ketertiban umum. Pemerintah juga akan memiliki wewenang untuk menuntut perusahaan teknologi seperti Facebook, Twitter, dan Google berbagi data non-pribadi dan pribadi yang dianonimkan untuk tujuan pembuatan kebijakan, khususnya kesejahteraan dan kebijakan sosial. Peran pemerintah pada perlindungan data telah membelok tajam ke arah lain, dari mengharapkan negara untuk mengikuti aturan data, seperti yang dijelaskan dalam RUU yang asli, untuk membebaskannya. Dengan tegas, pemerintah tampaknya telah memprioritaskan kontrol negara atas data dengan alasan untuk meningkatkan perlindungan data untuk warga negaranya.

Kedua, RUU yang direvisi memberi kekuatan pada Otoritas Perlindungan Data (DPA) yang baru untuk merancang aturan yang spesifik dan menyelesaikan perselisihan yang timbul. Badan tersebut akan menentukan bagaimana persetujuan tersebut dibingkai dan diterapkan. Keanggotaan dalam DPA cenderung melibatkan pejabat pemerintahan tingkat tinggi. Tidak jelas bagaimana otoritas baru akan berkembang karena jumlah data online yang meningkat secara eksponen awalnya karena semakin banyak warga India yang menggunakan internet. Apa yang juga tetap tidak jelas apakah regulator yang diusulkan dapat menjalankan fungsi dengan baik di bawah kewenangannya di masa depan, yang mana bisa memberikan ketidakpastian di antara perusahaan yang menginginkan penegakan aturan yang jelas.

Ketiga, RUU 2019 melonggarkan ketentuan mengenai lokalisasi data atau aturan yang mengharapkan perusahaan untuk mengumpulkan data pribadi untuk menyimpan salinannya di India. Regulasi baru tersebut mewajibkan perusahaan teknologi untuk menyimpan data sensitif, seperti keuangan dan biometrik, di server India tetapi memungkinkan data diproses di luar negeri

di kondisi tertentu. Meskipun pelokalan data ditempa, RUU baru berisi ketentuan penting – verifikasi identitas – yang dapat memengaruhi bagaimana *platform* media sosial seperti Facebook beroperasi dan bagaimana warga menggunakan *platform* yang digerakkan oleh konten. *Platform* seperti Facebook akan diperlukan untuk memberi pengguna cara untuk memverifikasi identitas mereka dan menampilkan tanda umum yang berkaitan dengan verifikasi sebelum mereka berkomunikasi secara daring. Dengan langkah ini, pemerintah berupaya membendung penyebaran berita palsu dan misinformasi dari *platform* ini.

RUU perlindungan data terbaru India tidak mirip dengan versi awalnya. Revisinya menghasilkan lebih banyak pertanyaan tentang apakah India dapat memajukan globalisasi, terutama mengingat digitalisasi yang cepat dan kontrol negara yang lebih luas. *Trade-off*-nya tampak sulit. RUU Perlindungan Data 2019, ketika disahkan, tetap berlaku untuk menambah kekuasaan negara atas bagaimana data dikumpulkan, diproses, dan digunakan, dan mendorong India untuk memiliki kontrol yang lebih besar, bukan keterbukaan, dalam hal tata kelola internet.

Indonesia – Meregulasi Data

Pembukaan

Ketika internet pertama kali digunakan secara luas di Indonesia di tahun 1990-an,[76] keamanan dan privasi data mulai dipandang sebagai hak asasi manusia yang harus dilindungi oleh negara.[77] Konstitusi Indonesia (Undang-Undang Dasar Republik Indonesia 1945) mengakui hak ini. Pasal 28G Ayat (1) UUD menyatakan bahwa "setiap orang berhak mendapatkan perlindungan untuk dirinya sendiri, keluarga mereka, kehormatan mereka, martabat mereka, dan harta benda mereka, dan mereka juga berhak atas rasa aman dan perlindungan dari ancaman apa pun yang mendorong mereka untuk melakukan atau tidak melakukan sesuatu, karena itu adalah hak asasi manusia."[78]

Ini berfungsi sebagai kerangka hukum untuk peraturan perlindungan data di Indonesia, di mana privasi data dianggap sebagai bagian dari hak asasi manusia. Selain itu, UU No. 39/1999 tentang Hak Asasi Manusia menyor-

[76] Lihat Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2017, Sejak Kapan Masyarakat Indonesia Menikmati Internet. Tersedia di https://stei.itb.ac.id/id/blog/2017/06/19/sejak-kapan-masyarakat-indonesia-nikmati-internet/. [Diakses pada 24 Juni 2020].

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

[78] Undang-Undang Dasar 1945 Republik Indonesia.

oti kebebasan privasi sehubungan dengan komunikasi melalui media elektronik.

Ketika penetrasi internet Indonesia meningkat, masalah terkait perlindungan data mulai mempengaruhi berbagai aspek kehidupan masyarakat. Wacana tentang perlindungan data tidak lagi hanya berkisar pada perlindungan data pengguna; semakin banyak tentang bagaimana data dikumpulkan, disimpan, diproses, dan digunakan.[79]

Urgensi Peraturan Privasi Data

Empat isu utama yang menyoroti urgensi untuk peraturan privasi data di Indonesia adalah:

1) Persepsi publik tentang privasi data

Tingkat penetrasi internet di Indonesia mencapai 73,7% pada tahun 2020.[80] Ini setara dengan 201,58 juta internet pengguna dari total populasi 273,52 juta orang.[81] Indonesia termasuk pasar lima besar secara global

Level penetrasi internet
73.7%

160 juta
pengguna aktif media sosial

[79] Undang-Undang No. 39/1999 tentang Hak Asasi Manusia.

[80] Lihat Pusat Survei Asosiasi Penyelenggara Jasa Internet & Indonesia, 2020, *Laporan Survei Internet APJII 2019-2020 (Q2)*. Tersedia di https://apjii.or.id/downfi le/downloadsurvei/infografi s_apjii.pdf%20. [Diakses pada 26 Maret 2021].

[81] Lihat Ibid.

untuk raksasa teknologi AS Facebook dan Twitter.[82] Ada 160 juta yang pengguna media sosial aktif pada Januari 2020, 8.1 persen meningkat dari April 2019.[83]

Istilah "*data is the new oil*" mewakili bagaimana perusahaan teknologi memperoleh manfaat dari aktivitas digital masyarakat. Skandal Cambridge Analytica tahun 2018 adalah salah satu kejadiannya, di mana jutaan data pribadi pengguna Facebook data tanpa persetujuan.[84, 85]

Masalah lainnya adalah tingginya jumlah pengguna internet yang tidak dibekali dengan pengetahuan yang memadai tentang privasi data dan bagaimana mereka harus mengelola data pribadi mereka Wahyudi Djafar, Wakil Direktur Riset di ELSAM, sebuah LSM hak asasi manusia, mencatat betapa seringnya orang-orang memposting data pribadi yang sensitif (alamat rumah, nomor telepon, dll) di berbagai platform media sosial.[86]

Meskipun beberapa organisasi masyarakat sipil telah menyerukan peningkatan kesadaran masyarakat tentang data pribadi, diperlukan upaya struktural oleh pemerintah untuk perlindungan terhadap risiko data pribadi. Menyediakan perangkat hukum dan/atau badan pengatur yang menyeluruh tentang per-

[82] Johny Plate di Reuters, 2019, "Indonesia needs to establish a data protection law urgently". Tersedia di https://www.reuters.com/article/us-indonesia-communications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Diakses pada 3 Juni 2020].

[83] We Are Social dan HootSuite, 2020, "Digital Indonesia", https://data-reportal.com/reports/digital-2020-indonesia. [Diakses pada 3 Juni 2020]

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

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

[86] Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan", ELSAM (daring). Tersedia di https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-di-indonesia/. [Diakses pada 24 Juni 2020].

lindungan data pribadi adalah contoh dari pendekatan struktural ini.

2) Peluang ekonomi dari peraturan perlindungan data

Indonesia, seperti banyak negara Asia Tenggara lainnya, mengalami pertumbuhan yang kuat dalam ekonomi digitalnya. Antara 2015 dan 2020, nilai ekonomi digital Indonesia tumbuh dari USD8 miliar menjadi USD40 miliar.[87]

Nilai ekonomi digital Indonesia

2015: USD8 miliar

2020: USD40 miliar

2025: USD150 miliar (perkiraan)

Pada tahun 2025 diperkirakan nilai devisa ekonomi digital negara akan mencapai USD150 miliar.[88] Pada tahun 2017, Presiden Joko Widodo mengeluarkan Peraturan Presiden 74/2017 tentang Roadmap *E-Commerce* Nasional, 2017-2019.[89] Kebijakan ini menekankan pada inisiatif untuk meningkatkan pertumbuhan ekonomi Indonesia melalui pengembangan ekonomi digitalnya. Peraturan perlindungan data yang kuat telah diadopsi di beberapa negara, seperti GDPR Uni Eropa, serta Kerangka Privasi yang diadopsi oleh Organisasi untuk Pengembangan Kerjasama Ekonomi (OECD) dan Kerjasama Ekonomi Asia-Pasifik (APEC).

---

[87] Jakarta Globe, 2020, "Jokowi hopes to unleash digital economy potential". Tersedia di https://jakartaglobe.id/tech/jokowi-hopes-to-unleash-indonesias-digital-economy-potential/. [Diakses pada 3 Juni 2020].

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

[89] Lihat Kementerian Komunikasi dan Informatika, 2017, Inilah Road Map E-Commerce Indonesia 2017-2019. Tersedia di https://kominfo.go.id/content/detail/10309/inilah-road-map-e-commerce-indonesia-2017-2019/0/berita. [Diakses pada 26 Juni 2020].

Namun Indonesia tertinggal karena tidak adanya peraturan perlindungan data umum. Ini berisiko merusak daya tawar negara dalam beberapa negosiasi perdagangan terkait ekonomi digital. Indonesia menghadapi masalah saat memperdagangkan data dengan negara lain yang sudah memiliki peraturan tersebut. Ketidakmampuan untuk berdagang data akan menjadi kendala bagi ekspansi aktivitas ekonomi Indonesia. Jadi undang-undang privasi data sangat penting jika Indonesia ingin tetap menarik investasi asing.[90]

3) Ancaman kebocoran data

Munculnya ekonomi digital di Indonesia juga diiringi dengan suatu masalah – perusahaan digital tidak hanya memberikan layanan kepada penggunanya tetapi juga mengumpulkan data pribadi. Meskipun demikian, aktivitas *e-commerce* di Indonesia juga berkembang pesat. Sebuah laporan dari We Are Social dan HootSuite memperkirakan bahwa 88% orang di Indonesia telah membeli produk secara online. Jadi, tak heran jika ban-

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

yak perusahaan e-commerce di Indonesia mengalami pertumbuhan yang pesat.

Namun, lanskap ekonomi digital tidak kebal terhadap kejahatan dan harus berurusan dengan insiden di masa lalu, termasuk pencurian informasi pribadi pengguna karena kebocoran data.[91, 92, 93] Kebocoran data cenderung terjadi di domain sosial-politik. Misalnya, Komisi Pemilihan Umum Indonesia mengalami pembobolan 2,3 juta informasi pemilih.[94] Urgensi perlindungan data pribadi telah menjadi lebih kritis selama pandemi Covid-19, karena lembaga pemerintah mengumpulkan data tentang pasien dan kasus-kasus potensial. Banyak insiden yang dilaporkan terkait kebocoran data pribadi.[95]

Kasus-kasus pelanggaran data masih diselidiki sekarang; mereka memberikan cerita-cerita peringatan tentang risiko dari kurangnya perlindungan legislatif untuk data pribadi. Pertama, ekosistem digital Indonesia (baik yang berkaitan dengan milik swasta atau milik pemerintah) rawan untuk peretasan digital. Sebagai negara dengan jumlah pengguna internet yang sangat besar, sudah seharusnya menjadi prioritas utama bagi pemerintah Indonesia untuk melindungi data di semua sektor dari serangan digital.

---

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

[92] Tempo.co, 2019, "Bukalapak confirms an attempted customer data breach". Tersedia di https://en.tempo.co/read/1186473/bukalapak-con- fi rm-of-an-attempted-customer-data-breach. [Diakses pada 3 Juni 2020].

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

[94] Setiawan, R., 2020, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", Tirto. Tersedia di https://tirto.id/fA5B. [Diakses pada 24 Juni 2020].

[95] Tempo.co, 2020, "Ministry still Tracing Indonesia's Covid-19 patients' data leak". Tersedia di https://en.tempo.co/read/1356052/ministry-still-tracing-indonesias-covid-19-patients-data-leak. [Diakses pada 28 Juni 2020].

Kedua, mengingat tidak adanya regulasi perlindungan data umum, pemerintah tidak dapat melaksanakan penegakan hukum secara efektif. Dalam kasus Tokopedia, sebagaimana adanya platform bisnis pribadi, regulasi perlindungan data umum akan mengarahkan pemerintah untuk mengambil langkah-langkah yang tepat dalam memberikan sanksi kepada Tokopedia, jika platform terbukti harus bertanggungjawab atas kebocoran data masif yang terjadi.

Selanjutnya, penelitian dari ELSAM mencatat bahwa beberapa perusahaan teknologi di Indonesia belum mengadopsi kebijakan perlindungan data apa pun, Sebagian karena belum ada peraturan yang dikeluarkan oleh Pemerintah Indonesia.[96]

4) Perdebatan tentang draf UU Perlindungan Data Pribadi

Perlindungan data pribadi telah mendapatkan perhatian dari organisasi masyarakat sipil (OMS) Indonesia. OMS seperti ELSAM, ICT Watch, dan SAFEnet telah mendesak pemerintah untuk mengadopsi RUU Perlindungan Data Pribadi (PDP).[97, 98, 99] Pemerintah, melalui Kementerian Komunikasi dan Informatika (Menkominfo), juga telah mendesak lembaga legislatif (Dewan Perwakilan Rakyat atau DPR) untuk mengesahkan undang-un-

[96] Lihat ELSAM, 2019, Penyalahgunaan Data Pribadi Meningkat, Perlu Akselerasi Proses Pembahasan RUU Perlindungan Data Pribadi. Tersedia di https://elsam.or.id/5806-2/. [Diakses pada 26 Juni 2020].

[97] ELSAM, 2019, "Pentingnya UU Perlindungan Data Pribadi". Tersedia di https://elsam.or.id/pentingnya-uu-perlindungan-data-pribadi/. [Diakses pada 3 Juni 2020].

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

[99] AntaraNews, 2019, "SAFENet harap menkominfo Johnny G Plate selesaikan UU PDP". Tersedia di https://www.antaranews.com/berita/1129032/safenet-harap-menkominfo-johnny-g-plate-selesaikan-uu-pdp. [Diakses pada 3 Juni 2020].

dang ini.[100] Rancangan tersebut telah tercantum dalam program legislasi nasional, untuk ditinjau dan diadopsi sebagai undang-undang, tetapi prosesnya telah ditangguhkan karena kurangnya prioritas. Wawancara dengan Novel Ariyadi, pakar keamanan siber di Indonesia, mengindikasikan bahwa hambatan ini bersifat politis: "Tidak ada keterbukaan dan alasan yang dapat diandalkan mengapa DPR belum mengesahkan UU-nya."[101]

Di tingkat regional, tekanan politik untuk mengeluarkan UU tersebut dapat dilihat dalam bagaimana ASEAN telah mendorong anggota-anggotanya untuk mengadopsi undang-undang perlindungan data pribadi yang lebih baik. ASEAN telah membentuk Kerangka Kerja Perlindungan Data Pribadi melalui Pertemuan Menteri Teknologi Informasi dan Telekomunikasi ASEAN (TELMIN). Kerangka kerja tersebut bertujuan untuk memperkuat perlindungan data pribadi bagi warga negara

[100] Johny Plate di Reuters, 2019, "Indonesia needs to establish a data protection law urgently". Tersedia di https://www.reuters.com/article/us-indonesia-communications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Diakses pada 3 Juni 2020].

[101] Wawancara dengan Novel Ariyadi, pakar keamanan siber dan kebijakan publik di Indonesia, 19 Juni 2020.

ASEAN dan meningkatkan Kerjasama di antara negara-negara anggota. Kerjasama ini terutama didorong oleh promosi perdagangan regional dan global, serta arus informasi.[102]

Meskipun kerangka kerja ini tidak dimaksudkan untuk membuat kewajiban di bawah hukum domestik, Indonesia tertinggal dibandingkan dengan Singapura, Malaysia, Thailand, dan Filipina. Selanjutnya, karena negara-negara ASEAN melakukan perdagangan yang signifikan dengan Eropa, bisnis-bisnisnya harus mematuhi peraturan-peraturan Uni Eropa. Dengan berlakunya GDPR, banyak negara ASEAN sudah mulai meninjau UU perlindungan data mereka.

Pendekatan-pendekatan Sektoral terhadap Perlindungan Data

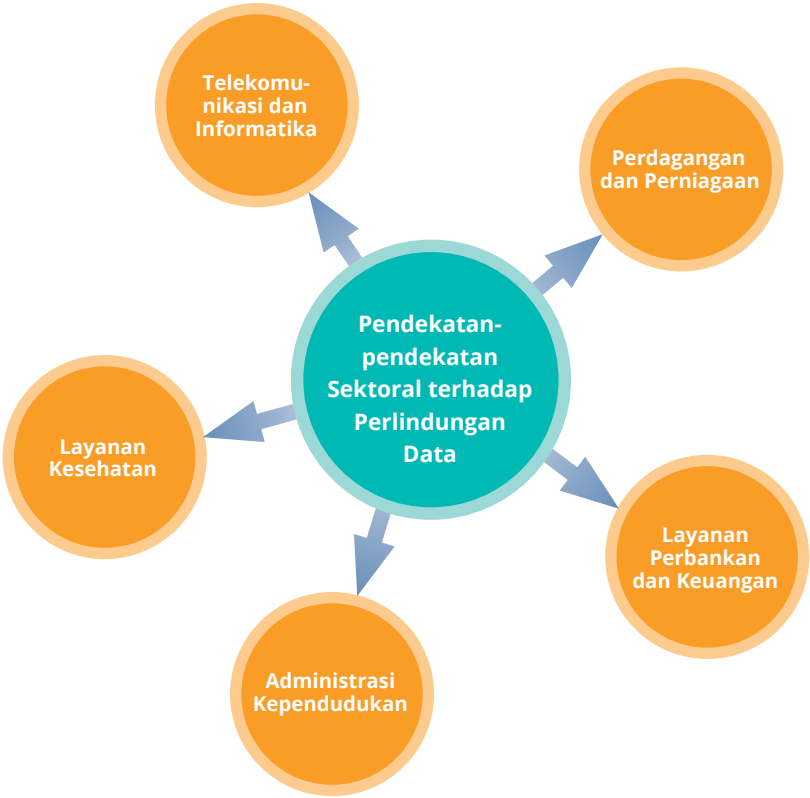
Perlindungan data pribadi di Indonesia diatur oleh setidaknya 30 peraturan yang dikeluarkan oleh berbagai badan pemerintahan dan kementerian.[103] Untuk mempelajari lebih dalam bagaimana perlindungan data diatur dan ditegakkan, bagian ini mengidentifikasi lima sektor yang paling terpengaruh oleh besarnya arus data. Dengan mempelajari sektor-sektor ini, kami menyimpulkan bahwa perlindungan data di Indonesia masih sangat sektoral, dan regulator data (yaitu, lembaga pemerintah) menangani perlindungan data sesuai dengan kebijakan mereka sendiri.

Telekomunikasi dan Informatika

Di sektor ini, konsep tentang perlindungan data berputar seputar kerahasiaan aliran informasi seseorang dan

[102] ASEAN, Pertemuan Menteri Telekomunikasi dan Teknologi Informasi (TELMIN).

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



komunikasi.[104] Meskipun penyadapan informasi dilarang sesuai UU No. 36/1999, operator telekomunikasi masih diberikan wewenang untuk merekam aktivitas telekomunikasi pengguna mereka untuk bukti transaksi, atas permintaan dari pengguna layanan.[105]

Seiring berkembangnya layanan digital, peraturan perlindungan data di bidang telekomunikasi dan informatika juga diperluas untuk mencakup penggunaan data oleh sistem elektronik, sebagaimana tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, juga dikenal sebagai "UU ITE". UU ini menekankan bahwa setiap aliran data pribadi harus diotorisasi sebelum data dipindahkan dari

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

[105] Ibid.

satu orang ke yang lain.[106] Namun, ini juga menciptakan kekurangan yang lain, karena membuktikan bahwa data sedang dipindahkan secara tidak sah seringkali membutuhkan proses yang rumit jika dibahas di pengadilan.[107]

Masalah lain yang muncul dari UU ITE adalah adopsi prinsip "hak untuk dilupakan", seperti yang dicontohkan oleh keputusan oleh Pengadilan Kehakiman Eropa Serikat (CJEU). Adopsi ini membutuhkan sistem elektronik untuk menghapus informasi elektronik yang "tidak relevan" dan/atau dokumen dari database dan layanannya. Namun, peraturan tersebut tidak menjelaskan secara rinci jenis-jenis informasi yang dapat dianggap "tidak relevan".[108] Celah ini dapat menyebabkan masalah lebih lanjut dalam potensi mengganggu kebebasan berpendapat di Indonesia.

Untuk meningkatkan perlindungan data pribadi saat dikumpulkan, disimpan, diproses, dan digunakan, Menkominfo telah menerbitkan beberapa peraturan (Peraturan Pemerintah & Peraturan Menteri) yang menjelaskan aspek-aspek yang lebih rinci dari manajemen data antara pengguna dan sistem elektronik. Misalnya, Peraturan Menkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik menguraikan hak-hak pemilik data dan tanggung jawab kemampuan penyelenggara sistem elektronik terkait pengelolaan data pengguna.[109] Namun, peraturan ini tidak sepenuhnya dipatuhi oleh sebagian besar pengelola sistem elektronik yang beroperasi di Indonesia, karena mereka melihat peraturan itu lemah (belum menjadi

[106] Undang-Undang No. 11/2008 tentang Informasi dan Transaksi Elektronik.

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

[108] Ibid.

[109] Peraturan Menkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

UU resmi).[110] Oleh karena itu, dapat dikatakan bahwa peraturan-peraturan tersebut tidak memiliki kekuatan hukum yang kuat atas pengelola sistem elektronik di Indonesia.

Peraturan-peraturan Perlindungan Data dalam Telekomunikasi dan Informatika

No	Contoh Peraturan	Poin Utama terkait Perlindungan Data	Kekurangan
1	UU No.36/1999 tentang Telekomunikasi	• UU ini menekankan kerahasiaan arus informasi dan komunikasi milik seseorang. Penyadapan informasi dilarang.	• UU ini masih mengizinkan operator telekomunikasi untuk merekam kegiatan pengguna untuk pembuktian transaksi.
2	UU No. 11/2008 tentang Informasi dan Transaksi Elektronik	• Arus data pribadi harus diotorisasi sebelum datanya dipindahkan dari satu aktor ke yang lainnya.	• Dibutuhkan proses hukum yang rumit untuk membuktikan bahwa datanya dipindahkan secara tidak sah.
3	UU No. 19/2006 tentang Amandemen UU No. 11/2008 tentang Informasi dan Transaksi Elektronik	• Adopsi prinsip "hak untuk dilupakan" • Dibutuhkan sistem-sistem elektronik untuk menghapus informasi elektronik yang "irelevan" dan/atau dokumen-dokumen dari layanan dan *database*-nya.	• Definisi dari informasi yang "irelevan" itu sendiri tidak jelas. Oleh karena itu, jika informasi apapun dapat dihapus berdasarkan definisi yang tidak jelas ini, kebebasan berpendapat di Indonesia menjadi dalam bahaya.
4	Peraturan Kominfo No. 20/2016 tentang Perlindungan Data Pribadi di Sistem Elektronik	• Peraturan ini menekankan pada tanggung jawab penyelenggara sistem elektronik dalam mengatur data-data yang dikumpulkan.	• Peraturan ini tidak dilihat sebagai peraturan yang mengikat secara hukum bagi penyelenggara sistem elektronik di Indonesia, sehingga tidak terlalu dipatuhi.

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

Perdagangan dan Perniagaan

Sebagai negara yang semakin gencar melakukan perdagangan dan perniagaan di lingkungan digital, peraturan perlindungan data Indonesia di sektor ini berhubungan dengan yang ada di bidang telekomunikasi dan informatika. Misalnya, UU No. 7/2014 tentang Perdagangan menyatakan bahwa setiap transaksi yang menggunakan sistem elektronik (*e-commerce*) harus sesuai dengan UU No. 11/2008 tentang Informasi dan Transaksi Elektronik atau "UU ITE".[111]

Anehnya, UU No. 8 Tahun 1999 tentang Perlindungan Konsumen tidak menekankan pentingnya perlindungan data pribadi, melainkan ketersediaan informasi yang tepat mengenai produk atau layanan penjual kepada konsumen.[112] Peraturan ini menyoroti fakta bahwa peraturan perlindungan data dalam sektor perdagangan dan perniagaan masih berdasarkan peraturan yang berlaku untuk bidang telekomunikasi dan informatika.

Peraturan Perlindungan Data dalam Perdagangan dan Perniagaan

No	Contoh Peraturan	Poin Utama terkait Perlindungan Data	Kekurangan
1	UU No.7/2014 tentang Perdagangan	• Dengan berkembangnya jumlah transaksi *e-commerce*, UU ini menyatakan bahwa perlindungan data pada transaksi *e-commerce* harus dilaksanakan sesuai UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE).	• Regulasi perlindungan data di Indonesia dalam perdagangan dan perniagaan sangat bergantung pada regulasi yang mengatur telekomunikasi sektor. • Aktor pemerintah yang mengawasi peraturan di sektor telekomunikasi juga harus ikut serta dalam penegakkan hukum kalo ada kebocoran data di sektor perniagaan.
2	UU No. 8/1999 tentang Perlindungan Konsumen	• Alih-alih menekankan perlindungan data pelanggan, UU ini menunjukkan pentingnya informasi mengenai produk penjual atau jasa.	

[111] Undang-Undang Perdagangan No. 7/2014.

[112] Undang-Undang No. 8/1999 tentang Perlindungan Konsumen.

Di sektor ini, peraturan perlindungan data lebih terfokus pada prinsip-prinsip kerahasiaan data. Bank dan penyedia layanan keuangan juga diharuskan untuk mengamankan informasi pribadi apa pun yang mereka kumpulkan dari pelanggan (yaitu, laporan keuangan, kredensial rekening bank, dll).[113] Diatur melalui UU Perbankan No. 10/1998, proses pengumpulan data diizinkan secara hukum, seperti yang dikatakan oleh peraturan perlindungan data di sektor ini bahwa bank dan penyedia jasa keuangan lainnya harus memiliki kapasitas yang cukup untuk menyimpan data pelanggan mereka dengan aman.[114]

Seiring kemajuan teknologi membawa berbagai inovasi layanan keuangan, pemerintah terutama mendirikan lembaga publik baru bernama "Otoritas Jasa Keuangan" atau OJK, yang bertugas untuk mengawasi bank dan penyedia jasa keuangan lainnya. OJK mengeluarkan beberapa peraturan tentang perlindungan data di sektor keuangan. Misalnya, Surat Edaran OJK No. 14/SEO-JK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Konsumen mencantumkan poin-poin data sensitif yang membutuhkan perlindungan karena sering digunakan untuk memverifikasi identitas pelanggan, seperti nama pelanggan ibu kandung, tanggal lahir pelanggan, alamat, dll.[115]

[113] Gazali, D., S. dan Rachmadi, U., 2010, "Hukum Perbankan", Sinar Grafika. Jakarta, hal. 30.

[114] Undang-Undang Perbankan No. 10/1998.

[115] Surat Edaran OJK No. 14/SEO-JK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Konsumen.

Peraturan Perlindungan Data dalam Perbankan dan Keuangan		
No	Contoh Peraturan	Poin Utama terkait Perlindungan Data
1	UU Perbankan Indonesia No. 10/1998	• Semua bank diharuskan untuk melindungi kerahasiaan semua informasi yang berhubungan dengan pengguna mereka.
2	Surat Edaran OJK No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pelanggan	• Mengingat pesatnya adopsi teknologi dalam sektor keuangan Indonesia, peraturan ini menekankan kebutuhan untuk melindungi tidak hanya data keuangan pelanggan, tetapi juga informasi lainnya yang dapat mengungkapkan identitas pelanggan (yaitu, tanggal kelahiran, nama pengguna ibu kandung, dll).
3	Surat Edaran OJK No. 77/ POJK.01/2016 tentang Jasa Peminjaman Berbasis Teknologi dan Informasi	
4	Surat Edaran OJK No. 13/ POJK.01/2018 tentang Inovasi Keuangan Digital di Sektor Keuangan	

Peraturan perlindungan data di sektor ini terutama berfokus pada perlindungan rekam medis pasien sebagai informasi rahasia. Diatur dalam beberapa UU, perlindungan data di sektor kesehatan mengakui hak pasien untuk mengelola datanya sendiri, karena rekam medis tersebut adalah informasi rahasia milik pasien tersebut. Akan tetapi, UU Kesehatan No. 36/2009 tidak membebankan administrasi atau hukuman pidana apapun untuk kebocoran rekam medis dan juga tidak memberikan mekanisme pemulihan bagi pasien jika catatan medis mereka dikompromikan.[116] Ini menciptakan celah dalam hal penegakan hukum tentang perlindungan data di bidang kesehatan.

Peraturan Perlindungan Data dalam Layanan Kesehatan

No	Contoh Peraturan	Poin Utama terkait Perlindungan Data	Kekurangan
1	UU No.36/2009 tentang Kesehatan	• Rekam medis pasien diklasifikasikan sebagai data sensitif dan harus dilindungi. • Pasien memiliki hak untuk mengatur rekam medis mereka sendiri.[117]	• UU tersebut tidak menetapkan hukuman terhadap kebocoran data atau mekanisme pemulihan untuk para pasien jika rekam medis mereka bocor.

[116] Undang-Undang Kesehatan No. 36/2009.

[117] Undang-Undang Kesehatan No. 36/2009.

Administrasi Kependudukan

Perlindungan data di sektor ini sangat bergantung pada kemampuan negara untuk menyimpan dan melindungi data warga negara. UU Nomor 23 Tahun 2006 tentang Administrasi Kependudukan mengatur tentang hak dan kewajiban tata negara untuk menjaga, merawat, dan melindungi kebenaran data warga.[118] Namun, karena UU tersebut telah melalui proses amandemen beberapa kali, ada definisi yang berbeda mengenai mana data yang harus "dilindungi" dan "diklasifikasikan" sebagai "data sensitif".[119] Misalnya, dalam peraturan awal disebutkan bahwa Nomor Induk Pribadi & Keluarga dikategorikan sebagai data sensitif. Namun, dalam amandemen berikutnya (UU No. 24/2013), NIP tidak lagi diklasifikasikan sebagai "data sensitif", dan sebagai gantinya jenis data lain seperti sidik jari dan data retina telah diklasifikasikan sebagai "data sensitif".[120]

Karena negara juga menjalankan proses pencatatan sipil yang menyimpan sejumlah besar jenis data vital, UU No. 43/2009 tentang Pengelolaan Arsip diterbitkan untuk menentukan periode penyimpanan data atau informasi yang disimpan, yaitu sepuluh hingga dua puluh lima tahun.[121]

[118] Undang-Undang No. 23/2006 tentang Administrasi Kependudukan.

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

[120] Undang-Undang No. 24/2003 tentang Amandemen UU No. 23/2006 tentang Administrasi Kependudukan.

[121] Undang-Undang No. 43/2009 tentang Manajemen Arsip.

Peraturan Perlindungan Data dalam Administrasi Kependudukan			
No	Contoh Peraturan	Poin Utama terkait Perlindungan Data	Kekurangan
1	UU No.23/2006 tentang Administrasi Kependudukan	• Negara memiliki tanggung jawab untuk menyimpan dan melindungi data-data vital warga negaranya. • Nomor Induk Pribadi dan Keluarga, Tanggal Lahir, Informasi Kelainan Fisik adalah beberapa jenis data yang dianggap sebagai data sensitif.	• Definisi yang berbeda-beda mengenai mana data yang sensitif bisa membuat kebingungan para penegak hukum dikarenakan banyaknya dan berbeda-bedanya definsi jenis data yang vital dalam peraturan-peraturan tersebut. • Masalah ini berasal dari ketidakjelasan klasifikasi data umum di Indonesia.
2	UU No. 24/2013 tentang Amandemen UU No. 23/2006 tentang Administrasi Kependudukan	• Informasi mengenai Kelainan Fisik, Sidik Jari, Retina, dan Tanda Tangan Pribadi adalah beberapa jenis data yang dianggap sebagai data sensitif.	
3	UU No. 43/2009 tentang Manajemen Arsip	• Semua data dan informasi yang disimpan oleh pemerintah memiliki periode penyimpanan 10 sampai 25 tahun. Setelah periode penyimpanan selesai, datanya bisa “dihancurkan”, atau “dibuka kepada publik” jika tidak mengandung informasi pribadi.[122]	• Mengingat data cenderung sulit untuk dihapus, peraturan ini belum menyediakan mekanisme yang tepat mengenai bagaimana datanya “dihancurkan” setelah melewati periode penyimpanan maksimum.

Berdasarkan penjelasan di atas, penelitian ini menyimpulkan dua poin penting tentang lanskap regulasi perlindungan data di Indonesia. Pertama, regulasi masih berbasis sektor, di mana masing-masing sektor memiliki definisi sendiri dari data yang akan dilindungi dan informasi mana yang akan diklasifikasikan sebagai "sensitif". Hal ini terjadi karena kurangnya peraturan kelembagaan yang menyeluruh yang mengatur tentang perlindungan data. Sebagai gantinya, tanggung jawab

[122] Undang-Undang No. 43/2009 tentang Manajemen Arsip.

diberikan kepada regulator data masing-masing sektor, yang mengontrol dan mendefinisikan mekanisme data ini (yaitu, Kemendagri dengan data pencatatan sipil, OJK dengan data keuangan dan perbankan, Kementerian Kesehatan dengan data rekam medis, dll). Menkominfo, bagaimanapun, memegang lebih banyak tanggung jawab yang signifikan karena memiliki UU Informasi dan Transaksi Elektronik atau "UU ITE", yang biasanya direferensikan oleh regulator data lain ketika mereka berurusan dengan data sensitif (seperti Kementerian Perdagangan yang mengandalkan "UU ITE" untuk mengatur perdagangan di sistem elektronik).

Kedua, ada celah dalam definisi data dan informasi dalam peraturan masing-masing sektor. Contohnya, "UU ITE" membutuhkan pengelola sistem elektronik untuk menghapus "informasi yang tidak relevan" dari platform mereka atau *database*. Tapi, undang-undang ini tidak memberikan rincian tentang definisi "informasi yang tidak relevan". Ini menciptakan potensi konflik dengan peraturan lain, seperti UU No. 14/2008 tentang Keterbukaan Informasi Publik.

Celah ini dapat membuat kebingungan lebih lanjut selama proses penegakan hukum. Penelitian ini menyoroti perlunya Indonesia memiliki regulasi perlindungan data secara umum yang memberikan kepastian hukum yang lebih komprehensif untuk pelaksanaan kebijakan manajemen data. Ini juga menyoroti kebutuhan untuk memiliki badan pengatur yang mandiri menyeluruh atau komisi untuk mengawasi proses penegakan hukum perlindungan data dan regulasi di Indonesia.

Masih ada banyak ruang untuk perbaikan dalam hal perlindungan data pribadi. Bagian berikut akan membahas bagaimana pemerintah mengonsep data pribadi, mengeksplorasi wacana tentang perlindungan data pribadi, dan menguraikan peran beberapa aktor kunci dalam pembuatan RUU perlindungan data pribadi.

Konseptualisasi Data oleh Pemerintah Indonesia

Seperti disebutkan di atas, tiga peraturan secara eksplisit mendefinisikan data pribadi: Undang-Undang Nomor 23 Tahun 2006 tentang Tata Usaha Negara, Peraturan Menkominfo No. 20/2016 tentang Perlindungan Data Pribadi (PDP) dalam Sistem Elektronik, dan Peraturan Pemerintah UU No.71/2019 tentang Implementasi Transaksi dan Sistem Elektronik. Dua yang pertama mendefinisikan data pribadi sebagai data individu yang disimpan, dipelihara, diverifikasi, dan dilindungi oleh pemerintah. Akan tetapi, definisi ini tidak menentukan apa yang dianggap sebagai data pribadi. Definisi yang lebih luas dapat ditemukan di regulasi yang terakhir, yang mendefinisikan data pribadi sebagai data apa pun mengenai seseorang yang dapat digunakan untuk mengidentifikasi suatu individu, baik secara langsung maupun tidak langsung, dengan menggunakan alat elektronik atau sarana non elektronik.

Definisi ini juga diadopsi dalam RUU PDP, yang diharapkan menjadi payung regulasi untuk peraturan yang ada tentang privasi data. Draf menempatkan data pribadi menjadi dua kategori: data umum dan khusus. Data umum meliputi nama, jenis kelamin, kebangsaan, agama, dan data lainnya yang jika digabungkan dengan informasi dapat mengidentifikasi individu. Data spesifik termasuk informasi yang berhubungan dengan kesehatan, biometrik, genetik, orientasi seksual, preferensi politik, catatan kriminal, data anak, data keuangan, dan data lainnya yang dijelaskan dalam peraturan lain yang ada. Namun, draf tersebut tidak secara eksplisit mendefinisikan apa itu data sensitif meskipun itu dianggap penting dan membutuhkan lebih banyak perlindungan dibandingkan dengan data pribadi umum.[123] Dalam

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

konteks lain, misalnya, Petunjuk Perlindungan Data Uni Eropa 1995, data sensitif diklasifikasikan berdasarkan tingkat bahaya atau ancaman yang mungkin terjadi kepada pemilik data jika data mereka diakses oleh pihak yang tidak bertanggung jawab. Tidak adanya definisi pengertian data positif berpotensi memicu multitafsir selama fase implementasi.

Selain terkait definisi data pribadi, RUU PDP mengandung beberapa konsep yang tidak disebutkan dalam regulasi-regulasi sektoral mengenai privasi data. Ia mengadopsi konsep hak untuk dilupakan yang artinya individu dapat mengajukan permohonan penghapusan data.[124] Sebelumnya, penghapusan data pribadi individu oleh operator sistem elektronik hanya dapat didasari oleh perintah pengadilan. RUU PDP juga menginkorporasikan konsep-konsep dan tanggung jawab dari pengontrol data, prosesor data, tipe-tipe data pribadi, hak-hak mengenai data, transfer data, dan syarat-syarat bagi pejabat pelindung data.[125]

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

[125] Ministry of Communication and Informatics, 28 Januari 2020, *Presiden Serahkan Naskah RUU PDP ke DPR RI.* Diakses dari https://www.kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkom-info012020-tentang-indonesia-akan-jadi-negara-asia-tenggara-kelima-yang-miliki-uu-pdp/0/siaran_pers [Diakses pada 5 Juni 2020].

Kemenkominfo menggarisbawahi empat tujuan utama dari UU PDP.[126] Pertama, menetapkan regulasi komprehensif untuk menyatukan regulasi-regulasi sektoral yang sudah ada namun masih terpecah-pecah. Hal ini menjadi penting dalam memastikan bahwa penegakkan hukum perlindungan data terstandarisasi di seluruh sektor. Kedua, untuk membangun keamanan data dengan mencegah dan membahas ancaman-ancaman potensial. Hal ini akan meningkatkan kesadaran di seluruh sektor dan mewajibkan organisasi untuk membangun sistem perlindungan data yang aman. Ketiga, untuk mempercepat ekspansi ekonomi digital Indonesia dengan membangun kepercayaan, transparansi, dan akuntabilitas di antara konsumen, organisasi swasta, dan pemangku kepentingan lainnya. Keempat, untuk meregulasi aliran data lintas-batas. RUU ini sangatlah ambisius dan mengambil pendekatan komprehensif yang mencakup domain publik dan swasta.

Namun formulasi dari UU sendiri menghadapi berbagai rintangan. Pembahasan dimulai pada tahun 2010, tetapi RUU terkini masih dalam pemeriksaan Dewan Perwakilan Rakyat (DPR).[127] Kemenkominfo mengakui bahwa terdapat tantangan, seperti mendapatkan persetujuan diantara kementerian-kementerian dan badan pemerintahan lainnya untuk menyatukan regulasi sektoral, serta memastikan bahwa hukum ditegakkan di seluruh sektor. Hal-hal ini merupakan upaya untuk menyeimbangkan perlindungan data dan inovasi digital.

Diskursus Mengenai Perlindungan Data Pribadi dan Hak atas Data

RUU PDP dibuat mendekati Regulasi Umum Perlindungan Data atau *General Data Protection Regulation* (GDPR) yang telah diimplementasikan di Uni Eropa. Menurut

[126] Wawancara dengan Hendri Sasmitha Yuda, Kepala Subdirektorat Perlindungan Data Pribadi, Kementerian Komunikasi dan Informatika 18 Juni 2020.

[127] Mengacu pada http://www.dpr.go.id/uu/detail/id/353, RUU telah ditinjau di rapat kerja Komisi I dengan pemerintah (Kemenkominfo, Kemendagri, dan Kemenkumham) pada 25 Februari 2020. [Diakses pada 27 Juni 2020].

Kemenkominfo, GDPR dianggap sebagai salah satu regulasi perlindungan data paling komprehensif di dunia. Model Uni Eropa memperlakukan privasi sebagai hak asasi manusia yang fundamental dan hal ini sejalan dengan konstitusi Indonesia. GDPR juga mencoba untuk menyeimbangkan perlindungan hak dengan kebutuhan untuk memastikan kelancaran fungsi ekonomi digital. Kemenkominfo mengklaim telah mengaplikasikan prinsip-prinsip ini ke RUU PDP.

Namun RUU ini tidaklah luput dari kritik. Terdapat setidaknya tiga isu utama dalam UU tersebut: 1) ambiguitas dari definisi-definisinya, 2) inkonsistensi atas kedaulatan data, dan 3) potensi konflik kepentingan pemerintah atas data penduduk. Pertama, mengenai definisi, walaupun RUU mencoba untuk mendefinisikan data pribadi, masih terdapat perbedaan-perbedaan dalam interpretasi akibat definisi yang luas. Sebagai contoh, tidak ada peraturan spesifik mengenai penggunaan *cookies*.

Kedua, kedaulatan data. Presiden Joko Widodo telah menyatakan bahwa Indonesia harus memprioritaskan kedaulatan data dalam berbagai kesempatan. Namun, regulasi yang ada tidak merefleksikan pernyataan ini. Amandemen PP PSTE 71, yang membolehkan data untuk disimpan, diproses, dan dikelola di luar wilayah Indonesia dianggap sebagai ancaman terhadap kedaulatan data.[128] Hal ini dapat dimengerti karena mengawasi data penduduk Indonesia yang terletak di negara-negara lain tidaklah mudah. Terdapat beberapa hukum-hukum transnasional dan isu-isu kedaulatan yang harus diperhatikan. Walaupun debat ini sangatlah kompleks, Kemenkominfo telah mengklarifikasi bahwa mereka memiliki akses dan dapat mengawasi data tersebut. Terlebih lagi, pemerintah yakin bahwa dalam era digital ini, Indonesia tidak boleh bergantung pada regulasi-regulasi "analog". Hal ini berarti regulasi-

[128] CNN Indonesia, 2019, "PP PSTE 'titipan asing' yang gadai kedaulatan data di Indonesia". Diakses dari https://www.cnnindonesia.com/teknologi/20191108152910-185-446726/pp-pste-titipan-asing-yanggadai-kedaulatan-data-indonesia . [Diakses pada 19 Juni 2020].

regulasi mengenai manajemen data lebih penting dari fitur-fitur fisik sepert pusat data.[129]

Ketiga, RUU PDP menggarisbawahi *consent* (persetujuan) sebagai dasar hukum dalam mengumpulkan, menyimpan, dan menggunakan data. Prosesor data harus mendapatkan persetujuan dari dan memberitahukan orang yang bersangkutan sebelum membagikan atau memindahkan data pribadi mereka.[130] Jika hal tersebut tidak lakukan, maka pelaku dapat dihukum penjara atau didenda. Selain isu persetujuan, RUU PDP juga menspesifikasikan bahwa pemilik data memiliki hak untuk: 1)mengetahui tujuan pemrosesan data, 2) menyetujui/tidak menyetujui pemrosesan data mereka, 3) menarik persetujuan, 4) meminta dan mendapatkan kompensasi untuk pelanggaran hak data mereka. Hal ini bertujuan untuk memberdayakan pemilik data untuk tidak hanya memutuskan bagaimana data mereka dikumpulkan, diproses, dan digunakan, tetapi juga untuk mendapatkan hak mereka.

Namun, RUU PDP memperbolehkan pengecualian dalam lima situasi, yaitu: 1) kepentingan pertahanan dan keamanan nasional, 2) ketika dibutuhkan dalam proses yudisial menurut regulasi yang ada, 3) kepentingan negara, khususnya kepentingan ekonomi atau finansial, 4) untuk penegakkan kode etik profesional, dan 5) untuk mengagregasikan data demi penelitian statistika dan ilmiah. Pengecualian ini menguntungkan bagi lembaga pemerintahan atau kementerian, namun terdapat kekhawatiran akan pemberian kekuasaan terlalu besar bagi pemerintah untuk mengakses data penduduk.

Kekhawatiran lain mengenai RUU PDP adalah kurangnya diskusi di level meta. Termasuk diskusi mengenai siapa yang harus diperbolehkan untuk mengatur data

---

[129] Republika, 2019, "PP PSTE Jadi Bentuk Kedaulatan Data". Diakses dari https://nasional.republika.co.id/berita/q1w1pt370/pp-pste-jadi-bentukkedaulatan-data. [Diakses pada 19 Juni 2020].

[130] Umali, T., 5 Juni 2019, "Indonesia drafts the Personal Data Protection Act", OpenGovAsia.com. Diakses dari https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/. [Diakses pada 5 Juni 2020].

seseorang dan bagaimana pengelola data dapat menggunakan data. Diskusi ini berlangsung panas, terutama ketika regulasi privasi data akan diimplementasikan, namun tingkat pemahaman dan kesadaran akan privasi data sendiri masih rendah. Kemungkinan eksploitasi data juga masih tinggi.

Kekhawatiran atas Implementasi

Selain tantangan-tantangan yang ada pada tahap formulasi, terdapat tantangan-tantangan pula dalam memastikan kepatuhan dan penegakkan. Salah satu kekhawatirannya adalah syarat jangka waktu respon untuk prosesor data dan pengelola data. Dalam RUU terkini, prosesor data diberikan 3 x 24 jam untuk menghentikan pemrosesan data dan 2 x 24 jam untuk memberikan akses data pribadi jika pemilik data mengajukan permohonan.

Jangka waktu ini dianggap sangat pendek, dan organisasi-organisasi dapat mengalami kesulitan untuk memenuhi kondisi ini.[131] Sementara itu, GDPR memperbolehkan organisasi-organisasi untuk memproses permohonan serupa dalam jangka waktu satu bulan sejak menerima permohonan. Regulasi di Malaysia memberikan jangka waktu 21 hari. Tidak semua organisasi memiliki kemampuan atau sumber daya untuk mengadopsi dan mematuhi regulasi tersebut dengan jangka waktu pendek. Sehingga, periode transisi dan kampanye yang luas menjadi penting untuk dilakukan. Kemenkominfo berencana untuk mengaplikasikan periode transisi selama 2 tahun untuk memperdalam pengetahuan tiap-tiap pemangku kepentingan yang terpengaruh oleh regulasi ini.

Kedua, pemerintah harus mengeluarkan pedoman teknis untuk industri dan sektor-sektor lainnya sebagai pelengkap dari UU ini setelah disahkan. Jika tidak, maka akan ada ambiguitas. Misalkan penyedia sistem elek-

[131] Wawancara dengan anonim, perwakilan sektor swasta di Indoensia, 25 Juni 2020.

tronik harus melakukan teknologi terstandarisasi dan sertifikasi untuk perlindungan data.

Ketiga, salah satu debat yang terpanas mengenai PDP adalah tidak adanya badan independen yang bertugas untuk mengawasi dan menegakkan regulasi. Hal ini penting untuk menghindari penyelewengan dan komersialisasi oleh pemerintah dan memastikan kepatuhan dari seluruh pihak terkait.[132] Di negara-negara lainnya, sebuah badan pengawas independen ditugaskan untuk menerima, memeriksa, dan merespon keluhan, memberikan nasihat, dan meningkatkan kesadaran masyarakat mengenai privasi data.[133]

Kritik dilayangkan karena tidak adanya badan independen dapat memicu ketidakpercayaan publik dalam penegakkan regulasi. Terlebih lagi, terdapat potensi konflik kepentingan karena Kemenkominfo akan memiliki peranan berganda sebagai pengawas, prosesor data, dan pengelola data. Kemenkominfo berargumen bahwa keputusan untuk tidak membuat badan pemeriksa independen diambil atas dasar efisiensi birokrasi. Namun, mereka masih terbuka untuk mempertimbangkan pendirian lembaga yang berada dibawah naungan pemerintah.

Karena RUU PDP mengadopsi konsep-konsep dari GDPR, isu lain adalah kesiapan pemangku kepentingan dalam pengelolaan data serta budaya, teknologi, dan sumber daya manusia yang diperlukan untuk melakukan perlindungan data. GDPR telah dikritik karena sulit untuk diimplementasikan. RUU PDP di Indonesia membutuhkan organisasi-organisasi untuk mengaplikasikan pengelolaan data dalam tiap-tiap organisasi, namun tidak semua sektor memiliki kebijakan perlindungan data umum. Di Indonesia sendiri, hanya sektor perbankan dan sektor finansial yang sudah mempraktekkan

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

[133] Ibid.

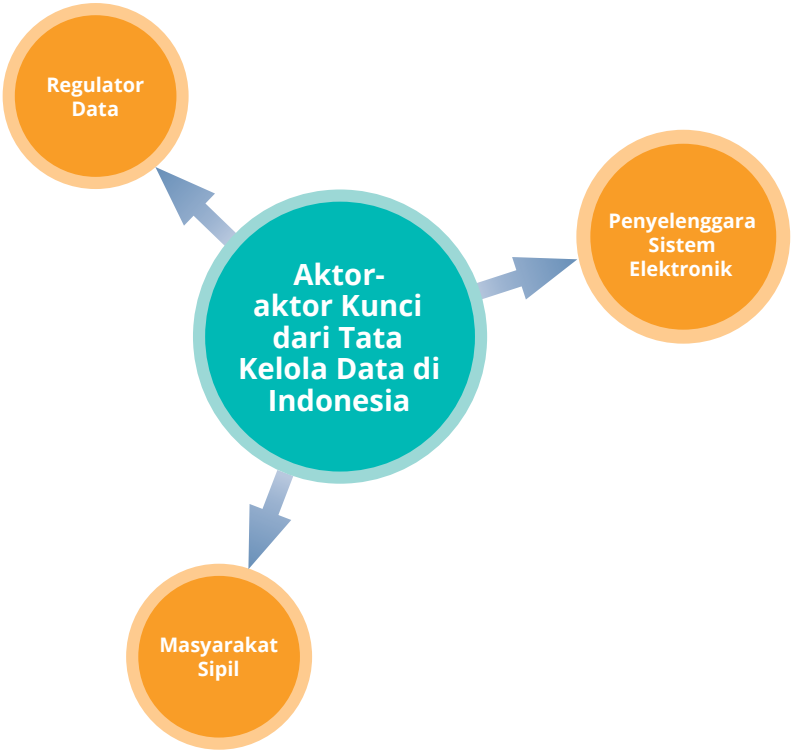
kebijakan perlindungan data.[134] RUU PDP juga memerintahkan organisasi untuk menunjukkan Pejabat Perlindungan Data (*Data Protection Officer* atau DPO) dalam organisasi mereka. Akan tetapi, ketersediaan DPO yang layak telah dipertanyakan. Dalam istilah praktisnya, kementerian terkait juga harus menciptakan standar kompetensi kerja nasional (NWCS) untuk memastikan efektivitas para DPO.

Pemerintah juga harus memperhatikan kesadaran terhadap privasi data. Salah satu tujuan utama dari UU PDP adalah untuk menjamin hak penduduk sebagai pemilik data. Namun pelaksanaan UU ini akan menjadi tidak efektif jika pemilik data tidak sepenuhnya menyadari hak-hak mereka. Sehingga, pembangunan literasi digital mengenai privasi data lewat pendidikan umum menjadi sangat diperlukan.

Aktor-aktor Kunci dari Tata Kelola Data di Indonesia

Formulasi RUU PDP serta implementasi dan penegakannya sangatlah berkaitan dengan aktor-aktor yang terlibat dalam pengelolaan data. Bagian ini menganalisis aktor-aktor kunci dari pengelolaan data di Indonesia berdasarkan kontribusi dan kepentingan mereka dalam formulasi RUU PDP.

[134] Wawancara dengan Novel Ariyadi, praktisi keamanan siber, 19 Juni 2020.



Regulator Data

Regulator data meregulasi aktivitas-aktivitas yang berhubungan dengan penggunaan data pribadi. Ia terdiri dari cabang eksekutif dan cabang legislatif. Hubungan antara kedua cabang ini cenderung stabil, dan dalam berbagai situasi, pembicara dari masing-masing institusi telah menyatakan bahwa mereka bekerja sama dengan baik. Akan tetapi, terdapat tiga isu kritis yang muncul:

1. Formasi badan perlindungan data
2. Lokasi pusat data
3. Pembagian data dengan sektor swasta

Karena RUU PDP mereferensikan GDPR sebagai model utama, kepentingan untuk memiliki badan perlindungan data kemungkinan didasari oleh praktik yang ada di negara-negara Eropa. Misalkan, Inggris telah mendirikan Kantor Informasi Komisioner (*Information*

Commissioner's Office atau ICO), badan independen yang bertugas untuk memenuhi hak-hak informasi penduduk Inggris. Fitur penting dari badan ini adalah imparsialitas yang memungkinkan mereka untuk beroperasi dengan sudut pandang netral. Dalam kasus Indonesia, apakah badan tersebut akan sepenuhnya independen atau berada dalam naungan institusi pemerintah masih diperdebatkan. Kemenkominfo mempresentasikan rencana untuk mendirikan badan tersebut tanpa mengelaborasi aspek parsialitas badan tersebut.

Reaksi dari pembuat kebijakan di DPR cukup beragam. Pada tahun 2019, seorang anggota dewan menyatakan bahwa mendirikan badan baru akan mengeluarkan biaya yang besar.[135] Pada tahun berikutnya, anggota dewan lain menyetujui rencana tersebut, dengan penambahan bahwa badan independen dibutuhkan untuk mencegah penyelewengan otoritas oleh pemerintah.[136] Perdebatan mengenai harus ada atau tidaknya badan perlindungan data menunjukkan perbedaan pendapat antara cabang eksekutif dan cabang legislatif. Menurut direktur TIFA Foundation, Shita Laksmi, badan yang bersifat edukatif kepada perlindungan data harus didirikan.[137] Namun, ia juga menambahkan bahwa pendirian badan independen kemungkinan tidak akan terjadi karena keengganan pemerintah untuk membiayai organisasi yang tidak berada dalam pengawasannya. Walaupun perdebatan ini masih berlangsung, progres terakhir menunjukkan bahwa badan khusus akan didirikan saat RUU disahkan.

Isu penting lainnya adalah lokasi dari pusat data. Pada tahun 2018, Menkominfo pada masa tersebut, Rudiantara, berargumen bahwa pusat data tidak harus

[135] Annur, C. M., 2019, "DPR Kritik Ide Pembentukan Lembaga Perlindungan Data Pribadi", *Katadata.* Diakses dari https://katadata.co.id/berita/2019/07/18/dpr-kritik-ide-pembentukan-lembaga-perlindungandata-pribadi. [Diakses pada 5 Juni 2020].

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

[137] Wawancara dengan Shita Laksmi.

berlokasi di Indonesia.[138] Beliau menambahkan bahwa pusat data yang berada di Indonesia hanya diperlukan untuk menyimpan data pribadi. Data-data lainnya dapat disimpan di server awan. Seorang anggota dewan pun setuju dan berargumen bahwa hanya data dengan tingkat kerahasiaan tinggi yang harus disimpan di pusat data yang berada di Indonesia.[139] Satu tahun kemudian, pandangan kedua institusi tersebut berubah. Ketika UU ITE ditetapkan pada akhir 2019, kanal-kanal media sosial yang beroperasi di Indonesia diharuskan untuk memiliki pusat data di Indonesia. Kedua cabang setuju dalam isu ini.

Perdebatan kunci ketiga adalah apakah data dapat dibagikan antara institusi pemerintahan dan sektor swasta. Kementerian Dalam Negeri (Kemendagri) menyatakan bahwa mereka membagikan data pribadi penduduk Indonesia dengan 1.227 institusi swasta.[140] Tujuan dari inisiatif tersebut adalah untuk mempermudah penggunaan teknologi digital dengan memotong keperluan prosedural ketika mendaftar layanan digital. DPR merespon inisiasi ini dengan tidak menghiraukan keputusan kementerian dengan dasar bahwa inisiatif tersebut dapat mengkompromi keamanan data pribadi.[141] Perdebatan antara kementerian dan DPR dalam isu ini tidak mengubah keadaan dimana Kemendagri membagikan data dengan sektor swasta.

---

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

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

[140] Damarjati, D., 2019, "Kemendagri: 1.227 Lembaga Bisa Akses Data Penduduk, Termasuk Swasta", *DetikNews.* Diakses dari https://news.detik.com/berita/d-4634210/kemendagri-1227-lembaga-bisa-akses-datapenduduk-termasuk-swasta. [Diakses pada 5 Juni 2020].

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

Deskripsi lebih detil mengenai aktor-aktor kunci dan kepentingan mereka dalam tata kelola data di Indonesia adalah sebagai berikut:

Aktor-aktor Kunci Regulator Data

Cabang	Aktor Kunci	Kepentingan dan Peranan
Cabang Eksekutif	Kementerian Komunikasi dan Informatika (Kemenkominfo)	• **Aktor kunci** dalam formulasi kebijakan**:** ◦ Direktorat Jenderal Aplikasi Informatika bertugas mengawasi perusahaan-perusahaan untuk memastikan keamanan dari sistem/ kanal elektronik mereka.[142] ◦ Ditunjuk oleh presiden untuk memimpin isu. • **Pandangan yang perlu digaris bawahi** ketika formulasi kebijakan: ◦ Kemenkominfo menyarankan untuk mendirikan Badan Perlindungan Data Pribadi.[143] ◦ Kemenkominfo menggunakan *General Data Protection Regulation* (GDPR) yang diimplementasikan Uni Eropa sebagai acuan.[144] ◦ Kemenkominfo berpendapat bahwa pemerintah akan menunjuk pejabat data pihak ketiga.[145] Formulasi kebijakan secara umum dilaksanakan oleh Subdirektorat Tata Kelola Perlindungan Data Pribadi.[146]

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

[143] Annur, 2019.

[144] Fauzan, R., 2020, "RUU Perlindungan Data Pribadi Gunakan GDPR Uni Eropa Sebagai Acuan", *Bisnis.com.* Diakses dari https://teknologi.bisnis.com/read/20191202/282/1176768/ruu-perlindungan-data-priba-digunakangdpr-uni-eropa-sebagai-acuan. [Diakses pada 5 Juni 2020]

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

[146] Lihat Kementerian Komunikasi dan Informatika, n.d., *Struktur Organisasi.* Diakses dari https://aptika.kominfo.go.id/profil/struktur-organisasi/. [Diakses pada 4 Juni 2020].

Cabang	Aktor Kunci	Kepentingan dan Peranan
	Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham)	• **Aktor kunci** dalam formulasi kebijakan: ◦ Kemenkumham telah ditunjuk oleh presiden untuk memimpin isu. ◦ Direktorat Jenderal Hukum dan Regulasi mengawasi harmonisasi dari regulasi yang timpang-tindih di tiap-tiap sektor pemerintah.[147] • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ Kepentingan Kemenkumham adalah untuk melindungi kedaulatan data dari pengguna kanal digital Indonesia • Formulasi dari kebijakan secara umum dilaksanakan oleh Direktorat Harmonisasi Peraturan Perundang-undangan II.[148]

[147] Lihat Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, n.d., *Direktorat Harmonisasi Peraturan Perundang-undangan II.* Diakses dari http://ditjenpp.kemenkumham.go.id/struktur-djpp/dithar-monisasi.html . [Diakses pada 11 Juli 2020].

[148] Ibid.

Cabang	Aktor Kunci	Kepentingan dan Peranan
	Kementerian Dalam Negeri (Kemendagri)	• **Aktor kunci** dalam formulasi kebijakan: ◦ Kemendagri telah ditunjuk oleh presiden untuk memimpin isu. ◦ Direktorat Jenderal Demografi dan Pencatatan Sipil bertugas untuk melindungi data pribadi masyarakat Indonesia yang dikumpulkan.[149] • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ Bekerjasama dengan 1.227 institusi, termasuk perusahaan swasta, untuk membagikan data pribadi yang disimpan oleh Dukcapil (dari e-KTP).[150] • Formulasi dari RUU PDP secara umum dilaksanakan oleh Direktorat Demografi dan Pencatatan Sipil.[151]
	Badan Sandi dan Siber Negara (BSSN)	• **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ Membantu pemerintah untuk mengesahkan undang-undang.[152] ◦ Berargumen bahwa undang-undang yang ada belum berbicara mengenai melindungi masyarakat dari penyadapan, tetapi lebih mengenai penyelewengan penggunaan data dalam pinjaman daring dan transaksi elektronik.[153]

[149] Lihat Kementerian Dalam Negeri, n.d., *Struktur Organisasi.* Diakses dari https://www.kemendagri.go.id/page/read/7/struktur-organisasi. [Diakses pada 11 Juli 2020].

[150] Damarjati, 2019

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

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

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

Cabang	Aktor Kunci	Kepentingan dan Peranan
Cabang Legislatif	Komisi I Dewan Perwakilan Rakyat Indonesia	• **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ Anggota Komisi I, Satya, mengkritik rencana pemerintah untuk mendirikan Badan Perlindungan Data 'memberatkan secara finansial'.[154] ◦ Anggota Komisi I, Yan, mendukung rencana pemerintah untuk mendirikan Badan Perlindungan Data untuk menghindari penyelewengan kekuasaan oleh pemerintah.[155] ◦ Ketua Komisi I, Meutya Hafid, menyatakan bahwa "undang-undang akan mencakup kewajiban perusahaan-perusahaan untuk membangun pusat data di Indonesia".[156]

Sumber: Penulis.

[154] Annur, 2019

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

[156] Gatra, 2020, *RUU Data Pribadi Akan Atur Pusat Data hingga RekamanC-CTV.* Diakses dari https://www.gatra.com/detail/news/471976/politik/ruu-data-pribadi-akan-atur-pusat-data-hingga-rekaman-cctv-. [Diakses pada 5 Juni 2020].

Selain dari empat institusi pemerintah di cabang eksekutif, terdapat kementerian-kementerian lain yang terlibat dalam formulasi RUU, yaitu: Kementerian Perdagangan, Kementerian Keuangan, Kementerian Kesehatan, Kementerian Energi dan Sumber Daya Mineral. Sebelumnya, kementerian-kementerian lain yang telah memiliki regulasi sektoral mengenai perlindungan data juga terlibat.[157] Namun, menurut juru bicara Kemenkominfo Hendri Sasmita Yuda, saat ini kementerian-kementerian tersebut hanya terlibat pada sesi-sesi konsultasi yang dilaksanakan oleh Kemenkominfo.[158]

Penyelenggara Sistem Elektronik

Penyelenggara sistem elektronik dapat didefinisikan sebagai organisasi manapun yang mengumpulkan, memproses, dan menyimpan informasi dari penduduk atau pengguna. Aktor-aktor kunci dalam kategori ini berasal dari institusi pemerintah hingga institusi non-pemerintah seperti: e-commerce, perusahaan media sosial, serta industri teknologi lainnya, badan-badan kementerian, komisi nasional, dan lain sebagainya. penyelenggara sistem elektronik adalah lembaga pertama yang diamati ketika terjadi suatu insiden karena mereka adalah pemilik dan pengelola sistem elektronik.

Tiap-tiap aktor kunci mempengaruhi formulasi kebijakan dengan cara yang berbeda-beda. Perusahaan-perusahaan swasta mengadvokasikan kepentingan mereka dengan dua cara: secara kolektif melalui kelompok kepentingan/asosiasi bisnis, dan secara individu lewat representasi diri. Biasanya mereka memberikan saran ke regulator data lewat wawancara publik/suatu acara untuk menunjukkan kepentingan mereka secara tidak langsung atau lewat dialog pribadi dengan pemerintah untuk menyampaikan kepentingan mereka secara langsung.

[157] Peraturan Pemerintah dan Peraturan Menteri secara struktur berposisi lebih rendah dari Undang-Undang.

[158] Wawancara dengan Hendri Sasmita Yuda dari Kementerian Komunikasi dan Informatika.

Institusi pemerintah yang mengelola sistem elektronik dalam operasional mereka tidak selalu memiliki pandangan yang kuat dalam formulasi kebijakan selain dari dukungan yang mereka berikan. Karena tidak ada institusi pemerintah yang perlu diinvestigasi lebih jauh, maka bagian ini akan berfokus kepada kepentingan dan peranan dari aktor-aktor kunci sektor swasta sebagai penyelenggara sistem elektronik.

Aktor-aktor kunci dari sektor swasta dan kepentingan mereka adalah sebagai berikut:

Aktor-aktor Kunci Penyelenggara Sistem Elektronik:

Metode Advokasi	Aktor Kunci	Kepentingan dan Peranan
Kolektif, menggunakan pernyataan publik	Asosiasi Cloud Computing Indonesia (ACCI)	• ACCI adalah asosiasi perusahaan-perusahaan komputasi awan di Indonesia. • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ ACCI mengadvokasikan bahwa demi kedaulatan data dan lain-lainnya, maka server data harus berlokasi di Indonesia.[159] ◦ ACCI mendorong Kemenkominfo untuk meminta pertanggungjawaban perusahaan-perusahaan e-commerce atas kebocoran data berdasarkan PP 71/2019.[160]

[159] Setyowati, D., 2019, "Pelaku Industri Telekomunikasi Minta Pusat Data Wajib Ada di Indonesia", *Katadata.* Diakses dari https://katadata.co.id/berita/2019/02/06/pelaku-industri-telekomunikasi-minta-pusatdata-wajibada-di-indonesia. [Diakses pada 5 Juni 2020].

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

Metode Advokasi	Aktor Kunci	Kepentingan dan Peranan
Kolektif, menggunakan konsultasi langsung	Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI)	• AFPI adalah asosiasi yang mengelola *Peer to Peer* (P2P) *Lending* atau sektor Pendanaan Fintech Daring di Indonesia.[161] • Diakui oleh Otoritas Jasa Keuangan (OJK) sebagai asosiasi resmi dari peminjaman berbasis teknologi dan penyedia layanan pinjaman di Indonesia sesuai dengan Surat No. S-5/D.05/2019.[162] • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ AFPI mendukung formulasi kebijakan karena mempromosikan kepercayaan antara pengguna teknologi finansial.[163]
Kolektif, menggunakan pernyataan publik	Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)	• APJII adalah asosiasi penyedia layanan internet Indonesia • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ APJII mendorong agar RUU segera disahkan demi melindungi data pribadi masyarakat Indonesia

[161] AFPI, n.d., *About.* Diakses dari https://afpi.or.id/en/about. [Diakses pada 30 Juni 2020].

[162] Ibid.

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

Metode Advokasi	Aktor Kunci	Kepentingan dan Peranan
Kolektif, menggunakan pernyataan publik	Asosiasi Big Data dan AI (ABDI)	• ABDI adalah asosiasi perusahaan-perusahaan teknologi yang berkaitan dengan teknologi data, analisis data, pengendalian data, dan ilmu data. • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ ABDI menyatakan bahwa mereka akan berpartisipasi dalam diskusi RUU dan kebijakan lainnya yang berhubungan dengan industri big data.[164] ◦ ABDI mengomentari PP 71/2019 bahwa pusat data harus berlokasi di Indonesia.[165]
Kolektif, menggunakan pernyataan publik	Indonesian e-Commercce Association (iDEA)	• Perusahaan-perusahaan e-commerce adalah aktor yang paling terlihat ketika insiden kebocoran data terjadi. • Beberapa perusahaan e-commerce yang datanya telah bocor termasuk: Tokopedia, Bukalapak, dan Bhinneka. • Idea adalah asosiasi perusahaan-perusahaan e-commerce di Indonesia • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ iDEA mengakui penggunaan data pribadi untuk menelusuri perilaku konsumen di e-commerce.[166] ◦ iDEA menyatakan bahwa mereka belum diundang pemerintah untuk berpartisipasi dalam diskusi mengenai RUU.[167]

[164] Lihat ABDI, n.d., *About.* Diakses dari https://www.abdi.id/tentang-abdi/. [Diakses pada 30 Juni 2020].

[165] Kamaliah, A. Kata Asosiasi Soal Data Center Tak Harus di Indonesia, *DetikInet.* Diakses dari https://inet.detik.com/law-and-policy/d-4775013/kata-asosiasi-soal-data-center-tak-harus-di-indonesia. [Diakses pada 5 Juni 2020].

[166] CNN Indonesia, 2018, *idEA Akui Jejak Data Pribadi Untuk Baca Perilaku.* Diakses dari https://www.cnnindonesia.com/teknologi/20181025185542-185341482/idea-akui-jejak-data-pribadi-untuk-baca-perilaku. [Diakses pada 30 Juni 2020]

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

Metode Advokasi	Aktor Kunci	Kepentingan dan Peranan
Individual	Perusahaan-perusahaan teknologi dan media sosial	• Perusahaan-perusahaan teknologi dan media sosial cenderung tidak terlibat dalam diskusi kebijakan. • Beberapa perusahaan teknologi dan media sosial yang berhubungan dengan diskusi kebijakan adalah Facebook dan Google. • **Pandangan yang perlu digaris bawahi** dalam formulasi kebijakan: ◦ Facebook dan Google setuju untuk membangun pusat data di Indonesia dengan pengaturan mengenai protokol transfer data.[168]

Sumber: penulis.

Berdasarkan kesimpulan diatas, seluruh aktor-aktor kunci dalam kategori penyelenggara sistem elektronik mendukung formulasi kebijakan. Mereka yakin bahwa kebijakan tersebut akan menciptakan ekosistem yang aman untuk bisnis mereka. Namun pandangan mereka mengenai konten-konten spesifik dari kebijakan beragam. Perusahaan layanan komputasi awan lokal cenderung mendorong lokasi server data untuk berada di Indonesia. Dalam berbagai kesempatan, ABDI dan ACCI mengadvokasikan agenda ini. Mereka berargumen bahwa keberadaan server data fisik di daerah lokal penting untuk memastikan kedaulatan data. Akan tetapi, menurut Tony Seno Hartono, ahli teknologi informasi Indonesia, hal ini belum tentu benar. Dalam wawancaranya dengan Center for Digital Society (CfDS), Hartono berargumen bahwa lokasi server data hanyalah satu dari tiga poin yang dibutuhkan untuk memastikan kedaulatan data.[169] Dua poin lainnya adalah keadaan privasi data dan keamanan data.

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

[169] Wawancara dengan Tony Seno Hartono

Secara konsep, privasi data berarti data hanya terlihat bagi pengguna yang berotoritas. Sementara itu, keamanan data meliputi tindakan-tindakan keamanan yang tersemat di data untuk memastikan kerahasiaan, integritas, dan aksesibilitasnya. Tony juga melanjutkan bahwa dalam sistem komputasi awan dimana data disimpan dalam awan, keadaan privasi data dan keamanan lebih penting daripada lokasi server.

Masyarakat Sipil

Masyarakat sipil terdiri dari organisasi non-pemerintah, organisasi non-profit, serta akademisi yang berfokus untuk mengadvokasi tata kelola data yang lebih baik. Mereka secara terus-menerus mengawasi performa regulator data dalam melindungi perlindungan hak digital pengguna, juga mendorong penyelenggara sistem elektronik untuk meningkatkan keamanan layanan mereka.

Terdapat informasi yang beragam tentang organisasi sipil mana yang tergabung dalam formulasi kebijakan. Berdasarkan wawancara yang dilakukan dengan beberapa perwakilan dari masyarakat sipil, regulator data belum mengundang organisasi masyarakat sipil untuk konsultasi dalam formulasi kebijakan. Akan tetapi, perwakilan pemerintah menyatakan bahwa regulator data telah berkonsultasi dengan organisasi masyarakat sipil. Komunikasi antara masyarakat sipil dan regulator data kemungkinan dilakukan secara informal. Beberapa organisasi masyarakat sipil telah mendukung kebijakan ini secara publik.

Aktor-aktor kunci dan kepentingan mereka secara detil adalah sebagai berikut:

Aktor-aktor Kunci Masyarakat Sipil.

Sub-kategori	Aktor Kunci	Kepentingan dan Peranan
Lembaga Swadaya Masyarakat	Southeast Asia Freedom of Expression Network (SAFEnet)	• SAFEnet adalah lembaga swadaya masyarakat (LSM) yang berfokus pada pemenuhan hak akses informasi, hak berekspresi, dan hak untuk merasa aman. • **Pandangan yang perlu digaris bawahi** dalam formulasi kebijakan: ◦ Direktur SAFENet Damar Juniarto menyatakan bahwa: (1) pemerintah harus melindungi data pribadi, bukan hanya data yang berpotensi untuk diperjualbelikan, tetapi juga data yang berpotensi mengancam nyawa; (2) pemerintah harus menetapkan kebijakan dengan cepat; (3) kebijakan akan menciptakan Indonesia yang lebih berdaulat.[170]
Lembaga Swadaya Masyarakat	ICT Watch	• ICT Watch adalah LSM yang bertujuan untuk mengembangkan kapital manusia Indonesia untuk literasi digital, ekspresi daring, dan tata kelola siber.[171] • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ Mendesak pemerintah untuk segera mengesahkan undang-undang.[172]

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

[171] Rizkinaswara L., 2019, "ICT Watch", *Aptika Kominfo.* Diakses dari https://aptika.kominfo.go.id/2019/07/ictwatch/. [Diakses pada 30 Juni 2020].

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

Sub-kategori	Aktor Kunci	Kepentingan dan Peranan
Lembaga Swadaya Masyarakat	Indonesia Cyber Security Forum (ICSF)	• ICSF adalah komunitas para profesional dan ahli keamanan siber. • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ ICSF menyarankan regulator data untuk mendirikan Badan Perlindungan Data Pribadi Independen.[173]
Akademis	Institute for Policy Research and Advocacy (ELSAM)	• ELSAM adalah organisasi hak asasi manusia yang berfokus pada pendirian sistem demokratis politis di Indonesia dengan mempromosikan aktivisme masyarakat sipil dan perlindungan hak asasi manusia. • **Pandangan yang perlu digarisbawahi** dalam formulasi kebijakan: ◦ ELSAM menyarankan regulator data untuk mendirikan Badan Perlindungan Data Pribadi Independen.[174] ◦ ELSAM meminta pemerintah, khususnya Kementerian Dalam Negeri, untuk tidak memberikan data pribadi ke institusi lain manapun tanpa persetujuan pemilik data.[175] ◦ ELSAM mengkritik pemerintah karena tidak memberikan opsi bagi pengguna untuk menghapus akun mereka.[176]

Sumber: penulis.

[173] Fauzan, R., 2020, "Pengamat: RUU Perlindungan Data Pribadi Masih Punya Kelemahan", *Bisnis.com.* Diakses dari https://teknologi.bisnis.com/read/20200212/101/1200621/pengamat-ruu-perlindungan-data-pribadi-masih-punya-kelemahan . [Diakses pada 5 Juni 2020].

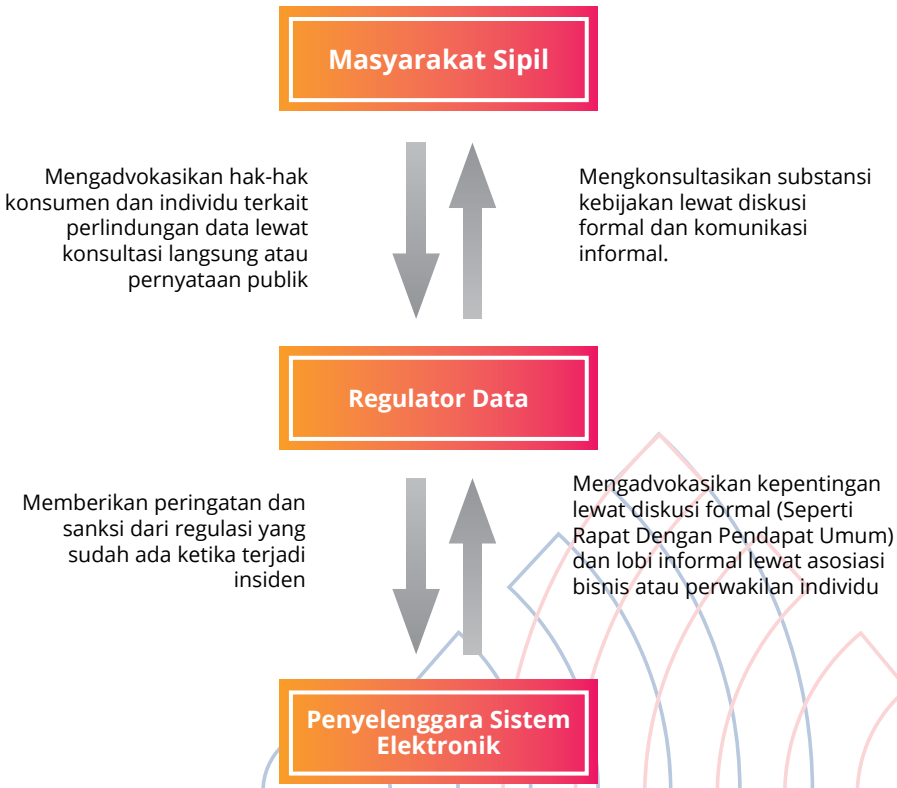
[174] Pertiwi, W. K., 2020, "ELSAM: Harus Ada Pengawas UU PDP di Luar Pemerintah", *Kompas.* Diakses dari https://tekno.kompas.com/read/2020/01/31/12580067/elsam--harus-ada-pengawas-uu-pdpdiluarpemerintah?page=all . [Diakses pada 5 Juni 2020].

[175] Ristianto, C., 2020, "Kemendagri Diminta Kaji Ulang Kerja Sama Data Kependudukan", *Kompas.* Diakses dari https://nasional.kompas.com/read/2019/08/02/13161321/kemendagri-diminta-kaji-ulang-kerja-sama-datakependudukan . [Diakses pada 5 Juni 2020].

[176] Kumparan, 2020, *Regulasi Tokopedia Larang Pengguna Hapus Akun, Langgar Hak Data Pribadi.* Diakses dari https://kumparan.com/kumparannews/regulasi-tokopedia-larang-pengguna-hapus-akun-langgar-hakdatapribadi-1tNCp40Q9au . [Diakses pada 5 Juni 2020].

Selain institusi-institusi tersebut, staf Kemenkominfo Hendri Sasmita Yuda juga menyinggung bahwa terdapat anggota-anggota masyarakat sipil yang dikonsultasikan oleh kementeriannya dalam memformulasikan kebijakan seperti ahli-ahli dari institusi-institusi terkenal seperti Universitas Gadjah Mada, Universitas Indonesia, dan Universitas Diponegoro. Mereka diundang ke diskusi-diskusi yang diselenggarakan oleh Kemenkominfo atau staf Kemenkominfo yang bersifat formal maupun informal. Akan tetapi, informasi publik mengenai keterlibatan dari aktor-aktor tersebut tidaklah tersedia.

Hubungan antar Para Aktor



Poin penting dari diskursus tata kelola data di Indonesia adalah formulasi UU PDP. Hal ini terjadi karena saat ini, regulasi data masih tersebar dalam berbagai regulasi sektoral dan penegakkan-nya masih kurang.

Peranan dan kepentingan dari aktor-aktor kunci disimpulkan sebagai berikut:

1. Regulator data, penyelenggara sistem elektronik, dan masyarakat sipil menciptakan hubungan yang berpusat pada regulator data sebagai pemegang otoritas dalam formulasi kebijakan. Masyarakat sipil dan penyelenggara sistem elektronik memegang peranan advokasi dan difasilitasi dengan kanal komunikasi formal dan informal saat berkonsultasi dengan regulator data.

2. Aktor-aktor regulator data (tiga kementerian dan Dewan Perwakilan Rakyat) berkesinambungan dalam keinginan mereka untuk menetapkan kebijakan. Akan tetapi, perdebatan muncul mengenai formasi badan perlindungan data, lokasi pusat data, dan pembagian data dengan sektor swasta.

3. Aktor-aktor penyelenggara sistem elektronik mendukung ide umum dari kebijakan. Aktor swasta menyuarakan kekhawatiran mereka secara lebih vokal dibanding tipe-tipe aktor kunci lainnya. Akan tetapi, tiap aktor swasta memiliki kekhawatiran tersendiri mengenai substansi kebijakan, tergantung pada kepentingan entitas bisnis atau asosiasi masing-masing.

4. Aktor-aktor masyarakat sipil meminta formulasi kebijakan selesai secepat mungkin. Akan tetapi, tiap-tiap aktor kunci menyalurkan kepentingannya dengan cara yang berbeda-beda. Terdapat dua cara bagi lembaga swadaya masyarakat dan akademisi untuk mengadvokasi kekhawatiran mereka: memberikan pernyataan publik dan melakukan konsultasi langsung dengan regulator data. Isu-isu kekhawatiran yang dibahas oleh aktor-aktor kunci masyarakat sipil adalah formasi badan perlindungan data pribadi independen, pembagian data intersektoral, dan opsi yang diberikan oleh penyelenggara sistem elektronik untuk menghapus akun pengguna.

Kesimpulan untuk Indonesia

Bab ini bermaksud untuk memberikan gambaran umum mengenai regulasi perlindungan data di Indonesia dan menggaris bawahi urgensi pengadopsian regulasi perlindungan data menyeluruh dalam bentuk UU PDP yang saat ini masih ditinjau oleh pembuat kebijakan. GDPR Uni Eropa merupakan sumber utama inspirasi RUU PDP di Indonesia.

Urgensi untuk menciptakan regulasi perlindungan data menyeluruh berasal dari empat masalah: 1) rendahnya kesadaran dan pengetahuan publik mengenai privasi data di tengah tingginya angka pengguna internet dan aktivitas digital; 2) pertumbuhan ekonomi digital yang terhambat akibat tidak adanya regulasi perlindungan data pribadi; 3) beberapa kasus kebocoran data menunjukkan bahwa ekosistem digital Indonesia rawan akan kejahatan digital dan tanpa regulasi yang selayaknya, persekusi legal terhadap kejahatan menjadi sangat sulit; 4) tekanan politis tinggi yang terjadi dalam proses perancangan UU PDP.

Perlindungan data saat ini dikelola lewat pendekatan sektoral yang tidak berhubungan. Terdapat lima sektor yang paling relevan dengan perlindungan data: 1) sektor telekomunikasi dan informatika yang berfokus pada kerahasiaan data. Kemenkominfo telah memperluas hal ini untuk mencakup data digital lewat regulasi-regulasi seperti "UU ITE" dan Permenkominfo No. 20/2016. 2) Sektor perdagangan masih sangat bergantung dengan regulasi dari sektor telekomunikasi dan informasi di tengah pertumbuhan aktivitas ekonomi digital. 3) Sektor perbankan dan layanan finansial berfokus kepada kerahasiaan data konsumen dan hal ini didukung oleh beberapa regulasi perbankan dalam tingkatan perlindungan data yang diperlukan. 4) Sektor kesehatan tidak memiliki regulasi yang secara jelas memberikan sanksi jika kebocoran rekam medis terjadi walaupun rekam medis termasuk sebagai data yang harus dilindungi. Terakhir, 5) Sektor administrasi sipil regulasi perlindungan dan penyimpanan data kependudukan.

Definisi data pribadi dijelaskan dalam Peraturan Pemerintah No.72/2019 dan diadopsi dalam RUU PDP. RUU PDP sendiri dimaksudkan sebagai regulasi menyeluruh atas privasi data. Kemenkominfo menjelaskan bahwa UU ini bermaksud untuk mengharmonisasi regulasi-regulasi sektoral, melakukan upaya preventif terhadap kejahatan yang bersangkutan dengan data, mempercepat pertumbuhan ekonomi digital Indonesia, dan meregulasi aliran data lintas-batas.

Walaupun pengadopsian regulasi ini memiliki urgensi yang sangat tinggi, UU PDP masih dalam tahap peninjauan legislatif. Beberapa isu penting mengenai RUU PDP adalah: pendirian badan perlindungan data, lokasi pusat data, dan apakah pemerintah dapat memberikan informasi pribadi penduduk Indonesia dengan sektor swasta atau tidak. Dua isu pertama telah diselesaikan sementara isu terakhir masih diperdebatkan.

Tantangan lainnya yang menghambat adopsi undang-undang ini adalah: kekhawatiran mengenai kepatuhan dan penegakkan, termasuk didalamnya adalah: singkatnya tenggat waktu yang diberikan ke prosesor data dan pengelola data, tidak adanya petunjuk teknis, tidak adanya badan pengawas independen, rendahnya tingkat kesiapan pemangku kepentingan dalam aspek regulasi perlindungan data, dan kurangnya pemahaman mengenai privasi data oleh pemilik data. Dari segala tantangan ini, faktor ketidakadaan badan pengawas independen merupakan faktor yang paling menghambat RUU PDP.

Terdapat tiga aktor kunci dalam tata kelola data: regulator data, penyelenggara sistem elektronik, dan masyarakat sipil. Regulator data, entitas yang meregulasi penggunaan data pribadi, dapat dibagi menjadi cabang eksekutif dan cabang legislatif. Cabang eksekutif terdiri dari Kemenkominfo, Kemenkumham, dan BSSN, dengan fokus dan tanggung jawab yang berbeda-beda mengenai perlindungan data.

Terdapat berbagai macam aktor yang dapat diidentifikasi sebagai penyelenggara sistem elektronik. Setiap organisasi, baik publik maupun swasta, yang menggu-

nakan data penggunanya dapat menjadi bagian dari penyelenggara sistem elektronik. Aktor-aktor kunci sektor swasta cenderung memiliki lebih banyakan masukan dibanding pemerintah dan mereka memberikan masukan tersebut secara kolektif lewat asosiasi-asosiasi. Perusahaan-perusahaan teknologi dan media sosial secara individu cenderung kurang terlibat dalam diskusi publik mengenai kebijakan PDP. Seluruh aktor kunci sektor swasta secara garis besar mendukung kebijakan PDP, namun masih ada perdebatan dalam beberapa konten spesifik.

Organisasi masyarakat sipil cenderung lebih kritis terhadap regulator data. Regulator data menyatakan bahwa mereka telah melibatkan organisasi masyarakat sipil dalam formulasi kebijakan, sementara beberapa organisasi masyarakat sipil menyatakan sebaliknya.

Tantangan Implementasi Saat Ini

Terdapat tiga faktor utama yang menjadi tantangan implementasi tata kelola data yang baik di Indonesia saat ini, yaitu: 1) rendahnya kapasitas negara untuk menetapkan regulasi yang kuat, 2) rendahnya tingkat kepatuhan masyarakat Indonesia, dan 3) kejadian-kejadian penting lain yang mengalihkan perhatian dari proses regulasi data. Perlindungan data pribadi saat ini dikelola lewat beberapa regulasi sektoral yang tidak saling berhubungan, sehingga memperlambat proses

pengelolaan data dan mempersulit pengadopsian standar intersektoral dalam mengelola data.

Isu lainnya juga berasal dari rendahnya pemahaman mengenai perlindungan data diantara penduduk Indonesia. Masyarakat Indonesia belum memiliki pemahaman yang cukup mengenai informasi pribadi yang dapat dibagikan dengan aman dan dengan siapa mereka dapat membagikan informasi tersebut akibat rendahnya literasi digital. Perlindungan data bukanlah kekhawatiran yang langsung dirasakan oleh masyarakat Indonesia secara umum, sehingga mengurangi urgensi politik bagi pembuat kebijakan. Rendahnya literasi digital juga dapat mengurangi efektivitas UU PDP ketika UU ini disahkan. Sehingga terdapat kebutuhan mendesak untuk menetapkan petunjuk teknis dan kampanye untuk membentuk individu dan usaha kecil menengah untuk memahami dan mematuhi undang-undang.

Terakhir, Indonesia, seperti halnya berbagai negara lainnya, tengah menghadapi kondisi sulit yang terjadi akibat pandemi Covid-19. Pemerintah berada dalam tekanan untuk menunjukkan tingkat responsivitas yang lebih baik dalam menghadapi pandemi. Dengan bertambahnya jumlah kasus yang ada, pengadopsian "UU Cipta Kerja" yang kontroversial telah mengambil perhatian akibat aksi demonstrasi besar-besaran yang dilakukan oleh mahasiswa dan aktivis untuk penghapusan UU tersebut. Dalam banyaknya isu yang dihadapi negara, perlindungan data pribadi dianggap kurang penting. Walaupun diskusi-diskusi mengenai RUU PDP oleh DPR dan pemerintah masih terus berjalan, pengadopsian dalam waktu dekat dianggap sulit. Walaupun terdapat insiden besar kebocoran data yang melibatkan perusahaan-perusahaan e-commerce dan institusi pemerintah, isu ini sepertinya tidak terlalu mengambil perhatian publik. Sehingga diperlukan upaya oleh pembuat kebijakan untuk menarik perhatian publik terhadap isu ini.

Membandingkan Tata Kelola Data – India dan Indonesia

Setelah membahas regulasi perlindungan data di India dan Indonesia pada bab-bab sebelumnya, bagian ini menguraikan hasil analisi komparatif kedua negara.

Peningkatan Penetrasi Internet

Penggunaan internet saat ini meningkat di kedua negara. Semakin banyak penduduk yang berada di ranah daring dan menggunakan internet untuk mengelola hidup dan kehidupan mereka. Seperti halnya masyarakat di negara maju, masyarakat India dan Indonesia lebih sering menggunakan internet lewat gawai, hingga kemudian memberikan ruang bagi perusahaan teknologi domestic dan asing untuk menciptakan aplikasi-aplikasi yang melayani kebutuhan dan keinginan pasar yang spesifik. Pada tahun 2018, hampir 65% masyarakat Indonesia, atau lebih kurang 172 juta orang, berada dalam ranah daring. Diantara 65% tersebut, hampir 95% menggunakan media sosial. Angka tersebut juga sama tingginya di India dan terus meningkat setiap tahunnya. Pada tahun 2014, terdapat 239 juta pengguna internet di India; angka ini kemudian meningkat drastis ke 560 juta pada tahun 2018.

Ekonomi Digital yang Makmur

Kedua negara memiliki ekonomi digital yang makmur. Berbagai perusahaan menciptakan beragam aplikasi serta layanan yang digunakan oleh masyarakat di negara masing-masing untuk melakukan komunikasi, transaksi, dan terlibat dalam kegiatan e-commerce. Aktivitas ekonomi di berbagai ranah seperti kesehatan, hiburan, dan perdagangan eceran yang membutuhkan dan menggunakan informasi serta pengetahuan digital sebagai faktor produksi juga mengalami peningkatan. Pada tahun 2015, ekonomi digital Indonesia bernilai 8 miliar USD, dan hanya dalam 5 tahun, ekonomi tersebut meningkat 5 kali lipat hingga 40 miliar USD pada tahun 2019. Diperkirakan bahwa valuasi ini akan naik ke 150 miliar USD pada tahun 2025. Ekonomi digital di India yang terdiri dari sektor-sektor seperti IT, elektronik, dan manufaktur, berkontribusi setidaknya 7% ke PDB India pada tahun 2018 atau sebesar 200 miliar USD. Pada tahun 2025, nilai ekonomi digital India diestimasi mencapai 435 miliar USD atau 2 kali lipat dari angka yang sekarang.

Tata Kelola Data Sektoral

Kedua negara sedang dalam proses mengadopsi legislasi menyeluruh untuk meregulasi data. Di Indonesia, ketidakadaan perundang-undangan dan otoritas regulatoris untuk mengawasi dan menangani isu dan konflik yang berkaitan dengan data menghasilkan peraturan-peraturan sektoral yang melindungi informasi pribadi masyarakat dan pengguna. Data pribadi di Indonesia saat ini dikelola oleh setidaknya 30 regulasi berbeda yang ditetapkan oleh berbagai lembaga pemerintah. Masing-masing sektor memiliki definisi spesifik mengenai data, bagaimana data ditangani, dan oleh siapa. Landskap data yang terpecah-pecah menciptakan suatu kebingungan bagi perusahaan dan masyarakat yang harus mengikuti standar yang berbeda-beda. Namun demikian, perihal data saat ini diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang

didukung oleh dua regulasi—Peraturan Pemerintah No. 71 tahun 2019 tentang Pengadaan Sistem dan Transaksi Elektronik (PP 71) dan Peraturan Menteri Komunikasi dan Informatika No. 20 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Regulasi PDP).

Sedangkan itu di India, Undang-Undang Teknologi Informasi (2000) mengatur berbagai isu di ruang siber seperti kejahatan siber, kanal media sosial, dan lain sebagainya. Undang-undang pengadaan IT juga mencakup persoalan yang menyangkut data, khususnya mengenai perlindungan data pribadi. Pengadaan spesifik yang mencakup informasi atau data pribadi sensitif (SPDI) mengharuskan perusahaan untuk memiliki kebijakan privasi, mengharuskan persetujuan untuk mengumpulkan atau mengirim informasi pribadi, dan memberitahukan darimana data tersebut diambil. Peraturan SPDI juga mengharuskan seluruh entitas di India yang memproses informasi pribadi mewakili individu. Di India, beberapa regulator memilikiperaturan spesifik untuk mengatur bagaimana perusahaan dan organisasi lainnya menangani informasi pribadi yang mereka kumpulkan. Sebagai contoh, Reserve Bank of India memilikiregulasi spesifik yang mempengaruhi data pembayaran. Seluruh data pengguna yang dikumpulkan dalam batas negara India harus dilokalisasi agar RBI dapat mengakses data tersebut. Otoritas telekomunikasi India

(TRAI) memiliki petunjuk mengenai perlindungan data pribadi. Industri dan sektor lainnya diatur oleh UU IT, sama seperti UU ITE Indonesia, yang menetapkan peraturan umum mengenai bagaimana perusahaan harus melindungi informasi pribadi yang dikumpulkan dengan cara yang berbeda-beda. Kurangnya UU IT dan adanya permintaan yang disebabkan oleh tingginya digitalisasi dan volume data yang terkumpul mendorong New Delhi untuk merancang undang-undang baru yang komprehensif untuk memenuhi kekosongan yang ada.

Tekanan untuk Meregulasi Data

Tekanan untuk meregulasi data berasal dari sumber yang berbeda. Di Indonesia, kebutuhan untuk melindungi data masyarakat saat mereka bertransaksi daring berasal dari potensi kebocoran data yang mengkompromi data pribadi, termasuk informasi pribadi yang sensitif. Kesenjangan keamanan mengenai kanal digital telah menyebabkan data diselewengkan atau dikompromi. Perlindungan data tergabung ke kekhawatiran terhadap isu keamanan siber yang terus meningkat. Walaupun permasalahan mengenai kejahatan siber dianggap relevan di India, mereka tidak muncul dalam diskusi-diskusi mengenai data. Tekanan untuk melindungi informasi pribadi masyarakat India berasal dari diskusi konstitusional yang berhubungan dengan privasi yang dianggap sebagai hak dibawah konstitusi India pada tahun 2017. Aadhaar, database biometrik India, telah meningkatkan kepekaan masyarakat India terhadap pentingnya informasi pribadi yang dapat digunakan untuk kepentingan publik dan swasta.

Mendefinisikan Data

Bagaimana undang-undang yang diajukan mendefinisikan data di kedua negara mengungkapkan bagaimana pembuat kebijakan mengonseptualisasikan data dan cara mengaturnya. Rencana undang-undang di Indonesia mengklasifikasikan data pribadi baik sebagai

data umum atau data khusus. Data umum terdiri dari informasi pribadi seperti nama, gender, agama, dan nasionalitas yang mengidentifikasi seorang individu. Sementara itu, data khusus mencakup informasi yang sekiranya sensitif seperti orientasi seksual, kondisi kesehatan, preferensi politik, rekam jejak keuangan, dan lain sebagainya. RUU PDP membagi data menjadi tiga kategori: data pribadi atau informasi yang dapat mengidentifikasi individu; data khusus, termasuk informasi sensitif seperti data yang berkenaan dengan data, biometrik, genetika, orientasi seksual, preferensi politik, rekam jejak kriminal, data anak-anak, data keuangan, dan lain-lain. RUU ini tidak secara eksplisit mendefinisikan data sensitif walaupun tetap dianggap penting dan memerlukan perlindungan lebih dibanding data pribadi yang lebih "umum".

Ada beberapa kategori data di India. Pertama adalah data pribadi atau informasi yang terkait dengan individu yang dapat digunakan untuk mengidentifikasi mereka. Data pribadi sensitif mengacu kepada informasi sensitif seperti data keuangan, data kesehatan, orientasi seksual, data genetik, data biometrik, keyakinan agama, kasta atau suku, dan lain-lain. Syarat dari *data mirroring* yang terdapat pada versi RUU pertama mengharuskan salinan dari sebuah data untuk disimpan di India. Namun hal tersebut lebih dilonggarkan dalam revisi RUU setelahnya. Saat ini hanya terdapat beberapa jenis data tertentu yang harus disimpan di dalam India. Data pribadi dapat ditransfer keluar dari India, akan tetapi, data pribadi yang bersifat "sensitif" harus disimpan di India. Serta diberikan izin untuk pembuatan salinan dari data tersebut jika syarat-syarat tertentu telah terpenuhi. Data pribadi penting harus disimpan di India tanpa pengecualian dan tidak dapat ditransfer keluar kecuali jika diizinkan oleh pemerintah.

Persetujuan (*Consent*)

Kedua RUU di India dan Indonesia mengacu dan mementingkan pada aspek persetujuan (*consent*). Ketentuan mengenai persetujuan dalam rancangan undang-

undang India mirip dengan ketentuan persetujuan dalam GDPR UE. Entitas yang mengumpulkan data di India (*data fiduciaries)* harus mendapatkan persetujuan dari individu atau yang memberikan informasi pribadi mereka (*data principals).* RUU terkait data juga mengamanatkan para *data fiduciaries* untuk mendapatkan persetujuan orang tua sebelum mengumpulkan data anak. Akan tetapi, RUU tersebut juga memiliki beberapa pengecualian yang membebaskan para *fiduciaries* dari pengumpulan data jika ada situasi menuntut yang berhubungan dengan keamanan nasional maupun penegakan hukum. Demikian pula, RUU Indonesia juga mengedepankan aspek persetujuan sebagai dasar penanganan data pribadi, kecuali jika ditentukan oleh peraturan lain. Persetujuan untuk mengumpulkan, memproses, menyimpan, menerbitkan, dan memusnahkan data pribadi harus diperoleh dalam Bahasa Indonesia. Di bawah RUU, organisasi-organisasi harus menerima persetujuan secara eksplisit untuk mengumpulkan data pribadi seperti nama, jenis kelamin, kebangsaan, agama, catatan medis, biometrik, dan orientasi seksual.

GDPR

GDPR telah mempengaruhi rancangan undang-undang data baik di India maupun Indonesia. Karena tidak ada kerangka aturan global yang mengatur data, peraturan perlindungan data Uni Eropa lah yang menjadi gambaran bagi New Delhi dan Jakarta untuk melegislasi perlindungan data. Dalam rancangan undang-undang Indonesia, pengguna diharapkan memberikan data pribadi kepada pengendali data (*data controller*) dan pengelola

data (*data processors*) yang akan memproses data atas nama para pengendali; proses ini menyerupai aturan GDPR. RUU Indonesia juga menggunakan gagasan privasi yang merupakan inti GDPR dan terkait dengan konstitusi Indonesia. Gagasan ini mencoba menyeimbangkan hak-hak sipil terkait informasi pribadi dengan cara menyediakan kondisi yang mendukung terjadinya inovasi ekonomi digital. India juga mengandalkan GDPR untuk menetapkan kerangka kerja yang bisa diikuti oleh perusahaan-perusahaan digital untuk mengumpulkan data individu di dalam platform mereka. Aspek lain dari GDPR yang digunakan India mencakup aturan untuk pemberitahuan dan persetujuan sebelum mengumpulkan dan menggunakan data, ketentuan untuk memproses data, dan batasan-batasan tertentu untuk memastikan bahwa data yang dikumpulkan terbatas pada layanan tertentu.

Kedaulatan Data (*Data Sovereignty*)

Meskipun terdapat keinginan besar untuk menasionalisasi data dan membuka nilai ekonominya, India dan Indonesia sama-sama mengalami kesulitan dalam penetapan tujuan ini. Namun, hal tersebut terjadi bukan tanpa alasan. Kedaulatan data atau aturan yang menganjurkan penyimpanan data nasional cenderung diprioritaskan di India. Pada versi pertama RUU India, terdapat peraturan yang mengharuskan lokalisasi data atau penyimpanan salinan dari semua data di dalam India. Namun, keinginan ini kemudian direduksi dalam versi kedua dari RUU tersebut. Dampaknya, hal ini memberikan kelonggaran persyaratan yang mengatur transfer dan pembagian data pribadi yang tidak dianggap sensitif. Niat untuk menasionalisasi data seolah-olah digagalkan oleh perusahaan teknologi asing dan pemerintah yang menentang lokalisasi. Pemerintah Indonesia juga memprioritaskan kedaulatan data tetapi peraturan STE 71 tidak mencerminkan dorongan ini. Sebagaimana memungkinkan data disimpan, diproses, dan dikelola di luar negeri selama data tersebut masih dapat diakses. Kedua negara tampaknya telah memilih aksesibilitas daripada kontrol penuh.

Regulator Data

Salah satu aspek penting dari kedua RUU tersebut adalah kewenangan kelembagaan yang akan bertugas untuk mengatur data. Undang-undang India menyerukan pembentukan *Data Protection Authority* (DPA) untuk mengawasi dan menegakkan ketentuan RUU, termasuk bagaimana data dibagikan lintas batas. Mandat DPA melingkupi berbagai fungsi dan persyaratan serta entitas yang dicakup, baik pemerintah maupun non-pemerintah. Sehingga muncul pertanyaan apakah DPA akan memiliki kapasitas cukup dalam menjalankan fungsinya. Sebagaimana kegagalan dapat menyebabkan kurangnya regulasi atau lintas regulasi, terutama oleh lembaga seperti RBI yang menangani data pribadi sekarang. Selain itu, RUU tersebut juga memberikan kekuasaan yang cukup besar kepada pejabat pemerintahan yang akan menangani dan mengawasi otoritas. Hal ini menimbulkan keraguan tentang apakah pemerintah akan tunduk pada aturan RUU tersebut. Sebaliknya, RUU Indonesia tidak memiliki badan indepeden yang akan mengawasi dan menegakkan aturan. Kondisi ini berpotensi membahayakan kepatuhan terhadap RUU tersebut. Kemenkominfo akan berfungsi sebagai pengawas, pengontrol, dan pengolah data. Sejauh ini, Kemenkominfo telah menolak seruan untuk membentuk badan regulator data independen dengan alasan pertimbangan efisiensi sekaligus mengakui keterbukaan mereka untuk mendirikan sebuah lembaga yang melaksanakan rancangan undang-undang tersebut setelah disahkan.

Kekhawatiran Perihal Aspek Institusional

Baik India maupun Indonesia memiliki tantangan yang kelak harus diahadapi bila RUU akhirnya diresmikan. Salah satu tantangan yang muncul adalah terkait kepatuhan dan penegakan undang-undang. Peraturan baru ini menuntut adanya regulator baru untuk mengelola dan mengawasi isu-isu maupun masalah yang

berada di bawah pengiriman data. Akibatnya, akan ada jeda dalam proses transisi dari peraturan sektoral yang sudah ada terhadap undang-undang baru. Jeda ini akan menimbulkan pertanyaan tentang seberapa cepat regulator baru tersebut dapat secara efektif melaksanakan tanggung jawab khusus dan menegakkan peraturan yang ada. Kekhawatiran lain yang muncul adalah independen dari regulator data di masa depan, apakah regulator data akan dapat melakukan penilaian, dengan mempertimbangkan kepentingan pemerintah dan aktor lain, terutama sektor swasta. Dengan kata lain, apakah pemerintah akan patuh dengan peraturan data baru atau akan mengecualikan diri sendiri? Serta, kekuatan penegakan macam apa yang akan dimiliki badan-badan baru atas entitas yang melanggar aturan yang mengatur pengumpulan dan pembagian atas data?

Selain kekhawatiran yang telah disebutkan, ada juga pertanyaan mengenai koordinasi terhadap isu data – akankah perusahaan dan organisasi lain memiliki staf yang diperlukan untuk mengolah pertanyaan terkait data, khususnya terkait kepatuhan? Di India, *data fiduciaries* atau firma dan organisasi yang mengumpulkan data harus menunjuk *data protection officers* (DPO), mendaftar ke otoritas terkait, melakukan penilaian dampak perlindungan data, dan menyerahkan fungsi pemrosesan data mereka untuk audit tahunan. Rancangan undang-undang data Indonesia juga mengamanatkan organisasi untuk menunjuk DPO untuk mengawasi dan mengelola aturan data baru di dalam organisasi. Masih dipertanyakan apakah tujuan ini akan terwujud, mengingat kembali tingkat kesadaran digital masyarakat umum Indonesia yang masih sangat rendah. Kedua negara harus mengelola dan mengatasi tantangan-tantangan institusional setelah rancangan undang-undang mereka disahkan.

Perbandingan Data Governance India-Indonesia

Aspek	India	Indonesia
Latar Belakang	India memiliki salah satu ekonomi digital dengan pertumbuhan tercepat di dunia. Aadhaar, program identitas biometrik digital unggulan dari 1.2 miliar warga India, telah mendukung ekonomi digital India. Salah satu program pemerintah India yang memanfaatkan Aadhaar adalah program Jan Dhan. Pemerintah India melanjutkan dorongan digital melalui investasi publik, inisiatif pemerintah, dan kebijakan pendukung. Industri telekomunikasi mendorong digitalisasi secara cepat dengan memangkas biaya peralatan digital yang mengelola aktivitas harian, paket data, dan biaya langganan internet. Pengguna data seluler India telah melonjak pesat dalam beberapa tahun terakhir karena penurunan harga paket data. Digitalisasi yang cepat ini telah memaksa pengguna internet India untuk mengungkapkan keprihatinan mereka atas privasi online (sumber: laporan UNCTAD) dan mendesak pemerintah untuk mengadopsi peraturan perlindungan data.	Empat masalah menjadi pendorong utama dalam penerapan peraturan perlindungan data di Indonesia Pertama, masih **rendahnya kesadaran dan pengetahuan masyarakat tentang privasi data**, meskipun jumlah pengguna internet di Indonesia cukup besar. Kedua, **kurangnya regulasi perlindungan data menghambat pertumbuhan ekonomi digital Indonesia**. Masalah lain muncul dari **ancaman kebocoran data** yang sudah pernah terjadi di beberapa sektor, seperti bidang ekonomi, medis, dan sosio-politik. Hal ini menunjukkan kelemahan dari ekosistem digital Indonesia, yang disebabkan oleh kurangnya regulasi menyeluruh yang secara hukum dapat menjatuhkan hukuman atas pelanggaran tersebut. Terakhir adalah **tekanan politik terhadap penyusunan Undang-Undang Perlindungan Data Pribadi**. Banyaknya pemangku kepentingan yang mendesak pengesahan RUU PDP menyebabkan tekanan terhadap pemerintah Indonesia untuk segera mengadopsi peraturan tentang perlindungan data.

Aspek	India	Indonesia
Regulasi Pemerintah yang Mengatur Perlindungan Data	India tidak memiliki undang-undang terkait dengan data. Namun ada sebuah kerangka kasar dalam ***IT Act* (2000) di bawah *Section 43A* tentang praktik keamanan dan prosedur penanganan data**. Situasi ini kemudian diperbaiki dengan penambahan ***Reasonable Security Practices and Procedures Rules* (RSPP)** yang bertujuan untuk melindungi data sensitif. Sebuah keputusan Mahkamah Agung India yang bersejarah kemudian menjadi katalisator dari penyusunan rancangan undang-undang perlindungan data oleh pemerintah India. Pada tahun 2018 diperkenalkan ***Personal Data Protection Bill 2018*** sebagai kerangka kerja komprehensif India mengenai perlindungan data pribadi. Versi terbaru RUU yang dikeluarkan pada tahun 2019 **(*Personal Data Protection Bill 2019*)** tersebut menjadi sasaran kritik ketika diperkenalkan di Lok Sabha. Revisi tersebut dianggap memberikan kekuatan dan kontrol kepada pemerintah atas data warga sipil tanpa adanya sistem *check and balance* yang tepat.	Seperti halnya India, saat ini Indonesia masih tidak memiliki undang-undang khusus dalam *data governance*. Dalam konteks Indonesia, **perlindungan data memiliki pendekatan sektoral sebagaimana tidak adanya peraturan yang mengatur secara menyeluruh**. Laporan tersebut menjelaskan pendekatan sektoral untuk perlindungan data di berbagai sektor pemerintah: telekomunikasi dan informatika, perdagangan, perbankan dan jasa keuangan, pelayanan kesehatan, dan pelayanan sipil. Setiap sektor memiliki fokus khusus pada perlindungan data dan mengelolanya melalui peraturan khusus dari masing-masing sektor. Pendekatan ini akhirnya membuat regulasi perlindungan data di Indonesia masih belum harmonis dan berbasis sektoral. Tentu saja, celah-celah di setiap regulasi sektor juga memperparah hal tersebut. Pada tahun 2019, pemerintahan Indonesia menyusun **Rancangan Undang-Undang Perlindungan Data Pribadi** sebagai kerangka dari regulasi perlindungan data Indonesia. Namun, sayang sekali pengesahan dari RUU PDP ini mengalami oleh DPR karena tidak diprioritaskan.

Aspek	India	Indonesia
Regulator Data	Dalam *Personal Data Protection Bill 2018*, badan pengatur dengan kapasitas pembuatan aturan dan ajudikasi dalam *data governance* adalah ***Data Protection Authority* (DPA)**. Pada RUU 2019, DPA tetap memiliki kekuatan namun didominasi keterlibatan pemerintah. Kritik terhadap DPA versi 2019 adalah tidak adanya anggota independen di lembaga pemerintahan. Hal tersebut dinilai akan mengurangi independensi DPA dalam penegakan peraturan perlindungan data.	Dalam RUU PDP, salah satu isu yang menjadi perdebatan panas adalah **tidak adanya badan independen yang bertanggung jawab atas penegakan dan pengawasan**. Ketentuan ini dikritik keras karena dapat menimbulkan ketidakpercayaan warga terhadap penegakan hukum dan potensi konflik kepentingan bagi pemerintah. Ketiadaan badan independen itu dijustifikasi oleh pemerintah sebagai upaya peningkatan efisiensi birokrasi. Ada juga perdebatan yang sedang berlangsung di DPR tentang pembentukan badan independen. **Namun, perlu dicatat bahwa keputusan ini belum final dan pemerintah masih terbuka untuk membentuk badan independen**.
Aktor *Data Governance*	1. ***Data principals*: masyarakat dan konsumen yang menyediakan data pribadi ke operator.** 2. ***Data fiduciaries*: Pemerintah, lembaga swasta, dan organisasi yang memproses dan mengatur data pribadi**	1. ***Data Regulator*: badan pemerintahan yang mengatur aktivitas terkait dengan penggunaan data pribadi. Dibagi menjadi dua cabang, cabang eksekutif (co: Kemenkominfo dan Kemendagri) dan cabang legislatif.** 2. ***Electronic System Manager*: organisasi apapun yang menggunakan data pribadi penggunanya untuk layanan organisasi (co: perusahaan media sosial).** 3. ***Civil Society*: entitas masyarakat sipil (co: LSM dan akademisi) yang mengadvokasi *data governance* di Indonesia.**

Aspek	India	Indonesia
Kategorisasi Data	Di dalam *Personal Data Protection Bill 2019*, data dikategorisasi menjadi ***personal data, non-personal data, sensitive personal data,*** **dan *critical personal data*.** 1. ***Personal Data*: setiap informasi yang berkaitan dengan seseorangan yang secara langsung atau tidak langsung mampu untuk mengidentifikasi orang tersebut.** 2. ***Non-personal Data*: data anonim.** 3. ***Sensitive Personal Data*: termasuk data keuangan, data kesehatan, orientasi seksual, informasi biometrik, data genetik, status interseks, kasta atau suku, dan keyakinan agama dan politik.**	Di dalam RUU PDP, data pribadi dibagi menjadi dua kategori, **data pribadi umum dan data pribadi spesifik**. 1. **Data Pribadi Umum: data pribadi seperti nama lengkap, gender, kewarganegaraan, dan agama, yang mampu untuk mengidentifikasi seseorang.** 2. **Data Pribadi spesifik: mencakupi data yang terkait dengan informasi kesehatan,data biometrik, data genetika, orientasi seksual, data keuangan, dan data lainnya sesuai peraturan perundang-undangan lain.** Perlu dicatat bahwa RUU tersebut tidak secara eksplisit mendefinisikan data sensitif, meskipun sangat penting untuk menjaganya.

Aspek	India	Indonesia
Perjalanan Menuju Pengesahan Undang-undang Data	Pesatnya digitalisasi masyarakat India meningkatkan kekhawatiran publik atas informasi dan data pribadi secara signifikan. Kesadaran bahwa informasi pribadi yang dikumpulkan dapat mengakibatkan hilangnya privasi memaksa pemerintah untuk memberlakukan undang-undang perlindungan data pribadi. Perusahaan India saat ini memikirkan kembali peran mereka dalam mengelola data pribadi dan mendesak pemerintah untuk membuat peraturan perlindungan data pribadi yang dapat membantu operasi bisnis dan produk mereka. Oleh karena itu, dengan alasan yang telah disebutkan memaksa pemerintah India untuk menyusun *Personal Data Protection Bill 2018*.	Tidak adanya undang-undang khusus mengenai perlindungan data pribadi telah merugikan masyarakat Indonesia yang makin berkembang secara digital. Sebagai salah satu negara dengan populasi pengguna internet terbesar secara global, cukup mengejutkan untuk mengetahui bahwa banyak orang Indonesia tidak dibekali dengan pengetahuan yang memadai tentang privasi data. Maka dari itu, keberadaan undang-undang perlindungan data pribadi akan mengurangi resiko terkait kurangnya pengetahuan ini. Seperti halnya India, Indonesia juga terdesak oleh sektor ekonomi digital yang sedang berkembang di negara tersebut - yang saat ini dirugikan oleh tidak adanya regulasi PDP. Tekanan dari aktor-aktor kunci seperti pengelola sistem elektronik dan masyarakat sipil juga mendorong respons pemerintah dalam membuat RUU PDP pada 2019.
Kekhawatiran dalam Implementasi UU	*Personal Data Protection Bill 2019* telah mendapat kritik atas beberapa ketentuannya. Salah satu perhatian dari kritik ini adalah mengenai persetujuan karena dianggap telah mengadopsi sistem "*blanket consent*". Sistem tersebut menjadi penghambat transparansi penanganan data. *Personal Data Protection Bill 2019* juga dikritik atas peningkatan kewenangan pemerintah dalam mengelola data pribadi yang ditunjukkan dengan pengurangan kekuasaan dan independensi DPA.	Tantangan utama dalam RUU PDP adalah untuk bisa memastikan kepatuhan dan penegakan di Indonesia. Namun, draf RUU PDP saat ini masih memiliki beberapa kelemahan nantinya saat disahkan. Pertama, waktu yang diberikan pada pengolah dan pengontrol data untuk menghentikan dan memberikan akses data pribadi terbilang cukup singkat. Kedua, perlu adanya pedoman teknis untuk industri dan sektor lain setelah undang-undang ini disahkan demi mengurangi ambiguitas. Terakhir, tidak adanya badan independen yang menimbulkan pertanyaan mengenai kepercayaan pemerintah dalam mengawasi dan menegakkan undang-undang perlindungan data.

Kesimpulan

Berdasarkan kajian yang telah dilakukan, disimpulkan bahwa baik India maupun Indonesia belum memiliki undang-undang yang mengatur *data governance* secara komprehensif. Kedua negara sedang dalam proses mengadopsi peraturan perlindungan data pribadi yang menyeluruh dan keduanya memiliki kekhawatiran mengenai penerapan peraturan tersebut. Namun, ada juga perbedaan dalam bagaimana India dan Indonesia berkembang menuju regulasi baru tersebut. Misalnya, ada tingkat urgensi yang berbeda di antara regulator di kedua negara. Rancangan undang-undang India mencakup ketentuan untuk pembentukan badan independen untuk mengawasi perlindungan data, sedangkan pada rancangan Indonesia tidak. Bagian ini diakhiri dengan ringkasan tantangan dan peluang utama India dan Indonesia dalam menerapkan peraturan perlindungan data pribadi yang kuat.

Tantangan Utama

India

Tantangan-tantangan utama India cenderung bersifat sosio-politik. Tingkat digitalisasi tidak merata di seluruh perusahaan dari berbagai sektor. Perusahaan TIK, layanan profesional, dan perawatan kesehatan terwakili di kuartil terbawah dari adopsi digital, sementara perusahaan transportasi dan konstruksi berada di kuartil teratas. Penggunaan internet data secara besar-besaran telah mendorong sejumlah besar (90%) pengguna internet India untuk mengungkapkan keprihatinan mereka mengenai privasi online. Ada kesadaran yang terus berkembang bahwa proses pengumpulan data dapat menyebabkan depersonalisasi dan dapat mengakibatkan hilangnya privasi seseorang secara signifikan. Sebelum penerbitan RUU yang diprakarsai oleh Komite Srikrishna, pihak swasta memandang bahwa data yang dikumpulkan adalah milik mereka, bukan milik pengguna. Selain itu, terdapat tantangan ketika memastikan apakah pemerintah pusat akan dibebaskan dari undang-undang data baru. Perkiraan ini menimbulkan pertanyaan mengenai norma baru yang terkait dengan privasi.

Indonesia

Di Indonesia, peraturan perlindungan data yang ada bersifat sangat sektoral. Berbagai sektor pemerintah memiliki persepsi dan lingkup perlindungan data masing-masing. Perlindungan data pribadi diatur oleh setidaknya 30 peraturan yang dikeluarkan oleh berbagai badan dan kementerian pemerintah yang mencakup telekomunikasi dan informatika, kesehatan, perdagangan, administrasi sipil, serta perbankan dan jasa keuangan. Pendekatan ini mengarah pada peraturan perlindungan data yang terfragmentasi dan berorientasi pada sektor karena tidak ada kebijakan menyeluruh terkait data pribadi. Kurangnya regulasi yang komprehensif mengakibatkan perbedaan perspektif tentang

data mana yang harus dilindungi dan diklasifikasikan sebagai “data sensitif”.

Selain itu, tantangan Indonesia terletak pada masyarakatnya. Banyak pengguna internet yang kurang memiliki kesadaran dan pengetahuan mengenai privasi data. Tanpa mereka ketahui, data mereka sedang dikumpulkan dan diproses. Tidak lagi menjadi hal yang aneh ketika kita menemukan pengguna internet Indonesia yang mengunggah informasi sensitif tentang diri mereka atau keluarga mereka oleh diri mereka sendiri. Akibatnya terjadi kasus pembobolan data, baik di platform milik swasta maupun pemerintah. Ketidak-mampuan pemerintah untuk secara efektif melakukan penegakan hukum terhadap pelanggaran data dapat menjadi tantangan untuk melindungi data masyarakat.

Perdebatan sengit tentang pembentukan badan per-lindungan data, klasifikasi data, dan berbagi data den-gan sektor swasta sedang berlangsung. Saat ini, masih belum ada badan perlindungan data yang mengatur dan mengawasi perlindungan data di Indonesia. Kebutuhan untuk membentuk lembaga perlindungan data belum dibahas dalam RUU PDP saat ini karena tidak ada mandat untuk membentuk lembaga tersebut dalam RUU tersebut. Hal ini menjadi perdebatan antara banyak pihak. Kemenkominfo berencana untuk mem-bentuk badan perlindungan data di bawah strukturnya tetapi pemerintah terbagi antara menyetujui rencana Kemenkominfo atau memisahkan badan tersebut. Draf saat ini mengidentifikasi data "umum" dan "spesifik" dalam hal klasifikasi data. Akan tetapi data "sensitif" tidak didefinisikan secara eksplisit meskipun penting. Kesenjangan ini dapat menyebabkan salah tafsir di masa depan.

Isu lain dari draf saat ini termasuk periode waktu pendek bagi pemroses data dan pengontrol data untuk dihentikan dan memberikan akses ke data pribadi dan kebutuhan pedoman teknis bagi industri setelah RUU PDP disahkan. Pada akhirnya, Indonesia masih harus meningkatkan kemampuan para pemangku kepentin-gan terkait untuk menerapkan kebijakan yang kuat.

Peluang Utama

India

Meskipun India menempati urutan terakhir dari 17 ekonomi maju utama dalam hal adopsi digital, dorongan menuju digitalisasi berkelanjutan telah diciptakan oleh program Aadhaar. Sejauh ini, India adalah satu-satunya negara berkembang berpenduduk besar yang telah memberikan sistem identitas digital berbasis biometrik kepada sebagian besar warga dewasanya. Dengan identifikasi yang aman dan terverifikasi, warga negara India dapat melakukan transaksi tanpa memerlukan dokumen tambahan, sehingga memotong jalur birokrasi. Program ini telah merangsang ekonomi digital india yang memicu diskusi tentang privasi. Tidak hanya itu, pemerintah India di bawah Perdana Menteri Modi telah memprakarsai beberapa inisiatif kebijakan seperti *Jan Dhan Programme*. Program tersebut mendorong akses keuangan bagi mereka yang tidak memiliki rekening bank. Selebihnya juga ada inisiatif Digital India yang akan mempromosikan infrastruktur digital yang kuat, layanan digital, dan literasi digital bagi warga negara India. Inisiatif semacam ini akan mendorong tuntutan untuk *data governance* yang kuat di masa depan.

Pembentukan dari Komite Srikrishna juga memberikan peluang untuk *data governance* India. Terlepas dari kekhawatiran atas perumusan rancangan undang-undang dan beberapa ketentuannya, adanya perkembangan *ICT Law*, *Personal Data Protection Bill 2018 & 2019* telah menunjukkan bahwa India secara bertahap bergerak menuju sebuah undang-undang perlindungan data pribadi yang komprehensif.

Indonesia

Peluang utama Indonesia kurang lebih sama seperti peluang India. Untuk Indonesia, keluarnya Strategi Nasional *Artificial Intelligence* (AI) baru-baru ini (pertengahan 2020) menunjukkan komitmen Indonesia untuk mengembangkan AI-nya untuk tata kelola digital. Salah

satu bab dalam Strategi Nasional tersebut menekankan pentingnya sertifikasi bagi talenta Indonesia. Strategi ini diharapkan dapat menekankan standar yang sudah ada sebelumnya, baik internasional maupun nasional. Tujuan sertifikasi adalah untuk mempersempit kesenjangan antara *supply* (tenaga kerja) dan *demand* industri (pasar tenaga kerja). Terlepas dari kurangnya diskusi tingkat nasional saat ini dan popularitas yang rendah di antara anggota pemerintahan, Strategi AI Nasional mungkin untuk mendorong pemangku kepentingan untuk menyelesaikan RUU PDP sesegera mungkin untuk mengikuti teknologi yang berkembang cepat dan penggunaan data yang semakin masif.

Selain strategi baru, berbagai program digital telah diluncurkan oleh Kemenkominfo Indonesia. Pertumbuhan ekonomi digital yang pesat ditambah dengan banyaknya platform *e-commerce* yang bermunculan di pasar Indonesia menjadi alasan pemerintah ingin terlibat dalam peningkatan kesadaran digital, literasi digital, dan keterampilan digital. Manifestasi dari ambisi ini disampaikan melalui program pelatihan komprehensif kementerian.

Faktor sosial juga mempengaruhi motivasi untuk menyediakan *data governance* yang kuat di Indonesia. Akibat beberapa kejadian beberapa tahun terakhir—seperti pelanggaran data terkait platform *e-commerce* terkemuka di Indonesia—pemerintah berada di bawah tekanan politik untuk menangani masalah ini. Perubahan tingkat komitmen untuk menyediakan regulasi data yang lebih baik juga dipengaruhi oleh LSM Indonesia yang telah menyatakan keprihatinan atas "lambatnya" kemajuan pemerintah dalam mengadopsi undang-undang PDP.

Pada dasarnya, kesuksesan dari implementasi undang-undang perlindungan data pribadi bagi dua negara berkembang terbesar di dunia masih jauh dari kenyataan. Sejauh manakah India dan Indonesia akan mengadopsi prinsip-prinsip *General Data Protection Regulation* milik Uni Eropa? Apapun hasilnya, seluruh dunia akan terus melihat, sebagaimana suatu saat kedua negara ini akan dijadikan acuan maupun tolak ukur bagi negara berkembang lainnya.

Bibliografi

ABDI, n.d., *About*. Tersedia di https://www.abdi.id/tentang-abdi/. [Diakses pada 30 Juni 2020].

AFPI, n.d., *About*. Tersedia di https://afpi.or.id/en/about. [Diakses pada 30 Juni 2020].

Annur, C. M., 2019, "DPR Kritik Ide Pembentukan Lembaga Perlindungan Data Pribadi", *Katadata*. Tersedia di https://katadata.co.id/berita/2019/07/18/dpr-kritik-ide-pembentukan-lembaga-perlindungan-datapribadi. [Diakses pada 5 Juni 2020].

Annur, C. M., 2019, "Survei APJII: Penetrasi Pengguna Internet di Indonesia Capai 64,8%", *Katadata*. Tersedia di https://katadata.co.id/berita/2019/05/16/surveiapjii-penetrasi-pengguna-internet-di-indonesi-acapai-648. [Diakses pada 26 Juni 2020].

AntaraNews, 2019, "SAFENet harap menkominfo Johnny G Plate selesaikan UU PDP". Tersedia di: https:// www.antaranews.com/berita/1129032/safenetharap-menkominfo-johnny-g-plate-selesai-kan-uupdp. [Diakses pada 3 Juni 2020].

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

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

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

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

Bhandari, Vidya and Renuka Sane, "Protecting Citizens from the State post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna report and the Data protection bill 2018", http://docs.manupatra.in/newsline/articles/Upload/7B08CF55-E27D4A44-A292-3882F08E9053.pdf.

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

Buletin APJII, 2019, "Perlindungan Data Pribadi Mutlak Diperlukan", *APJII*. Tersedia di https://blog.apjii.or.id/index.php/2019/08/20/perlindungan-data-pribadi-mutlak-diperlukan/. [Diakses pada 30 Juni 2020].

Burhan, F. A., 2020, "Asosiasi Bahas UU Fintech hingga Data Pengguna di Istana". *KataData*. Tersedia di https://katadata.co.id/berita/2020/01/24/asosiasibahas-uu-fi ntech-hingga-data-pengguna-di-istana. [Diakses pada 30 Juni 2020].

Burhan, F. A., 2020, "Cegah Pemerintah Salahgunakan Data Pribadi, DPR Minta Lembaga Khusus", *Katadata*. Tersedia di https://katadata.co.id/berita/2020/02/25/cegah-pemerintah-salahgunakandata-pribadi-dpr-minta-lembaga-khusus. [Diakses pada 5 Juni 2020].

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

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

CNN Indonesia, 2019, *BSSN Tanggapi Penyadapan Tanpa UU Perlindungan Data Pribadi*. Tersedia di https://www.cnnindonesia.com/teknologi/20190812183821-185-420671/bssn-tanggapipenyadapan-tanpa-uu-perlindungan-data-pribadi. [Diakses pada 5 Juni 2020].

CNN Indonesia, 2019, *SAFE Net Respons Pidato Jokowi soal Perlindungan Data Pribadi*. Tersedia di https://www.cnnindonesia.com/teknologi/20190816203213-185-422140/safe-net-responspidato-jokowi-soal-perlindungan-data-pribadi. [Diakses pada 5 Juni 2020].

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

CNN Indonesia, 2019, "PP PSTE 'titipan asing' yang gadai kedaulatan data di Indonesia". Tersedia di https://www.cnnindonesia.com/teknologi/20191108152910-185-446726/pp-pste-titipanasing-yang-gadai-kedaulatan-data-indonesia. [Diakses pada 19 Juni 2020].

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

Damarjati, D., 2019, "Kemendagri: 1.227 Lembaga Bisa Akses Data Penduduk, Termasuk Swasta", *DetikNews*. Tersedia di https://news.detik.com/berita/d-4634210/kemendagri-1227-lembaga-bisaakses-data-penduduk-termasuk-swasta. [Diakses pada 5 Juni 2020].

Direktorat Aplikasi dan Informatika, n.d., *Tugas dan Fungsi Direktorat Jenderal Aplikasi dan Informatika*. Tersedia di https://aptika.kominfo.go.id/profi le/tugas-dan-fungsi/#:~:text=Tugas%20Pokok,di%20bidang%20penatakelolaan%20aplikasi%20informatika. [Diakses pada 5 Juni 2020].

Djafar, W., 2019, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan", *ELSAM*. Tersedia di https://referensi.elsam.or.id/2020/03/hukum-perlindungan-data-pribadi-diindonesia/. [Diakses pada 24 Juni 2020].

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

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

ELSAM, 2019, *Penyalahgunaan Data Pribadi Meningkat, Perlu Akselerasi Proses Pembahasan RUU Perlindungan Data Pribadi*. Tersedia di https://elsam.or.id/5806-2/. [Diakses pada 26 Juni 2020].

ELSAM. 2019, "Pentingnya UU Perlindungan Data Pribadi". Tersedia di https://elsam.or.id/pentingnya-uu-perlindungan-data-pribadi/ . [Diakses pada 3 Juni 2020].

Fauzan, R., 2020, "Pelaku Dagang-el Soroti Salah Satu Ketentuan UU Perlindungan Data Pribadi", *Bisnis. com*. Tersedia di https://teknologi.bisnis.com/read/20200304/266/1209168/pelaku-dagang-elsoroti-salah-satu-ketentuan-uu-perlindungan-datapribadi. [Diakses pada 30 Juni 2020].

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

Gatra, 2020, *RUU Data Pribadi Akan Atur Pusat Data hingga Rekaman CCTV*. Tersedia di https://www.gatra.com/detail/news/471976/politik/ruu-datapribadi-akan-atur-pusat-data-hingga-rekaman-cctv-. [Diakses pada 5 Juni 2020].

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

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

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

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

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

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

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

Ihsannudin, 2019, "Menkominfo: Google dan Facebook Berencana Bangun Pusat Data di Indonesia", *Kompas*. Tersedia di https://nasional.kompas.com/read/2019/12/06/09533131/menkominfo-googledan-facebook-berencana-bangun-pusat-data-diindonesia. [Diakses pada 30 Juni 2020].

Indonesian Banking Law No. 10/1998.

Indonesian Health Law No. 36/2009.

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

Indonesian Law No. 23/2006 on Civil Administration.

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

Indonesian Law No. 39/1999 on Human Rights.

Indonesian Law No. 43/2009 on Record Management.

Indonesian Law No.8/1999 on Consumer Protection.

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

Indonesian Trade Law No. 7/2014.

Jakarta Globe, 2020, "Jokowi hopes to unleash digital economy potential". Tersedia di https://jakartaglobe.id/tech/jokowi-hopes-to-unleash-indonesiasdigital-economy-potential/. [Diakses pada 3 Juni 2020].

Jawa Pos, 2019, "ICT Watch desak UU Perlindungan Data Pribadi segera dirampungkan". Tersedia di https://www.jawapos.com/oto-dan-tekno/teknologi/01/08/2019/ict-watch-desak-uu-perlindunganda-ta-pribadi-segera-dirampungkan/. [Diakses pada 3 Juni 2020].

Johny Plate in Reuters, 2019, "Indonesia needs to establish data protection law urgently". Tersedia di https://www.reuters.com/article/us-indonesiacommunications/indonesia-needs-to-urgently-establish-data-protection-law-minister-idUSKBN1XQ0B8. [Diakses pada 3 Juni 2020].

Kamaliah, A., "Kata Asosiasi Soal Data Center Tak Harus di Indonesia", *DetikInet*. Tersedia di https://inet.detik.com/law-and-policy/d-4775013/kata-asosiasisoal-data-center-tak-harus-di-indonesia. [Diakses pada 5 Juni 2020].

Kartika, M., 2019, "BSSN Dukung RUU Perlindungan Data Pribadi Segera Disahkan", *Republika*. Tersedia di https://republika.co.id/berita/q1zhdy428/ bssn-dukung-ruu-perlindungan-data-pribadi-segeradisahkan. [Diakses pada 5 Juni 2020].

Kementerian Dalam Negeri, n.d., *Struktur Organisasi*. Tersedia di https://www.kemendagri.go.id/page/read/7/struktur-organisasi. [Diakses pada 11 Juli 2020].

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

Kominfo, 2018, *Rudiantara Sebut Data Center Tak Perlu di Indonesia*. Tersedia di https://kominfo.go.id/content/detail/14742/rudiantara-sebut-data-center-takperlu-di-indonesia/0/sorotan_media. [Diakses pada 30 Juni 2020].

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

Kumparan, 2020, *Regulasi Tokopedia Larang Pengguna Hapus Akun, Langgar Hak Data Pribadi*. Tersedia di https://kumparan.com/kumparannews/regulasitokopedia-larang-pengguna-hapus-akun-langgarhak-data-pribadi-1tNCp40Q9au. [Diakses pada 5 Juni 2020].

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

McKinsey & Company, 2016, "Unlocking Indonesia's digital economy". Tersedia di https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Diakses pada 3 Juni 2020].

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

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

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

NITI Aayog, “National Strategy for Artificial Intelligence”, Juni 2018, https://niti.gov.in/writereaddata/fi les/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

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

OkeNews, 2018, *Evita Nursanty: Pusat Data dengan Tingkat Confidentiality Tinggi Wajib Berada di Indonesiatara Sebut Data Center Tak Perlu di Indonesia*. Tersedia di https://nasional.okezone.com/read/2018/10/01/337/1958125/evita-nursanty-pusatdata-dengan-tingkat-confi dentiality-tinggi-wajib-berada-di-indonesia. [Diakses pada 30 Juni 2020].

Pertiwi, W. K., 2020, “ELSAM: Harus Ada Pengawas UU PDP di Luar Pemerintah”, *Kompas*. Tersedia di https://tekno.kompas.com/read/2020/01/31/12580067/elsam--harus-ada-pengawas-uu-pdp-di-luarpemerintah?page=all. [Diakses pada 5 Juni 2020].

PTI News, “India’s data consumption may touch 25 GB per month per user by 2025: Ericsson”, *PTI News*, 16 Juni 2020.

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

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

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

Republika, 2019, "PP PSTE Jadi Bentuk Kedaulatan Data". Tersedia di https://nasional.republika.co.id/berita/q1w1pt370/pp-pste-jadi-bentuk-kedaulatan-data. [Diakses pada 19 Juni 2020].

Ristianto, C., 2020, "Kemendagri Diminta Kaji Ulang Kerja Sama Data Kependudukan", *Kompas*. Tersedia di https://nasional.kompas.com/read/2019/08/02/13161321/kemendagri-dimintakaji-ulang-kerja-sama-data-kependudukan. [Diakses pada 5 Juni 2020].

Rizkinaswara L., 2019, "ICT Watch", *Aptika Kominfo*. Tersedia di https://aptika.kominfo.go.id/2019/07/ictwatch/. [Diakses pada 30 Juni 2020].

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

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

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

See Kementerian Komunikasi dan Informatika, n.d., *Struktur Organisasi*. Tersedia di https://aptika.kominfo.go.id/profi l/struktur-organisasi/. [Diakses pada 4 Juni 2020].

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

Setiawan, R., 2020, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", *Tirto*. Tersedia di https://tirto.id/fA5B. [Diakses pada 24 Juni 2020].

Setyowati, D., 2018, "Empat Urgensi UU Perlindungan Data Pribadi di Indonesia", *Katadata*. Tersedia di https://katadata.co.id/berita/2018/04/10/4-urgensiuu-perlindungan-data-pribadi-di-indonesia. [Diakses pada 26 Juni 2020].

Setyowati, D., 2019, "Pelaku Industri Telekomunikasi Minta Pusat Data Wajib Ada di Indonesia", Katadata. Tersedia di https://katadata.co.id/berita/2019/02/06/pelaku-industri-telekomunikasiminta-pusat-data-wajib-ada-di-indonesia. [Diakses pada 5 Juni 2020].

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

Siagian, P., 2017, "Hepatitis Patients Struggle with Discrimination in Workplace", *The Jakarta Post*. Tersedia di https://www.thejakartapost.com/life/2017/11/15/hepatitis-patients-struggle-with-discrimination-inworkplace.html. [Diakses pada 3 Juni 2020].

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

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

Tempo.co, 2020. ”Ministry still Tracing Indonesia’s Covid-19 patients’ data leak”. Tersedia di https://en.tempo.co/read/1356052/ministry-still-tracingindonesias-covid-19-patients-data-leak. [Diakses pada 28 Juni 2020].

Tempo.co, 2019, “Bukalapak confirms of an attempted customer data breach”. Tersedia di https://en.tempo.co/read/1186473/bukalapak-confirmofan-attempted-customer-data-breach. [Diakses pada 3 Juni 2020].

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

The 1945 Constitution of the Republic of Indonesia.

The Jakarta Post, 2020, “Data breach jeopardizes more than 15 million Tokopedia users, report finds”. Tersedia di https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Diakses pada 3 Juni 2020].

The Jakarta Post, 2020, “E-commerce platform Bhineka.com reported to be the latest target of data theft”. Tersedia di https://www.thejakartapost.com/news/2020/05/13/e-commerce-platform-bhinneka-com-reported-to-be-latest-target-of-data-theft.html. [Diakses pada 3 Juni 2020].

Umali, T., 2019, “Indonesia drafts the Personal Data Protection Act. Open Gov Asia”. Tersedia di https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/. [Diakses pada 5 Juni 2020].

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

We Are Social and Hootsuite, 2020, “Digital Indonesia”. Tersedia di https://datareportal.com/reports/digital2020-indonesia. [Diakses pada 3 Juni 2020].

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

Yatim, S., 2019, “The privacy battle in Indonesia- the longer the battle, the more consumers stand to lose”, *The Jakarta Post*. Tersedia di https://www. thejakartapost.com/academia/2019/02/21/theprivacy-battle-in-indonesia-the-longer-the-battlethe-moreonsumers-stand-to-lose.html. [Diakses pada 3 Juni 2020].

Yuniar, R., 2018, “This Week in Asia. Facebook’s Cambridge Analytica scandal puts Indonesia’s tech firms on the spot”. Tersedia di https://www.scmp.com/week-asia/business/article/2143763/facebooks-cambridge-analytica-scandal-puts-indonesias-tech-firms. [Diakses pada 3 Juni 2020].

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

Tentang Penulis

Institute of South Asian Studies, National University of Singapore

Karthik Nachiappan adalah seorang *Research Fellow* pada Institute of South Asian Studies, National University of Singapore dengan *joint appointment* pada NUS South Asian Studies Programme. Penelitiannya saat ini berfokus pada ekonomi politik teknologi di India, khususnya isu-isu seperti regulasi data, keamanan siber, media sosial, dan kecerdasan buatan, serta bagaimana kebijakan mempengaruhi posisi India dalam aturan global yang mencakup masalah teknologi ini.

Ronojoy Sen adalah seorang *Senior Research Fellow* (dan Research Lead, Politics, Society and Governance) di Institute of South Asian Studies dan the South Asian Studies Programme, National University of Singapore. Dia telah bekerja selama lebih dari satu dekade dengan pers koran India terkemuka, terakhir sebagai editor untuk The Times of India. Buku terbarunya adalah *Nation at Play: A History of Sport in India* (Columbia University Press/Penguin, 2015). Ia juga penulis *Articles of Faith: Religion, Secularism, and the Indian Supreme Court* (Oxford University Press, 2010) dan telah menyunting beberapa buku, yang terbaru adalah *Media at Work in China and India* (Sage, 2015). Dia telah berkontribusi pada volume yang disunting dan telah diterbitkan di beberapa jurnal terkemuka. Dia juga menulis secara rutin untuk surat kabar. Dia memiliki gelar Ph.D. dalam ilmu politik dari University of Chicago dan *read history* di Presidency College, Calcutta.

Center for Digital Society (CfDS), Universitas Gadjah Mada

Mulya Amri adalah seorang spesialis dalam kebijakan publik dan anggota panel ahli di Katadata Insight Center, yang berbasis di Jakarta. Dia memimpin beberapa tim peneliti dan analisis data dari awal proyek hingga penyampaian hasil proyek dengan topik terkait ekonomi, bisnis, kebijakan publik, dan digitalisasi. Mulya ikut bersama menulis 20 buku dan bab buku, sebagian besar dengan topik *subnational competitiveness* dan *urban governance*. Dia juga memiliki pengalaman kerja 20 tahun bekerja dengan pejabat pemerintah, bisnis, dan kelompok masyarakat sipil di Indonesia, Singapura, Brunei, Filipina, Cina, dan Amerika Serikat. Mulya memiliki gelar Ph.D. dalam kebijakan publik dari National University of Singapore, gelar Masters dalam *urban planning* dari University of California, Los Angeles, dan gelar sarjana dari Institut Teknologi Bandung, Indonesia.

Diah Angendari adalah seorang dosen pada Departemen Ilmu Komunikasi dan *Executive Secretary* bagi Center for Digital Society, Universitas Gadjah Mada. Penelitiannya berfokus pada topik komunikasi strategis dan penggunaan TIK dalam komunikasi, termasuk literasi digital, dan privasi data.

Anisa Pratita Kirana Mantovani adalah *Manager* dari Divisi Riset pada Center for Digital Society, Universitas Gadjah Mada. Penelitiannya berfokus pada keamanan siber dalam Hubungan Internasional, *digital health*, literasi digital, privasi data, serta kebijakan publik inovatif.

Janitra Haryanto adalah seorang *Project Officer* pada Divisi Riset pada Center for Digital Society, Universitas Gadjah Mada. Dia telah menuliskan lebih dari 20 publikasi tentang topik kebijakan digital dan inovatif, termasuk ekonomi digital, media sosial, dan politik. Dia juga bekerja sebagai konsultan untuk Asia Development Bank (ADB) dalam *youth financial inclusion project*.

Raka Wicaksana sebelumnya pernah terlibat dalam sebuah *international youth leadership NGO* dan industri penelitian yang berfokus kepada isu-isu digital kontemporer. Saat ini dia sedang membantu Direktur Jenderal Aplikasi dan Informatika di bawah Kementerian Komunikasi dan Informatika Republik Indonesia. Minat penelitiannya mencakup perumusan kebijakan digital dan agenda transformasi digital.