CIPS
Center for Indonesian Policy Studies

RINGKASAN KEBIJAKAN

Maret 2021

Ringkasan Kebijakan No. 7

Kerahasiaan Data dalam Peraturan Perundang-Undangan Perlindungan Data Pribadi di Indonesia

oleh Gliddheo Algifariyano Riyadi

Pesan Utama

- Mulai dari pinjaman *online* hingga jenis usaha lainnya, pertumbuhan layanan digital model baru mewajibkan perusahaan untuk mengambil, memproses, dan menyimpan data pribadi. Sementara itu, data-data pribadi tersebut tetap merupakan properti individu dan pemiliknya mempunyai hak untuk mengatur dan mengelola data mereka sendiri.

- Dewan Perwakilan Rakyat (DPR) Republik Indonesia tengah membahas Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang diajukan oleh Kementerian Komunikasi dan Informatika (Kominfo). Di dalam RUU tersebut pemilik data diberikan sejumlah hak untuk mengatur dan mengelola data pribadi mereka sendiri. Hal ini membuat perusahaan bertanggung jawab untuk menunjukkan kepatuhan berkaitan dengan hak individu.

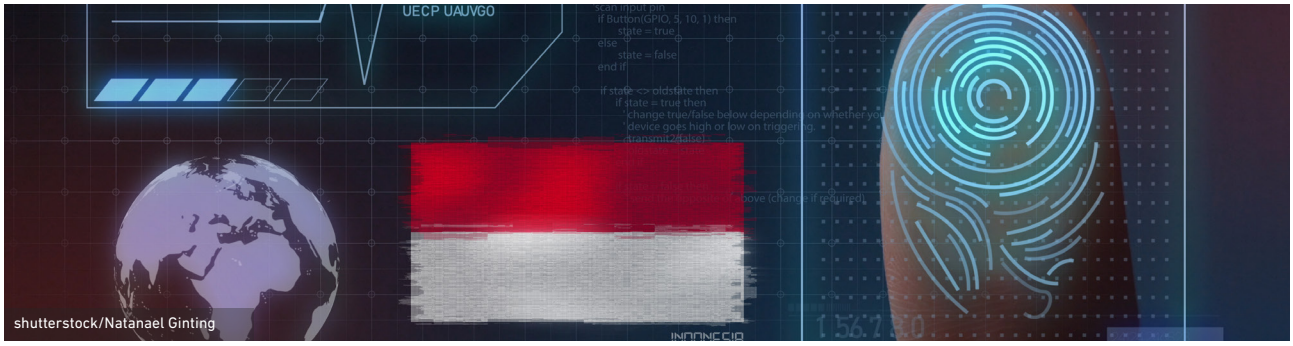
- Akan tetapi, RUU ini memiliki pengecualian terkait hak pemilik data tersebut, yaitu ketika data mereka dibutuhkan untuk masalah pertahanan dan keamanan nasional, penegakkan hukum, administrasi negara, pengawasan sektor keuangan atau moneter, sistem pembayaran, atau stabilitas sistem keuangan. Pengecualian-pengecualian tersebut memberikan pemerintah akses tidak terbatas ke data pribadi. Oleh karena itu, sebaiknya ada definisi dan batasan khusus yang mengatur akses pemerintah tersebut, yaitu yang mewajibkan transparansi tujuan pengecualian dan periode penyimpanan data.

- RUU PDP harus mengikuti pendekatan berbasis risiko. Area-area berisiko tinggi haruslah yang melibatkan aktivitas-aktivitas sistematis dan ekstensif untuk menampilkan profil individu, untuk memproses kategori-kategori khusus dari sebuah data, dan untuk memantau area yang dapat diakses oleh publik. Mereka yang berencana untuk terlibat dalam kegiatan ini harus berkonsultasi dengan otoritas pengawas yang berwenang di Indonesia sebelum melakukan kegiatan tersebut. Mereka perlu melakukan penilaian dampak privasi terperinci dan memberi tahu individu yang berpotensi terkena dampak jika terjadi pembobolan data.

- Wewenang untuk mengawasi kerahasiaan data harus berada di sebuah komisi independen. Akan tetapi, RUU PDP berencana memberikan fungsi pengawasan tersebut ke pihak kementerian di pemerintah, hal ini justru dikhawatirkan berpotensi menyebabkan terjadinya konflik kepentingan.

- Mengingat perusahaan jasa digital perlu terus berinovasi, maka mereka seringkali dihadapkan dengan ketidakpastian apakah mereka melakukan pelanggaran peraturan kerahasiaan data atau tidak. Untuk memitigasi risiko tersebut, pemerintah sebaiknya mempertimbangkan penggunaan ruang uji terbatas (*regulatory sandbox*) untuk memfasilitasi kepatuhan teknologi baru terhadap peraturan privasi data yang ada, dan untuk turut berpartisipasi membuat kebijakan baru seperti yang dilakukan *Personal Data Protection Commission* (PDPC) di Singapura ketika mereka menguji dan mengubah Undang-Undang (UU) PDP Singapura.

Pentingnya Perlindungan Data Pribadi



Ada perbedaan yang sangat mendasar antara keamanan data dan kerahasiaan data. Keamanan data mengacu pada penyimpanan data pribadi dan data sensitif dengan aman agar terhindar dari gangguan, peretas, atau ancaman internal (SNIA, 2019). Sementara itu, kerahasiaan data melibatkan prosedur persetujuan, pemberitahuan khusus, serta kewajiban lain dalam proses pengelolaan data. Kerahasiaan data melindungi hak privasi konsumen individual dan perusahaan (Petter, 2019). Baik perlindungan maupun kerahasiaan data dianggap sebagai bagian dari perlindungan data pribadi.

Kerahasiaan data pribadi adalah sebuah hak subyek data individu. Hal ini mengacu pada tujuan pengumpulan data dan pemrosesan, preferensi kerahasiaan, dan cara lembaga mengelola data pribadi. Peraturan nasional tentang kerahasiaan data biasanya fokus pada bagaimana mengumpulkan, memproses, membagikan, mengarsipkan, dan menghapus data (Ameed & Natgunanathan, 2016).

Mengingat hak ini dimiliki oleh semua orang tanpa terkecuali, kerahasiaan data pribadi memberikan kuasa bagi para individu untuk menentukan penggunaan data pribadi mereka. Pemilik data memiliki hak untuk mengizinkan

pengelola data memproses dan menggunakan data mereka. Namun ketika melakukan itu, pemilik data harus memiliki hak resmi untuk meminta informasi tentang identitas digital mereka sendiri, serta memiliki tujuan meminta dan menggunakan data pribadi mereka tersebut, dan juga informasi tentang lembaga yang meminta data tersebut (Tourkochoriti, 2016). *EU General Data Protection Regulation* (EU GDPR) 2016/679 mengatur bahwa hanya data yang memadai dan relevan yang dapat diproses oleh pengelola data, sementara itu jumlah datanya harus dibatasi sesuai dengan apa yang dibutuhkan untuk tujuan yang telah disetujui oleh pemilik data (Drake, 2016).

Sebagai tolak ukur internasional untuk kerahasiaan data pribadi, EU GDPR mendefinisikan data pribadi dalam Pasal 4 (1) sebagai segala bentuk informasi yang terkait dengan seseorang yang diidentifikasi atau bisa diidentifikasi. EU GDPR mengizinkan identifikasi seseorang tersebut berdasarkan nama, nomor identifikasi, data lokasi, dan identifikasi *online* mereka. Data pribadi juga termasuk informasi yang memberikan identitas fisik, fisiologi, genetik, mental, komersial, budaya atau sosial dari seorang pemilik data. Di antara kategori umum tersebut ada beberapa data pribadi yang sensitif, sehingga data tersebut mendapatkan perlindungan tingkat tinggi dalam EU GDPR Pasal 9, karena nilai pentingnya bagi pemilik data. Data pribadi yang sensitif tersebut di antaranya adalah data genetik, data biometrik dan kesehatan, informasi mengenai asal ras dan etnik, opini politik, kepercayaan religius dan ideologi, serta keterlibatan mereka dalam kegiatan umum (GDPR, 2018).

Kepemilikan data pribadi adalah hal yang krusial dalam era digital. Setiap individu diminta untuk memberikan data pribadi ketika menggunakan layanan *online*, membeli produk *online*, mendaftarkan akun surat elektronik, membuat janji dokter, membayar pajak, menandatangani kontrak, dll. Data-data pribadi tersebut seringkali dikumpulkan tanpa sepengetahuan individu yang bersangkutan dan dilakukan oleh perusahaan atau lembaga yang tidak berinteraksi langsung dengan orang tersebut (Privacy International, 2013). Data mereka dapat digunakan tanpa kuasa pemiliknya untuk menuntut pertanggungjawaban dari pihak yang memproses data mereka dan ketika data pribadi pemilik diproses tanpa persetujuan secara eksplisit sebelumnya. Padahal, persetujuan dalam kegiatan pertukaran data adalah fitur penting kerahasiaan data (Jiska, 2016).

Pertumbuhan eksponensial ekonomi digital di Indonesia memperbesar desakan untuk melindungi kerahasiaan data secara hukum. Pada 2025, ekonomi digital diharapkan bisa berkontribusi sebesar US$ 100 miliar terhadap perekonomian nasional dan menjadi kekuatan ekonomi digital terbesar di ASEAN (Rosadi, 2018).

Pertumbuhan tersebut harus dibarengi dengan perlindungan kerahasiaan data pribadi. Meskipun dianggap bisa meningkatkan kepercayaan pada ekonomi digital (Butarbutar, 2019), hal ini sepertinya tidak memengaruhi perilaku konsumen digital di Indonesia. Sebuah survei oleh Mastel dan APJII pada 2017 menemukan bahwa 79% responden di Indonesia keberatan ketika data pribadi mereka dipindahkan tanpa izin dan 98% mendukung pengesahan UU Perlindungan Data Pribadi (UU PDP). Akan tetapi, pada praktiknya konsumen Indonesia sepertinya tidak terlalu mengkhawatirkan penggunaan data pribadi mereka. Sebuah studi menemukan bahwa pengguna tidak mempelajari atau memahami kebijakan kerahasiaan perusahaan yang jasanya mereka gunakan, termasuk bagian syarat dan kondisi yang berhubungan dengan penggunaan data pribadi mereka (Reynaldi & Tidana, 2020).

Di saat perusahaan-perusahaan Eropa yang beroperasi di Indonesia patuh kepada aturan EU GDPR, karena di dalamnya juga diatur terkait kegiatan perusahaan Eropa di luar wilayah Uni Eropa, banyak perusahaan Indonesia tidak mengatur perlindungan data pribadi dalam kebijakan dan prosedur mereka dengan benar (Reynaldi & Tifana, 2020). Kebanyakan dari mereka juga memiliki pemahaman yang kurang akan konsep kerahasiaan data dan perlindungan data konsumen.

Sementara itu, Indonesia belum memiliki kerangka kerja hukum yang konsisten untuk kerahasiaan data. Peraturan dan kewajiban yang ada saat ini tersebar di setidaknya 32 UU dan regulasi yang berbeda-beda (Aprilianti, 2020). Kesenjangan di antara regulasi-regulasi tersebut mengganggu penegakkan hukumnya (Nugroho, 2020). UU Informasi dan Transaksi Elektronik (ITE) Nomor 19 Tahun 2016 dan UU Administrasi Kependudukan Nomor 24 Tahun 2013 misalnya, memiliki klasifikasi data umum dan data sensitif yang kontradiktif.

Undang-Undang Dasar (UUD) RI melindungi hak warga negaranya akan perlindungan data pribadi atau privasi dalam Pasal 28 G (1). Akan tetapi, jaminan dalam konstitusi tersebut masih harus diregulasi lebih baik dalam UU lebih lanjut (Djafar, Sumigar, & all, 2016). Dewan Perwakilan Rakyat (DPR) RI saat ini tengah membahas RUU Perlindungan Data Pribadi (RUU PDP) agar negara secara efektif bisa melindungi data pribadi warga negara Indonesia, dan juga karena negara lain mewajibkan perlindungan data dalam hubungan dagang mereka dengan Indonesia (Djafar & Wahyudi, 2020).

Kementerian Komunikasi dan Informatika (Kominfo) mulai merancang RUU ini pada tahun 2014 dan mengajukannya ke parlemen pada tahun 2020 (Karunian, 2020). Ada setidaknya empat sesi dialog pada tahun 2020 antara parlemen dan akademisi, Indonesian E-commerce Association (idEA), Asosiasi Fintech Indonesia (AFTECH), Koalisi Advokasi PDP, dan Kominfo (Rizkinaswara, 2020). Dalam rapat dan konsultasi tersebut, pemerintah berupaya untuk mengakomodasi pandangan dari kalangan industri dan pemangku kepentingan yang lain dalam proses penulisan RUU. RUU PDP termasuk dalam Agenda Prolegnas tahun 2020 dan awalnya ditargetkan untuk selesai pada November 2020, namun pada akhir tahun 2020 yang lalu deliberasi belum tercapai dan DPR belum mengesahkannya menjadi UU.

Bagian yang Diperdebatkan dari RUU PDP yang Dirancang oleh Kominfo dan DPR

Beberapa bagian RUU PDP masih diperdebatkan dan akibatnya menghambat pengesahan RUU PDP menjadi UU.

- RUU PDP membuka akses pemerintah ke data pribadi
- RUU PDP memberikan pengecualian di mana persetujuan pemilik data tidak dibutuhkan untuk diakses data pribadinya ketika terkait masalah:
    - pertahanan dan keamanan nasional
    - proses penegakkan hukum
    - pengawasan sektor jasa keuangan
    - stabilitas sistem aturan moneter, pembayaran, dan keuangan
    - kepentingan masyarakat dalam administrasi negara

Pemerintah diwajibkan untuk memberikan alasan yang jelas ketika mau mengakses data pribadi. Dalam hal pertahanan dan keamanan nasional misalnya, harus ada keadaan mendesak sehingga pemerintah harus mengakses data pribadi seseorang. Selain itu, kalau pengadilan memberikan izin, pemerintah juga memiliki hak untuk mengakses data pribadi terkait proses penegakkan hukum.

Akan tetapi, mengizinkan pemerintah untuk mengakses data pribadi masyarakat memiliki risiko penggunaan data untuk tujuan politik atau bahkan ekonomi (Greenleaf, 2017). Hal tersebut mungkin tidak akan terjadi pada masa administrasi pemerintahan yang ada sekarang, namun tetap membuka kesempatan bagi administrasi yang akan datang yang bisa mengambil informasi individu masyarakat tanpa persetujuan pemilik data.

Dalam konteks ini, regulasi baru yang dibuat oleh Badan Pusat Statistik (BPS) tentang Pengelolaan Pengumpulan Data juga penting. Pada awal 2021, rancangan regulasi tersebut mewajibkan perusahaan untuk menyediakan data kepada BPS sebagai badan pemerintah. BPS tidak mengumpulkan data pribadi apapun dan oleh karena itu wewenang BPS untuk mengumpulkan data tidak tercantum dalam pengecualian persetujuan RUU PDP. Akan tetapi regulasi tersebut memberikan BPS wewenang untuk mengumpulkan data, seperti identitas perusahaan (nama, izin, dll.), jumlah pengguna (agregat dan per wilayah), jumlah karyawan, pendapatan, nilai transaksi, dan metode pembayaran. Regulasi BPS tersebut dijadwalkan akan dikeluarkan dan berlaku pada Februari 2021. Penting untuk dipahami bahwa BPS, sebagai pusat data utama pemerintah, hanya memiliki akses ke data umum perusahaan. Kerahasiaan data perlu dilindungi dan BPS harus membatasi diri mengumpulkan data pribadi konsumen perusahaan. Di sisi lain, perusahaan juga harus mempertahankan hak untuk menolak memberikan data semacam itu.

Mirip dengan RUU PDP, Pasal 23 dalam GDPR juga mengatur tujuan khusus di mana pemerintah negara anggota Uni Eropa dapat mengesahkan UU yang mengizinkan badan pemerintah untuk mengakses data pribadi. Dengan pembatasan bahwa UU tersebut "menghormati inti dari hak dan kebebasan dasar dan memang merupakan sebuah upaya yang diperlukan dan proporsional dalam komunitas yang demokratis" UU nasional dapat menggagalkan hak kerahasiaan data dalam hal pertahanan nasional dan keamanan umum, penegakkan hukum, moneter, isu anggaran dan perpajakan, kesehatan masyarakat dan jaminan sosial. Akan tetapi, pasal yang sama tersebut di dalam GDPR juga secara jelas menyatakan bahwa UU semacam itu harus merinci tujuan dari pemrosesan data, kategori data yang diakses, ruang lingkup pembatasan, pengamanan untuk mencegah penyalahgunaan dan akses yang melanggar aturan atau transfer data, periode penyimpanan data, hak pemilik data untuk diinformasikan tentang pembatasan, dll. (GDPR, 2018).

Dalam hal RUU PDP Indonesia, harus ada jaminan bahwa setelah pemerintah mengakses data pribadi, data tersebut tidak akan digunakan untuk tujuan lain yang tidak disebutkan sebelumnya dan tidak dibocorkan ke

masyarakat. Pemerintah di banyak negara berupaya untuk melindungi kerahasiaan data pribadi. Di Indonesia, data pribadi milik Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) di bawah Kementerian Dalam Negeri pernah dijual dengan berbagai harga dan dengan paket yang bisa disesuaikan di situs friendmarketing.com. Menurut laporan berita, tersangka yang ditangkap ditemukan memiliki data dari 50.854 keluarga, termasuk 1.162.864 Nomor Induk Kependudukan (NIK), 761.435 nomor telepon seluler, 129.421 nomor kartu kredit dan 64.164 nomor rekening (VOI, 2020).

Pendekatan berbasis risiko perlu digunakan untuk melindungi data pribadi

Sanksi RUU PDP masuk dalam kategori administratif dan pidana. Sanksi administratif diawali dengan teguran tertulis, diikuti dengan penangguhan sementara, kompensasi kesalahan penanganan data pribadi, dan denda administratif. Aturan pidana dalam RUU PDP membuat pelaku pelanggaran kerahasiaan data dapat dituntut karena tindak kriminal.

Pemberlakuan sanksi RUU PDP dilakukan setelah diputuskan bahwa seseorang atau sebuah lembaga telah melanggar kerahasiaan data pribadi. Akan tetapi, perlu dilakukan penyesuaian dalam RUU PDP untuk menjelaskan tingkat pengawasan dan beratnya sanksi yang tergantung pada volume data yang dilanggar dan kerugian yang disebabkan oleh pihak yang tidak patuh.

Mengikuti praktik oleh pihak yang berwenang atas perlindungan data di Perancis, CNIL, RUU PDP harus meminta kepada mereka yang berencana untuk mengelola data pribadi untuk pertama-tama mengidentifikasi kerugian yang dapat muncul dari pemrosesan data. Pengawas kemudian harus mengevaluasi besarnya kerugian dan menilai kerentanan sistem dan operasi mereka. Menurut Lembar Putih atau laporan resmi *International Association of Privacy Professionals* (IAPP), EU GDPR juga menggunakan pendekatan berbasis risiko untuk isu kepatuhan. Meskipun tidak tercantum secara eksplisit dalam peraturannya, tetapi konsep tersebut menentukan kriteria penilaian penalti untuk kasus ketidakpatuhan yang menyebabkan kerusakan fisik, materi, atau moral pemilik data. Konsekuensi yang merusak secara khusus dianggap berat ketika pemilik data mengalami "diskriminasi, pencurian identitas atau penipuan, kerugian finansial, kerusakan reputasi, kehilangan data rahasia yang dilindungi oleh kerahasiaan profesional, pengungkapan nama samaran, atau kerugian ekonomi atau sosial lainnya yang signifikan" (Maldoff, 2016).

Mengikuti contoh EU GDPR, RUU PDP juga harus membedakan tingkat risiko yang muncul dari kegiatan pemrosesan data. Area-area berisiko tinggi haruslah yang melibatkan aktivitas-aktivitas sistematis dan ekstensif untuk menampilkan profil individu, untuk memproses kategori-kategori khusus dari sebuah data, dan untuk memantau area yang dapat diakses oleh publik. Siapapun yang berencana untuk terlibat dalam kegiatan-kegiatan ini harus berkonsultasi dengan pihak berwenang di Indonesia sebelum melakukan kegiatannya. Mereka harus melakukan penilaian dampak yang rinci dan memberitahukan individu yang berpotensi terkena dampaknya apabila ada kasus kebocoran data.

RUU PDP memberikan wewenang pengawasan kepada pihak kementerian pemerintah

RUU PDP berencana menetapkan wewenang pengawasan untuk kerahasiaan data. Pasal 58 dan 59 menyatakan bahwa peran ini akan dipegang oleh pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo). Keputusan itu dianggap kontroversial karena Kominfo adalah sebuah lembaga negara yang kebal terhadap UU ini, karena mereka juga mengolah data pribadi. Jika Kominfo mengawasi pelaksanaan kerahasiaan data, wewenang sebagai regulator dan pengawas berpotensi menimbulkan konflik kepentingan terkait pengelolaan data pribadi yang dilakukan oleh Kominfo sendiri.

RUU PDP seharusnya membentuk badan independen untuk perlindungan data pribadi yang berlaku sebagai pemegang wewenang pengawasan dalam proses pelaksanaan RUU PDP. Singapura, misalnya, telah membentuk

lembaga independen yang mengawasi masalah PDP, sesuai dengan UU yang berlaku di Singapura. Oleh karena itu, *Personal Data Protection Commission* (PDPC) Singapura bisa berlaku secara independen ketika mengawasi pengelolaan data pribadi oleh pemerintah dan lembaga swasta. Britania Raya juga telah melakukan penunjukkan penugasan dan kuasa untuk mengawasi kerahasiaan data kepada lembaga independen, yaitu Kantor Komisioner Informasi atau *The Information Commissioner's Office* yang merupakan badan negara non-departemen yang melapor secara langsung kepada parlemen (Information Commissioner's Office, 2018a).

Cara-Cara Inovatif untuk Mengembangkan UU Kerahasiaan Data

Dalam ekonomi digital yang berkembang cepat, perusahaan kerap ada di bawah tekanan untuk berinovasi. Mereka perlu memperbaharui produk dan layanan mereka, tampilan pengguna, dan interaksi dengan konsumen. Teknik manajemen modern, yang sarat ketangkasan dan kolektivitas, merupakan indikasi bagi perusahaan di sektor ekonomi digital untuk merespons pasar yang terus berubah dengan lebih cepat dan efektif. Kekhawatiran akan tertinggal dan kalah dari pesaing mereka dibarengi dengan adanya risiko bahwa alat dan aplikasi pemrosesan data mereka yang baru kemungkinan termasuk dalam pelanggaran peraturan kerahasiaan data. Oleh karena itu, merupakan hal yang penting untuk mengembangkan kebijakan dan peraturan kerahasiaan data yang tidak menghambat perusahaan untuk berinovasi.

Sebuah mekanisme yang cocok untuk mengatasi masalah ini adalah *regulatory sandbox* (Ruang Uji Terbatas), yang membantu menjembatani pemerintah sebagai regulator dan pihak swasta dalam membangun kerangka kerja yang terbuka akan inovasi. Awalnya mekanisme ini dikembangkan di sektor keuangan dengan tujuan mengizinkan perusahaan untuk menguji produk inovatif, layanan, atau model bisnis mereka sementara dikecualikan dari beberapa kewajiban. Otoritas berwenang yang mengawasi jalannya uji terbatas ini tidak memberlakukan beberapa aturan administratif dan menggunakan kesempatan tersebut untuk tujuan meningkatkan inovasi. Cara tersebut mengizinkan perusahaan untuk menguji inovasi yang mereka buat dan memahami ekspektasi pengawasan, sementara pemerintah mendapatkan gambaran teknologi baru selama masa pengujian sehingga mereka bisa mulai menyesuaikan pengawasan mereka (Taylor Wessing LLP, 2020). Indonesia sebetulnya memiliki beberapa pengalaman dalam menerapkan Ruang Uji Terbatas. Bank Indonesia (BI) mengeluarkan Peraturan BI Nomor 22/23/PBI/2020 tentang Sistem Pembayaran yang memberikan kerangka kerja peran BI dalam menstimulasi inovasi melalui Ruang Uji Terbatas untuk menguji peraturan dan kebijakan yang mengatur inovasi baru (Suleiman, 2021).

The Information Commissioner's Office di Britania Raya menggunakan Ruang Uji Terbatas untuk perlindungan kerahasiaan data pribadi. Fase strategi teknologi 2018-21 mereka yang disebut fase beta ini berencana untuk mengundang sekitar 10 lembaga dari sektor swasta dan pemerintah untuk mendukung kerahasiaan data dan inovasi. Dari Juli 2019 hingga September 2020, lembaga-lembaga tersebut diharapkan bisa menanggulangi masalah penggunaan data pribadi dalam teknologi yang muncul atau tengah berkembang, pertukaran data yang kompleks, menciptakan pengalaman pengguna yang baik, dan membangun kepercayaan masyarakat dengan memastikan transparansi dan kejelasan penggunaan data, serta tantangan perlindungan data khusus lainnya (Information Commissioner's Office, 2018b). Perusahaan farmasi Novartis misalnya, berpartisipasi dalam sebuah Ruang Uji untuk mengidentifikasi risiko kerahasiaan data ketika menggunakan aplikasi suara dalam sebuah situasi klinis serta apa yang harus mereka lakukan untuk menanggulangi risiko-risiko tersebut (Business at OECD, 2020).

Pengalaman lain dan lebih dekat dari Indonesia, misalnya, Singapura yang menggunakan Ruang Uji Terbatas ketika merevisi UU PDP mereka (Monetary Authority of Singapore, 2019). *Infocomm Media Development Authority* (IMDA) Singapura dan *Personal Data Protection Commission* (PDPC) melibatkan enam kontributor data untuk pengujian dan validasi konsep yang juga melibatkan pertukaran data umum dan pribadi. Di bawah Kerangka Kerja Pertukaran Data Terpercaya atau *Trusted Data Sharing Framework*, Ruang Uji Terbatas dimulai dengan fase keterlibatan di mana perusahaan memberikan rencana mereka untuk berinovasi dengan menggunakan data. Jika fase ini tidak bisa memastikan bahwa mereka telah mematuhi peraturan yang berlaku, maka IMDA/PDCP akan memberikan panduan untuk mengurangi ketidakpastian terkait inovasi tersebut. Akhirnya, jika kekhawatiran tersebut masih tetap belum tertangani, maka regulator dan perusahaan bekerja sama untuk membuat panduan baru atau kebijakan baru sebagai amandemen terhadap UU yang sudah ada. Ketika Singapura memperbarui UU PDP mereka dan tengah membuat panduan terkait, Facebook berkolaborasi dengan IMDA dalam sebuah proyek Ruang Uji Terbatas. Sebagai bagian dari proyek Facebook Accelerator - Singapura, Ruang Uji Terbatas mencari

panduan dari regulator dan ahli di sektor industri terkait ketika bekerja dengan startups untuk bersama-sama membuat cara terkait pemberitahuan dan dinamika persetujuan dapat diimplementasikan dalam produk dan layanan yang inovatif (Business at OECD, 2020).

Pengalaman di Singapura dan Britania Raya bisa memberikan pelajaran yang sangat baik bagi proses penyusunan peraturan tentang kerahasiaan data dan RUU PDP di Indonesia.

Referensi

Ameed, M., & Natgunanathan. (2016). Protection of big data privacy. *IEEE access*, 1821-1834.

Aprilianti, I. (2020). Melindungi Masyarakat: *Memajukan Hak-Hak Konsumen Digital*. Diambil dari laman CIPS: https://www.cips-indonesia.org/digital-consumer-rights-pp27

Bank Indonesia (2017). *FREQUENTLY ASKED QUESTIONS: PERATURAN ANGGOTA DEWAN GUBERNUR NO.19/14/PADG/2017 TENTANG RUANG UJI COBA TERBATAS (REGULATORY SANDBOX)*. Diambil dari laman Bank Indonesia: https://www.bi.go.id/elicensing/helps/FAQ%20REGSAND.pdf

Butarbutar, R. (2019). Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia. *3rd International Conference on Law and Governance*, 154-163.

Business at OECD (BIAC). (2020). Regulatory Sandboxes for Privacy Analytical Report, November 2020. Diambil dari laman BIAC: https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

Desy, S. (2020). MOEC Denies 1.3 Million Employee Data Leaks. Diambil dari laman KataData: https://katadata.co.id/desysetyowati/digital/5ece8096d6625/kemendikbud-bantah-1-3-juta-data-pegawainya-bocor

Djafar, W., Sumigar, F., & all, e. (2016). *Perlindungan Data Pribadi di Indonesia: Ulasan Pelembagaan Dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM Press.

Drake, G. (2016). Navigating the Atlantic: understanding EU data privacy compliance amidst a sea of uncertainty. *S. Cal. L. Rev.*, *91*, 116-128.

GDPR. (2018). Regulation (EU) 2016/679 (General Data Protection Regulation) version OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. Diambil dari laman Info GDPR: https://gdpr-info.eu

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Indonesia and Turkey*, 10-13.

Information Commissioner's Office. (2018a). About Information Commisioners Officers. Diambil dari laman ICO: https://ico.org.uk/about-the-ico/

Information Commissioner Office. 2018b. *Sandbox beta phase: Discussion Paper*. Diambil dari laman ICO: https://ico.org.uk/media/2614219/sandbox-discussion-paper-20190130.pdf

Jiska, C. (2016). The spy next door: Eavesdropping on high throughput visible light communications. *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*.

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

Maldoff, Gabriel. (2016). The Risk-Based Approach in the GDPR: Interpretation and Implications. *White Paper by the International Association of Privacy Professionals (IAPP)*. Diambil dari laman IAPP: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

Monetary Authority of Singapore. (2019). *Overview of Regulatory Sandbox*. Diambil dari laman MAS: https://www.mas.gov.sg/development/fintech/regulatory-sandbox

Nugroho, A. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding* 7.7, 183-189.

Petter, J. (2019). *Data Privacy Guide: Definitions, Explanations and Legislation*. Diambil dari laman Varonis: https://www.varonis.com/blog/data-privacy/

Privacy International. (2013). *A Guide for Policy Engagement: Part 1 Data Protection Explained*. Diambil dari laman Privacy International: https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf

Reynaldi, F., & Tifana, N. (2020). Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Perlindungan Data Pribadi. Universitas Padjajaran Press.

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

Rosadi, S. (2018). Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia.". *Brawijaya Law Journal 5.1* , 143-157.

SNIA. (2019). *What is Data Privacy?* Diambil dari laman edukasi SNIA: https://www.snia.org/education/what-is-data-privacy

Suleiman, Ajisatria. (2021). Meningkatkan Perlindungan Konsumen Fintech P2P Lending Berpenghasilan Rendah. Center for Indonesian Policy Studies.

Taylor Wessing LLP. (2020). Regulatory Sandboxes. Diambil dari laman Lexology: https://www.lexology.com/library/detail.aspx?g=419b7b84-bde0-4c29-bb63-41df2aa3d0b1

Tourkochoriti, I. (2016). The Snowden revelations, the Transatlantic Trade and Investment Partnership and the divide between US-EU in data privacy protection. *University of Arkansas at Little Rock Law Review 36*, 161-176.

VOI. (2020). We are Personal Data That is Sold and Purchased, 4 Agustus 2020. Diambil dari: https://voi.id/en/tulisan-seri/10237/we-are-personal-data-that-is-sold-and-purchased

TENTANG PENULIS

Gliddheo Algifariyano Riyadi adalah *research trainee* di CIPS *Emerging Policy Leaders Program* (EPLP) 2020. Saat ini dia bekerja sebagai Analis Organisasi dan Pemerintahan di Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah. Sebelum bergabung dalam EPLP, Gliddheo bekerja sebagai Analis Riset dan Kebijakan di Komisi Pemantauan Otonomi Daerah. Dia mendapatkan gelar sarjana Ilmu Politik dari Universitas Indonesia pada tahun 2019.

CIPS
Center for Indonesian Policy Studies

Center for Indonesian Policy Studies (CIPS) merupakan lembaga pemikir non-partisan dan non profit yang bertujuan untuk menyediakan analisis kebijakan dan rekomendasi kebijakan praktis bagi pembuat kebijakan yang ada di dalam lembaga pemerintah eksekutif dan legislatif.

CIPS mendorong reformasi sosial ekonomi berdasarkan kepercayaan bahwa hanya keterbukaan sipil, politik, dan ekonomi yang bisa membuat Indonesia menjadi sejahtera.

Center for Indonesian Policy Studies

contact@cips-indonesia.org

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

www.cips-indonesia.org

Kerja kami bergantung pada dukungan Anda. Kunjungi **www.cips-indonesia.org/donate** untuk mendukung CIPS.