PERLINDUNGAN DATA PRIBADI DI INDONESIA

MENYIKAPI LIBERALISASI EKONOMI DIGITAL

LAPORAN PENELITIAN:

Tim Penyusun:
Olisias Gultom (IGJ)
Auditya Firza Saputra (PSHK)
Muhammad Faiz Aziz (PSHK)

Juni 2021

DAFTAR ISI

DAFTAR ISI 2
DAFTAR TABEL 4
DAFTAR GAMBAR 4
BAB 1 5
PENDAHULUAN 5
1.1. PENGANTAR 5
1.2. 'DATA', 'INFORMASI' DAN 'BIG DATA' 6
1.3. LIBERALISASI EKONOMI DIGITAL 7
1.4. ISU YANG DISOROTI 12
1.5. DEFINISI OPERASIONAL 12
1.6. BATASAN RUANG LINGKUP KAJIAN 14
BAB 2 15
KONSEP DATA PRIBADI DALAM SISTEM HUKUM INDONESIA 15
2.1. PENGANTAR 15
2.2. ASPEK HUKUM PRIVAT 16
2.2.1. Data dalam Perspektif Hukum Benda 16
2.2.2. Data dari Aspek Hukum Perikatan 18
2.3. DATA DARI ASPEK HUKUM EKONOMI 19
2.3.1. Nilai Ekonomi Langsung 19
2.3.2. Nilai Ekonomi Tidak Langsung 22
2.4. ASPEK HUKUM PUBLIK DARI DATA 23
2.4.1. Otoritas yang Mengurusi Perlindungan Data Pribadi di Indonesia 25
2.5. PENTINGNYA PELINDUNGAN DATA DAN INFORMASI PRIBADI: PRIVASI, KEAMANAN DAN OTONOMI INDIVIDU 27
2.6. INISIATIF KOMUNITAS INTERNASIONAL 30
BAB 3 32
PERBANDINGAN KONSEP HUKUM PELINDUNGAN DATA PRIBADI 32
3.1. PRINSIP-PRINSIP PERLINDUNGAN DATA PRIBADI 32
3.2. GDPR UNI EROPA 32
3.2.1. Lawfulness, Fairness and Transparency 34
3.2.2. Purpose Limitation 34
3.2.3. Data Minimization 35
3.2.4. Accuracy 36
3.2.5. Storage Limitation 36
3.2.6. Integrity and Confidentiality 36
3.3. PERBANDINGAN PRAKTIK DI BEBERAPA NEGARA 38

3.3.1. Perlindungan Data Pribadi di Amerika Serikat *38*
3.3.2. Perlindungan Data Pribadi di Kanada *41*
3.4. SIKAP INDONESIA DALAM PERJANJIAN INTERNASIONAL TENTANG PENGATURAN ARUS DATA LINTAS NEGARA 44
BAB 4 46
PEMETAAN REGULASI PERLINDUNGAN DATA PRIBADI DI INDONESIA 46
4.1. PENGANTAR 46
4.2. REGULASI INTI 48
4.2.1. Tingkat Undang-Undang *48*
4.2.2. Tingkat Peraturan Pelaksana *54*
4.3. REGULASI PENUNJANG 85
4.3.1. Sektor Bisnis *85*
4.3.2. Sektor Perbankan dan Jasa Keuangan *89*
4.3.3. Sektor Pelayanan Publik *92*
4.3.4. Sektor Kesehatan *97*
4.4. REGULASI DALAM PROSES 99
Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP) *99*
BAB 5 110
CATATAN TEMUAN BERDASARKAN PEMETAAN REGULASI 110
5.1. DIMENSI SUBSTANSI HUKUM 110
5.2. DIMENSI STRUKTUR 118
5.3. DIMENSI KULTUR 121
5.4. KERENTANAN MASYARAKAT ATAS BIAS ALGORITMA 121
BAB 6 125
PENUTUP 125
6.1. KESIMPULAN 125
6.2. SARAN 126
BIBLIOGRAFI 127
LAMPIRAN 1274

DAFTAR TABEL

Tabel 4.2.1.1 Pemetaan Substansi Pelindungan Data dalam UU ITE..... 50
Tabel 4.2.2.1 Pemetaan Substansi Pelindungan Data dalam PP PSTE..... 57
Tabel 4.2.2.2 Pementaan Regulasi PDP Pada PP PMSE.....68
Tabel 4.2.2.3 Pemetaan Regulasi Permen Kominfo PDPSE..... 71
Tabel 4.2.2.4 Pemetaan Regulasi Permenkominfo PSE-LP..... 79
Tabel 4.2.2.5 Kategori Sistem Elektronik dalam Peraturan BSSN Pengamanan Sistem Pengamanan PSE.....84
Tabel 4.3.1.1 Pemetaan Regulasi Penunjang Sektor Bisnis..... 85
Tabel 4.3.2.1 Pemetaan Regulasi Penunjang di Sektor Perbankan..... 89
Tabel 4.3.3.1 Regulasi Penunjang Sektor Pelayanan Publik.....93
Tabel 4.3.4.1 Regulasi Data Pribadi di Sektor Kesehatan.....97
Tabel 4.4.1.1 Perbandingan Hak Subjek Pemilik Data Pribadi dalam RUU PDP dan GDPR 102
Tabel 4.4.1.1 Perbandingan Pengaturan Cross-Border Data Flow.....108

DAFTAR GAMBAR

Gambar 1.2.1 Hubungan antara Data & Informasi.....6
Gambar 1.5.1 Ruang Lingkup Ekonomi Digital.....14
Gambar 3.1.1 Konstruksi Siklus Hidup Data menurut GDPR..... 32
Gambar 4.4.1 Rancangan Muatan Substansi RUU PDP..... 100

BAB 1

PENDAHULUAN

1.1. Pengantar

"*The world is going digital and there's no escape".* Kalimat tersebut sering muncul di internet tatkala menelusuri tema-tema pencarian tentang digitalisasi. Suka tidak suka, segala aspek kehidupan hari ini bergerak ke arah digital. Seluruh inovasi teknologi di masa depan diproyeksikan mengusung tema digital. Sementara kehadiran pandemi di awal 2020 makin mengakselerasi pengkonversian seluruh aktivitas manusia menjadi digital dan secara bersamaan transformasi ini juga menelurkan banyak persoalan baru terkait perlakuan atas data-data pengguna internet yang dikumpulkan. Sebab, dengan *big data*, perusahaan teknologi informasi menjadi pihak yang paling diuntungkan dari skenario ini.

Di satu sisi, arah orientasi ekonomi dunia juga semakin bergerak liberal. Serangkaian edisi revolusi industri dan perkembangan teknologi yang dibawanya menciptakan skema industrialisasi baru di mana doktrin-doktrin tentang laju perdagangan dunia menuntut terciptanya pasar yang bebas dan terbuka. Dalam hemat itu, berbagai aturan untuk mempersulit terjadinya perdagangan lintas batas dinilai sebagai hambatan. Menurut Adams, 'ekonomi liberal' adalah sistem ekonomi yang diatur pada jalur individu, artinya, keputusan ekonomi terbesar dibuat oleh individu atau rumah tangga daripada oleh institusi atau organisasi kolektif.[1] Sistem itu menampilkan aktor-aktor privat sebagai pemain utama dan kegiatan lagi proses ekonomi diserahkan sebesar-besarnya pada pasar yang biasanya dilaksanakan dalam bentuk perdagangan bebas. Asumsinya, ketika pasar menetapkan otoritas ekonomi, ia akan punya caranya sendiri untuk menemukan kesesuaian antara permintaan dan penawaran sedang intervensi negara diminimalisasi untuk hanya terlibat manakala terjadi kegagalan pasar.

Di sisi lain, perusahaan-perusahaan teknologi informasi pemilik server raksasa berikut para penyedia layanan jasa *daring* pengelola data masih berhutang sebuah pekerjaan rumah tentang bagaimana memproteksi data masyarakat penggunanya dengan sebaik-baiknya. Begitu pun negara dan komunitas internasional: punya andil menentukan bagaimana cara pekerjaan rumah tersebut diselesaikan. Bagaimana tidak, dalam lalu lintas aktivitas digital yang kian intensif itu, terutama di negara-negara berkembang seperti Indonesia, data dan informasi sering dipandang sebatas *by-product* saja. Literasi akan kerahasiaan data masih rendah,[2] padahal data pribadi berikut kumpulannya telah jadi komoditas eksklusif yang ramai-ramai dilabeli hak milik, bahkan cukup leluasa diperdagangkan dari satu yurisdiksi negara ke lainnya. Perdebatan tentang konsep

---

[1] Adams, *Political Ideology*, (Manchester University Press: 2001), dikutip dari Mohammad Fajar Iksan dkk, 'Impact of digital economic liberalization and capitalization in the era of industrial revolution 4.0: case study in Indonesia', *Problems and Perspectives in Management*, Vol. 18 No. 2, (June 2020), 290-301, doi:10.21511/ppm.18(2).2020.24, hlm. 291.

[2] Lihat: Kementerian Komunikasi dan Informatika, "Status Literasi Digital Indonesia: Survei di 34 Provinsi", (November 2020), hlm. 24, diunduh dari https://bit.ly/3vxukVq.

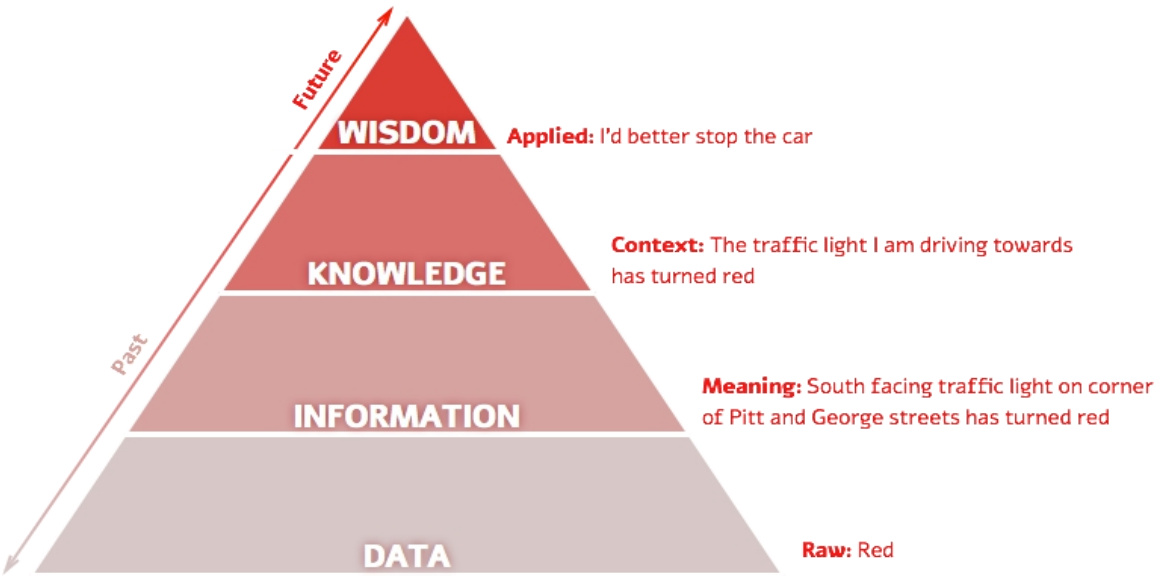
perlindungan data pribadi yang benar-benar berperspektif keadilan semakin santer dibicarakan, baik di level nasional maupun internasional.

1.2. 'Data', 'Informasi' dan 'Big Data'

Bagi awam, istilah 'data' seringkali digunakan untuk menggeneralisasi sesuatu yang bernilai sebagai informasi. Tentu pandangan tersebut tak bisa sepenuhnya disalahkan mengingat penggunaan istilah data memang memiliki cakupan operasional luas. Pada kegiatan riset, misalnya, istilah data dipakai untuk merujuk pada kumpulan sumber informasi yang telah diolah sehingga memiliki nilai implementatif. Namun, dalam konteks teknologi informasi, ada perbedaan cukup mendasar antara data dan informasi.

Data adalah segala sesuatu yang disimpan di dalam memori menurut format tertentu, sementara, informasi adalah 'hasil pengolahan data' yang sudah dapat diterima oleh akal pikiran penerima informasi, yang nantinya dipakai untuk mengambil keputusan.[3] Artinya, tidak semua data bisa dipakai untuk mencapai pengetahuan. Data sendiri pada dasarnya bisa bersifat terstruktur maupun tidak terstruktur. Contohnya dalam dunia pemrograman (komputer), data berwujud angka-angka algoritmik yang terdiri dari 0 dan 1. Tentu saja angka-angka ini tidak langsung punya nilai tanpa dilekatkan pada variabel-variabel tertentu. Pelekatannya pada variabel tertentu merupakan proses 'pengidentifikasian' di mana sebuah data mentah berubah jadi informasi. Selanjutnya setelah menjadi informasi, data-data yang saling berkorespondensi bisa dianalisis dan teraplikasikan menjadi pengetahuan (*intelligence* atau *knowledge*) guna mengetahui pola-pola kontekstual. Pada puncaknya, siklus akhir dari data mampu membentuk *wisdom* karena memahami sebuah prinsip yang dapat diaplikasikan untuk masa depan dalam pemecahan masalah. Alur yang dimaksud dipaparkan pada Gambar 1.2.1.

Gambar 1.2.1 Hubungan antara Data & Informasi



[3] Winardi Fertian, "Perbedaan Data dan Informasi", binus.ac.id, 14 Juli 2016, diakses dari https://bit.ly/342zKfQ.

Sementara, *big data* (atau maha data) adalah istilah untuk segala himpunan data dalam jumlah besar, rumit, dan tidak terstruktur sehingga menjadikannya sukar ditangani apabila menggunakan perangkat manajemen basis data atau aplikasi pemrosesan data tradisional belaka.[4] Menurut Djafar, istilah *big data* biasa digunakan untuk menjelaskan penerapan Teknik-teknik analisis untuk mencari, mengumpulkan dan merujukkan secara silang kumpulan data dalam jumlah besar untuk mengembangkan sistem kecerdasan dan wawasan.[5] Maha data memenuhi beberapa kriteria, yang disebut 3V, yakni: varietas, *velocity* (atau kecepatan) dan volume. Kumpulan data berjumlah besar ini didapatkan dari sumber-sumber umum maupun khusus semisal kumpulan data pelanggan perusahaan tertentu.[6] Karena varietas dan volumenya yang besar, konsepsi big data berangsur-angsur berubah, tidak hanya mencakup data yang bersifat umum, namun juga informasi yang dikumpulkan oleh sektor privat. Faktor itulah yang mendasari lahirnya definisi maha data sebagai kemunculan kumpulan data baru bervolume besar yang berubah dengan cepat, kompleks, dan melampaui jangkauan kemampuan analisis lingkungan perangkat keras dan perangkat lunak yang umumnya digunakan untuk pemrosesan data. Keunggulan dari *big data,* sebagai babak lanjut dari pemanfaatan data dan informasi, merupakan modal penting dalam menciptakan *knowledge* dan *wisdom.* Pada penelitian ini, penggunaan istilah 'data' dalam terminologi 'data pribadi' ke depannya akan sering dipakai bergantian, yang secara makna dapat merujuk pada kedua konteks (baik data maupun informasi). Penggunaan satu peristilahan ini sengaja dimaksudkan guna memudahkan pembaca yang tidak begitu akrab dengan istilah-istilah teknis dalam dunia komputer.

1.3. Liberalisasi Ekonomi Digital

Revolusi industri telah mencapai jilid keempatnya. Setelah mesin uap hingga otomasi industri, kini giliran kecerdasan buatan hadir mendominasi aktivitas produksi manusia. Dalam skenario itu, data dibutuhkan untuk menunjang kecerdasan buatan: semakin banyak data yang dimiliki semakin sempurna pula logaritma kecerdasan buatan dalam memecahkan problem yang diajukan. Mayoritas data di era masyarakat informasi hari ini dikumpulkan lewat platform media baru seperti internet, yang belakangan telah didapuk sebagai budaya massa. Revolusi digital itu menciptakan pelbagai inovasi canggih yang relatif terbuka bagi semua untuk berpartisipasi di dalamnya sebagai penggunanya. Tuntutan atas manfaat praktis tadi membuat kemudahan-kemudahan yang ditawarkan jadi menggiurkan semua orang. Menurut Sudibyo situasi ini menciptakan suatu dilema sosial, sebab banyak orang terbuai dengan kedermawanan penyedia platform yang memberikan berbagai fasilitas guna secara gratis walau di sisi lain harus menggelontorkan dana yang tak sedikit membangun teknologi tersebut.[7] Akan tetapi, faktanya pemanfaatan perangkat-perangkat digital oleh publik luas tidak berarti diberikan oleh pemiliknya dengan cuma-

---

[4] *Ibid.*

[5] Wahyudi Djafar, "Hukum Perlindungan Data Pribadi di Indonesia", makalah untuk materi kuliah umum "Tantangan Hukum dalam Era Analisis Big Data" Universitas Gadjah Mada Yogyakarta, tanggal 26 Agustus 2019.

[6] *Ibid.*

[7] Lihat: Agus Sudibyo, *Jagat Digital: Pembebasan dan Penguasaan,* (Jakarta: Kepustakaan Populer Gramedia, 2019), hlm. 5.

cuma. Dalam skenario itu, timbal balik yang harus diberikan *user,* tentu saja, mewujud dalam nilai tukar data. Atau lebih tepatnya: data perilaku pengguna.

Problemnya, tidak semua penggunanya internet sadar bahwa data mereka dikumpulkan, atau mungkin tahu namun kurang peka perihal kepentingan proteksi data. Kesadaran itu baru datang di belakang manakala terjadi kerugian, semisal serangan siber, yang terpaksa disesali. Karena itu, tanpa inisiatif kebijakan perlindungan dari otoritas, hal ini sangat mungkin menciptakan model eksploitasi baru.

Terlihat, misalnya, ketika seseorang mendaftar akun layanan digital seperti sosial media atau sejenisnya, situs mewajibkan pendaftar meng-*input* serangkaian data dan informasi tentang identitas pribadinya. Beberapa *platform* bahkan mengharuskan pengguna mengunggah data-data penting seperti foto kartu identitas kependudukan atau nomor rekening bank. Tak henti di situ, platform lain, contohnya saja, seperti *Facebook, Instagram*, *YouTube* bahkan tak hanya sekedar mengumpulkan data pribadi, melainkan juga merekam tampilan diri kita secara visual. Fitur pengenalan wajah yang dimiliki kecerdasan buatan, contohnya *Google Lens*, mampu mengidentifikasi siapa kita hanya berdasarkan mimik wajah pada foto. Pada titik ini, bisa dikatakan data-data pribadi yang awalnya kita masukan mulai melengkapi informasi tentang diri kita. Belum lagi peron digital lainnya seperti *marketplace* yang diam-diam merekam jejak, pola, dan riwayat konsumsi berikut preferensi komoditas barang atau jasa konsumen. Bukan tidak mungkin, dengan gencarnya akuisisi atau penggabungan perusahaan penyelenggara sistem elektronik belakangan, penyedia marketplace bisa saja tiba-tiba terafiliasi kepemilikan dengan perusahaan penyedia layanan sosial media; dan ketika itu terjadi, satu per satu data-data yang tertampung merangkai kesatuan informasi utuh yang mengaktualisasikan diri kita. Seluruh akumulasi itu menciptakan *cloning* digital dari kehidupan luring kita. Titik klimaksnya: kecerdasan buatan seakan bisa lebih kenal diri kita dibanding diri kita sendiri. Maka, wajar jika data tak ubahnya komoditas yang paling ramai ditambang hari ini, sebab, data jadi modal berharga untuk merekayasa sosial, atau bahkan memanipulasi perilaku manusia.

Sementara isu perlindungan atas data pribadi masih belum terselesaikan, isu keadilan dan etis mencuat lantaran pihak yang paling diuntungkan dari kapitalisasi *big data* tak lain adalah para perusahaan pemilik server. Pasalnya dengan kumpulan teknik-teknik analisis data yang bisa kapan saja dipakai, pemasaran jadi makin mudah. Begitu pun periklanan. Seluruh segi kehidupan manusia dari ranah privasi hingga publik bisa dilacak, diproyeksi, dan diprediksi lewat data. Termasuk pula pemerintah dalam hal surveilans. Dalam hal itu, hasil olahan data-data bagi bisnis sangat penting untuk mendeteksi demografi spesifik konsumen. Pelaku usaha bisa memahami kecenderungan dan pola hidup, konsumsi, bahkan hingga kepribadian konsumennya; meski saat ini analisis big data masih bergantung pada kecerdasan manusia, namun dalam perkembangannya nanti, Forgo dkk menyebut, "…*Big Data will in the future increasingly result in automated decision-making, where autonomous machines carry out certain tasks without human intervention"*.[8]

[8] Nikolaus Forgo, Stefanie Hanold dan Benjamin Schutze, "The Principle of Purpose Limitation", dalam Marcelo Coralles (Ed) dkk, *New Technology, Big Data and the Law,* (Springer Verlag, 2017), hlm. 22

Paralel, seiring komodifikasi data serta imbas globalisasi ekonomi, permintaan atas aliran bebas data dari satu negara ke negara lain meningkat. Dengan terbukanya kemungkinan melakukan transfer data lintas batas negara, perusahaan dagang di satu belahan dunia bisa semakin mudah berekspansi di negara-negara baru yang belum sempat terjamah olehnya, atau setidak-tidaknya dengan modal temuan dari data, mereka mampu mengidentifikasi pasar baru yang cocok dengan inti bisnis yang dijalankan. Praktis kegunaan *big data* memberikan efisiensi dalam pelbagai aspek ekonomi digital.

O'Neil dalam *Weapon of Math Destruction* menyebut bahwa, di balik berbagai kemudahan yang ditawarkan, ada sisi gelap dari era algoritma yang cukup destruktif. Itu tercipta imbas dari eksploitasi *big data,* yang menurutnya akan semakin memperparah ketidaksetaraan yang sebelumnya sudah terjadi.[9] Kontras dengan apa kebanyakan yang masyarakat hari ini percaya, baginya algoritma matematis dalam sistem komputer tidaklah objektif. Sebab, sejak awal logaritma kecerdasan buatan dioptimalkan ke sebuah definisi kesuksesan versi penciptanya.[10] Tak ada jaminan bahwa konsepsi 'sukses' versi penciptanya sama dengan yang dipahami publik. Jangan dilupakan pula bahwa penciptanya punya kepentingan ekonomis atas inovasinya tersebut; sementara masyarakat, di sisi lain, hanya jadi konsumen yang terkatung-katung sambil terbelenggu layar gawai dalam gencarnya hegemoni *big data*.

Situasi timpang atas data itu, menurut O'Neil, punya tiga problem utama, yaitu ketidakjelasan, ketiadaan regulasi yang cukup, dan kondisi yang sulit untuk dikontestasi. Dengan kata lain, jika teknologi *big data* tidak diterapkan dengan hati-hati, atau terlalu diasumsikan objektif untuk membantu pengambilan keputusan, mesin-mesin ini rentan untuk menciptakan problem baru, yang salah satunya adalah diskriminasi. Problem semakin parah ketika mengetahui bahwa mesin yang memiliki kemampuan mengambil keputusan secara otomatis itu disusun berdasarkan pembelajaran historis menggunakan data-data atau *Big Data* dari masyarakat yang sebenarnya diskriminatif atau mengandung bias. Praktis, hal itu akan membuat sistem tersebut cenderung mempertahankan pola diskriminasi atau bias lainnya, atau bahkan memperkuatnya. Masalah sebelumnya jelas mempersulit perubahan masyarakat menjadi lebih baik, bahkan memiliki peluang mempertahankan persoalan atau kerusakan yang terjadi pada suatu sistem dalam masyarakat.

West mengistilahkan fenomena serupa dengan istilah *data capitalism*.[11] Pergerakan ini akan membawa peradaban dunia melampaui kapitalisme gaya usang seketika data telah didapuk jadi sumber monetasi utama. Bukan sekedar jadi tujuan akhir dari penciptaan nilai, tapi penguasaan atas data juga merepresentasikan kekuasaan politik. Kuasa kapital menelurkan konsep baru dimana orang-orang dengan modal intelektual yang mampu menerjemahkan data-data itu yang jadi pemegang kendali, sekaligus menyingkirkan kapitalisme gaya lama yang terkungkung modal finansial. West menyebut, *"[...] Data*

---

[9] Lihat: Cathy O'Neil, *Weapon of Math Destruction: How Big Data Increases Inequality and Threaten Democracy,* (New York: Crown Publisher, 2016).

[10] Pendapat O'Neil dalam wawancara pada film dokumenter-investigatif karya Jeff Orlowski, "The Social Dilemma", Netflix, 2020.

[11] Lihat: Sarah Myers West, 'Data Capitalism: Redefining the Logics of Surveillance and Privacy', *Business & Society*, Vol. 58(1) 20–41, 2019, doi: 10.1177/0007650317718185

capitalism results in a distribution of power that is asymmetrical and weighted toward the actors who have access and the capability to make sense of data. This uneven distribution is enacted through capitalism and justified by the association of networked technologies with the political and social benefits of online community, drawing upon narratives that generally fall within the rubric of technological utopianism".[12] Lagipula, tentang data jadi modal mencapai kursi kekuasaan bukan sekedar hipotesis belaka: skandal *Cambridge Analytica* jadi salah satu buktinya. Konglomerat besar berhasil mengkapitalisasi kecerdasan para ilmuwan jenius data untuk memenangkan sosok Donald Trump jadi Presiden Amerika Serikat. Konon, kontroversi itu bermula dari aktivitas akses ilegal terhadap data 87 juta profil pengguna Facebook oleh perusahaan agensi tanpa persetujuan pemilik data.[13] Pada kesempatan lainnya, perkawinan algoritma kecerdasan buatan dan *big data* berhasil memanfaatkan momentum untuk mempropagandakan keputusan keluarnya Inggris dari Uni Eropa (*Vote Brexit*); sekalipun pada kasus itu diklaim bahwa penyingkapan atas data ditampilkan secara anonim, nyatanya serangkaian fenomena tadi membawa kerugian kebudayaan karena mendekadensikan kualitas demokrasi.

Transformasi dan meningkatnya risiko tersebut disikapi oleh beberapa negara maju dengan membentuk regulasi terkait perlindungan data pribadi. Diantaranya memperkenalkan konsepsi hak individu atas privasi data, di mana tiap-tiap pemrosesan atas data yang dilakukan pengendali hanya bisa dilakukan sepengetahuan dan persetujuan pemiliknya. Tak hanya itu, isu lain yang diangkat, salah satunya mendorong pengaturan perihal transfer data lintas batas negara. Ada dua *barrier* yang umumnya digunakan untuk membatasi transfer data lintas batas: pertama, kebijakan restriksi bersyarat untuk pemindahan data ke luar negeri; dan kedua, kewajiban melokalisasi penempatan data di dalam negeri.[14] Kebijakan pertama umumnya diberlakukan untuk data-data yang dikelola sektor privat; sementara yang kedua jadi kewajiban bagi sektor publik. Dari keduanya, sebagian pihak menilai kebijakan restriksi cenderung lebih ekonomis dan minim efek disruptif dibandingkan dengan kewajiban melokalisasi data. Dalam hemat maksimalisasi keuntungan, tentu kebijakan yang kedua tidak populer karena menambah ongkos-ongkos operasional; tak ayal, proposal mendorong pelonggaran arus data lintas negara banyak datang dari pelaku industri digital untuk dibicarakan pada perundingan level internasional.

Lebih jauh, data terkini UNCTAD menyebutkan bahwa 66% negara di dunia telah memiliki legislasi terkait hukum perlindungan data pribadi sementara 10% masih di level proses pembuatan naskah, termasuk Indonesia.[15] Uni Eropa, misalnya, pada 2016 menyepakati sebuah paket regulasi Panduan Umum Pelindungan Data Umum, atau biasa disebut GDPR, pada 2016. Keberhasilan itu membayar rintisan inisiasi yang telah dilakukan sejak dua dekade ke belakang.[16] Instrumen tadi mengharuskan perlakukan data

---

[12] *Ibid.,* hlm. 23.

[13] Lihat: Christine Olivier Schenable, Bernice Simone Elger, dan David shaw, 'The Cambridge Analytica affair and internet-mediated research", *Embo Reports,* Vol. 19(1), Juli 2018, doi:10.15252/embr.201846579

[14] 'International: US-EU cross-border data transfers', dataguidance.com, November 2019, diakses dari https://www.dataguidance.com/opinion/international-eu-us-cross-border-data-transfers

[15] UNCTAD, 'Data Protection and Privacy Legislation Worldwide', diakses dari https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[16] Lihat: Orla Lynskey, *The foundations of EU data protection law,* (Oxford: Oxford University Press, 2016), hlm. 4-6.

terbatas dalam koridor penghormatan privasi dan hak individu pemilik data (*data subject*) sehingga informasi yang dikumpulkan tidak bisa dipergunakan untuk tujuan lain selain dari tujuan awal yang diketahui *user* saat mendaftar suatu layanan digital. Dalam konteks transfer dan penempatan data lintas negara, GDPR juga mengatur bahwa aktivitas *cross-border data transfer* hanya bisa dilakukan terbatas ke negara-negara yang sudah memiliki standar yang memadai. Organisasi yang lebih dekat dengan Indonesia seperti ASEAN sejak 2018 mulai merintis kerangka kerja strategis tata kelola data digital. Diantaranya seperti *ASEAN Cross Border Data Flows Mechanism* dan *ASEAN Data Protection and Privacy Forum*. Mekanisme sukarela buah diskusi forum Asia Tenggara ini mendorong, salah satunya, pembentukan klausul kontrak kerja sama intra-negara anggota, juga kemudahan dalam memfasilitasi transfer data di dalam kawasan semaksimal mungkin (*maximize data flows*).

Beranjak ke negara lain, seperti Republik Rakyat Tiongkok (RRT) dan Vietnam, kebijakan yang dipilih pemerintah cenderung lebih proteksionis. Mengedepankan alasan kepentingan keamanan nasional dan perlindungan industri dalam negeri, tata kelola data dikendalikan secara dominan oleh otoritas yang berada di bawah kendali langsung pemerintah.[17] Kebijakan *China Cybersecurity Law 2016*, yang mulai berlaku sejak Juni 2017, misalnya, mengatur keharusan lokalisasi data terkhusus untuk data-data yang bersifat strategis. Tapi, persoalan krusial yang mengganjal datang dari negara asal produsen layanan sistem elektronik terbesar seperti Amerika Serikat, yang cenderung percaya pada pendekatan *self-regulation*, mengingat perusahaan-perusahaan pendominasi industri maha data itu lebih menghendaki intervensi otoritas publik atas data seminimal mungkin atas nama komitmen pada perdagangan bebas. Berbeda dengan Uni Eropa, proteksi atas data pribadi dalam konteks kebijakan di AS dilakukan secara sektoral lewat aturan spesifik pada masing-masing kegiatan ekonomi yang diatur.

Liberalisasi data memberikan berbagai dampak baik secara langsung maupun tidak langsung. Proposal WTO seperti yang diusulkan oleh perusahaan besar, membuka ruang yang sangat luas bagi liberalisasi perdagangan dan ekonomi, liberalisasi data merupakan bagian didalamnya, telah menjadi acuan atau bahan dasar dalam perundingan-perundingan *Free Trade Agreement* (FTA). Kesepakatan FTA sendiri dilakukan dalam bentuk *comprehensive* yang terintegrasi dengan berbagai hal, tidak hanya sebatas kesepakatan perdagangan. Perluasan ini sudah tentu memberikan dampak yang lebih luas terlebih dengan adanya konsekuensi melakukan ratifikasi perundang-undangan masing-masing negara mengikuti hasil kesepakatan. Kesepakatan liberalisasi data pada perdagangan bebas akan berdampak pada kebijakan perlindungan data secara luas, termasuk data pribadi dan sangat rentan mengancam masyarakat. Pola ini menjadikan FTA menjadi pintu masuk bagi liberalisasi secara lebih luas.

Nasib negara-negara berkembang seperti Indonesia berada dalam situasi ambang. Di satu sisi, pasca keberlakuan GDPR, Indonesia turut mengalami ‘efek Brussels’ karena harus ikut menyeragamkan standar pelindungan agar kerja sama di bidang ekonomi digital bisa berlanjut. Di sisi lain, ketiadaan regulasi spesifik tentang perlindungan data pribadi

[17] Beiten Burkhardt, ‘China: Protection of Personal Information – Moving Closer to a Chinese GDPR?”, lexology.com, (14 April 2021), diakses dari https://bit.ly/3yPugDg.

jadi salah satu alasan yang membuat kita terkatung-katung tanpa pendirian. Penundaan demi penundaan pengesahan Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP) membuat Indonesia kehilangan momentum puncak karena belakangan pembicaraan di level internasional mulai mengarah ke pelonggaran proteksi. Sementara tingkat pengguna internet Indonesia terus tumbuh bahkan diproyeksi menjadi salah satu yang terbanyak di dunia.[18] Akhirnya, Indonesia cenderung tunduk dan mengadopsi model-model aturan yang ditetapkan negara atau organisasi internasional lain atau mengupayakan mendorong penyelesaian secara dialog lewat perjanjian bilateral. Tapi, pilihan dialogis itu membuat persoalan semakin rumit karena ada standar yang tidak seragam antar satu perjanjian dan lainnya. Otoritas tampak seakan tak punya sikap dan pendirian yang pasti karena diikat oleh standar proteksi data pribadi yang berbeda-beda. Hubungan kerja sama perdagangan di sektor ekonomi digital antarnegara juga membawa masalah baru terkait pemrosesan data, sebab, kerangka regulasi di satu negara sangat mungkin memengaruhi kebijakan di negara lain. *"[...]Privacy and data protection are increasingly cross-sectoral and international issues. The actions of a regulator in one country can directly affect another, and regulatory co-operation as well as higher level of trust is required between regulators*".[19] Dalam menentukan arah kebijakan perlindungan data pribadi di level internasional, posisi tawar Indonesia tentu tak sekuat negara lain. Faktor kepercayaan tinggal jadi satu-satunya yang bisa ditumpu oleh negara seperti Indonesia. Posisinya semakin dilematis mengingat demografi Indonesia jadi potensi besar bagi ekspansi pasar internasional.

1.4. Isu yang Disoroti

Berdasarkan latar belakang sebelumnya, kajian ini akan menelaah dua isu utama, antara lain:

- Peraturan perundang-undangan apa saja yang telah disusun oleh Pemerintah Indonesia dalam rangka menghadapi liberalisasi ekonomi digital? Apa yang sudah diatur dan apa yang belum diatur?
- Bagaimana peraturan perundang-undangan di Indonesia telah melindungi hak-hak masyarakat dari potensi dampak yang muncul dari aturan liberalisasi perdagangan digital yang diatur di dalam perjanjian perdagangan bilateral, regional, dan multilateral?

1.5. Definisi Operasional

Untuk selanjutnya dalam penelitian ini, yang dimaksud dengan:

a. 'Digital Ekonomi' adalah aktivitas perdagangan barang dan jasa melalui fitur digital atau sistem elektronik, termasuk namun tidak terbatas pada *e-commerce,* perdagangan dataset tentang demografi konsumen yang terolah sebagai komoditas, dalam yurisdiksi

[18] Akhdi Martin Pratama, 'Pengguna Internet Indonesia hingga Kuartal II 2020 Capai 196,7 Juta Orang', kompas.com, 9 Oktober 2020.

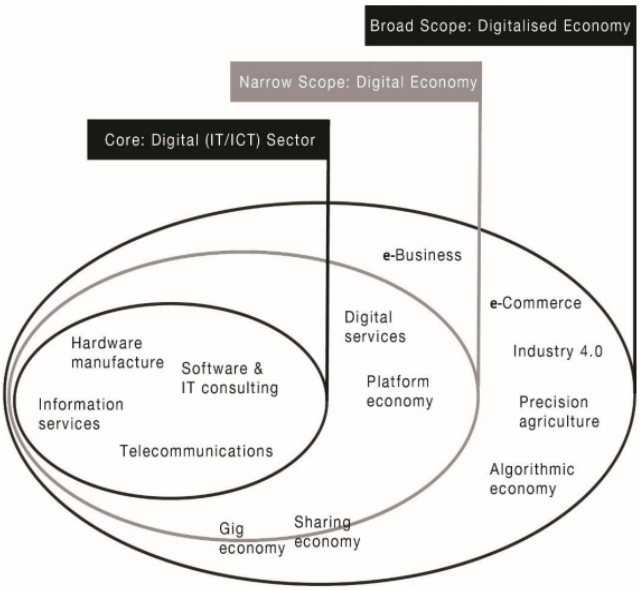
[19] Intermedia, 2020, dalam Muhammad Faiz Aziz, "Pelindungan Data/Informasi Pribadi di Masa Pandemi Covid-19", materi presentasi untuk webinar #ngoPI Vol. 2, PPI Scania Swedia dan PSHK, 9 Mei 2020.

nasional maupun lintas batas negara.[20] [Lihat: Gambar 1.5.1.] Namun, untuk penyederhanaan pembahasan, kajian ini dibatasi pada konteks yang beririsan langsung tentang pemrosesan data pribadi.

b. Liberalisasi' adalah serangkaian upaya yang umumnya diinisiasikan secara kolektif di tingkat internasional untuk membebaskan atau meminimalisir hambatan (*barrier)*, baik berupa tariff ataupun non-tariff semisal regulasi ataupun restriksi, dalam konteks ekonomi digital terutama di lingkup kegiatan pemrosesan data, khususnya pada isu transfer data lintas batas negara.
c. 'Pengelola Data' adalah penyelenggara sistem elektronik sebagaimana diatur dalam UU ITE, termasuk lembaga publik yang mengelola data warga masyarakat dan lembaga swasta yang mengelola data konsumen ataupun lainnya, yang sudah terelektronisasi menjadi informasi elektronik.
d. 'Pemrosesan data' merupakan kegiatan yang berkaitan langsung dengan pengumpulan, pemanfaatan, penyimpanan, pembukaan dan transfer, pemusnahan data pribadi konsumen layanan sistem elektronik, oleh data kontroler ataupun pihak lain yang ditunjuknya.
e. 'Data kontroler' (*data controller*), atau sesekali bisa juga disebut pengendali dan/atau pengelola data, adalah pihak yang melakukan pemrosesan data pribadi, secara manual atau otomasi, melalui metode pengarsipan dalam sistem elektronik.
f. 'Otoritas' merujuk pada entitas pemerintah yang berwenang dan bertanggung jawab sebagai pelaksana fungsi pengendalian data pribadi.

[20] Dalam Laporan Digital Ekonomi UNCTAD 2019, ada dua perspektif dalam mendefinisikan digital ekonomi, yakni secara luas dan sempit. Secara luas, digital ekonomi meliputi kegiatan seluruh kegiatan ekonomi yang berbasis digital, baik fasilitas teknologi digital, seperti perdagangan software, manufaktur perangkat keras, jasa konsultasi dan telekomunikasi berbasis digital; maupun jasa-jasa platform digital seperti e-commerce, e-business. Secara sempit, digital ekonomi merujuk pada aktivitas *digital services* dan *platform economy*. Lihat: UNCTAD, *Digital Economy Report 2019*, (New York: United Nations, 2019), hlm. 5-6.

Gambar 1.5.1 Ruang Lingkup Ekonomi Digital



Sumber: UNCTAD, *Implementing World Summit on the Information Society Outcomes,* 2017, https://unctad.org/system/files/official-document/ecn162018crp2_en.pdf, hlm. 8.

1.6. Batasan Ruang Lingkup Kajian

Kajian ini dibatasi spesifik pada perlindungan data pribadi di ranah penyelenggaraan sistem elektronik dalam konteks pemrosesan data secara umum, dan secara khusus perihal regulasi terkait transfer data lintas batas negara. Penulis menyadari bahwa, untuk membuat kajian menyeluruh atas masing-masing aspek dalam digital ekonomi, dibutuhkan tak kurang dari lusinan buku yang menyoroti tiap-tiap masalahnya. Oleh karena itu, pembatasan dalam kajian ini krusial diperlukan untuk menjaga mengalirnya narasi pembahasan dan sekaligus menghindari pembahasan yang terlalu jauh meluas. Dengan kata lain, mengacu pada dimensi ekonomi digital yang luas sebagaimana dalam Gambar 1.3.1., penelitian ini tidak akan mendalami konteks pengaturan pada isu komoditas perangkat lunak dan keras yang sebenarnya juga merupakan bagian integral dari kegiatan ekonomi digital. Fokus diutamakan pada aspek pelindungan data pribadi secara umum, dengan catatan beberapa aspek terkait *e-commerce* mungkin akan sedikit-banyak diulas sebagai penunjang pembahasan. Pembatasan ruang lingkup kajian ini juga mempertimbangan jangka waktu penelitian yang relatif pendek sehingga jika pun harus dipaksakan meluas, dapat dipastikan tidak akan mengeluarkan produk riset yang mendalam.

BAB 2

KONSEP DATA PRIBADI DALAM SISTEM HUKUM INDONESIA

2.1. Pengantar

Sejarawan kondang Yuval Noah Harari dalam *Homo Deus* menyebut jika sejak kebangkitan sains dan teknologi, data telah diperlakukan oleh manusia bak kultus baru. Sebutan yang ia pakai: *data religion.*[21] Berbagai penemuan penting di bidang ilmu pengetahuan dan teknologi farmasi berikut industri medis senantiasa membutuhkan tunjangan data-data sebagai modal awal. Fenomena 'datafikasi' mengalami perluasan seiring meningkatnya kebutuhan akan data guna menunjang aktivitas sektor-sektor publik. Sehingga, berbagai irisan objek yang mengandung nilai informatif, sebagaimana umumnya sebuah data, diatur dalam peraturan perundang-undangan, dalam ranah privat maupun publik.

Dalam sistem hukum Indonesia hari ini, ihwal data diatur dalam banyak produk hukum lintas sektor lagi dimensi. Misalnya, data dalam konstruksi sebagai 'benda' menurut hukum kebendaan perdata; atau dalam kaitannya dengan perdagangan, data sebagai komoditas dalam hemat hukum bisnis. Begitu pun dalam hal praktik kedokteran, rekam medis seseorang yang diatur dalam UU Kesehatan juga tergolong merupakan data pribadi. Di kesempatan lain, data juga berfungsi sebagai dokumentasi atau arsip kependudukan atau kenegaraan yang menunjang aktivitas administrasi negara; pelacakan; statistik pembangunan dan seterusnya. Pun menyangkut persoalan penegakan hukum, beberapa pasal di undang-undang memuat sanksi pidana atas pelanggaran data privasi seseorang, termasuk larangan untuk pengumpulan data lewat penyadapan ilegal.

Dalam kaitannya dengan keterbukaan informasi, ada undang-undang sendiri yang mengatur tata cara mengakses data dan informasi. Belum lagi berbicara aspek hukum internasional dari data, mengingat benda itu belakangan marak dikompromikan dalam berbagai hubungan dagang internasional, atau lebih luas lagi dalam berbagai perundingan internasional. Jadi, disadari atau tidak, data menjadi bagian tak terpisahkan yang memiliki dimensi yuridis sangat luas.

Sebelum lebih jauh, penting untuk memahami tiga paradigma dasar atas data. Dari situ, kita bisa memetakan perlakuan-perlakuan seperti apa yang ideal atas data. Paradigma yang dimaksud terdiri dari: (1) data pribadi sebagai data personal (individual); (2) data pribadi sebagai properti yang dilekatkan kepemilikan; dan (3) data pribadi menjadi data publik ketika teragregat. Yang pertama, data pribadi pada dasarnya merupakan hak individu dari pemilik data sepenuhnya mengingat informasi yang terkandung merepresentasikan serta menyangkut pula identitas dan otonomi diri *data subject.* Ihwal privasi sendiri sejatinya turunan dari doktrin hak milik:[22] gagasannya adalah bahwa seseorang berhak bebas menikmati otonomi hidupnya baik materiil maupun immateriil

---

[21] Yuval Noah Harari, 'Data Religion', dalam *Homo Deus: A Brief History of Tomorrow*, (London: Vintage, 2016), hlm. 428-462. Bandingkan dengan, Yuval Noah Harari, 'Dataism is Our New God', *New Perspective Quarterly,* Vol. 34 Issue 2, (Mei 2017): 34-43. DOI: 10.1111/npqu.12080.

[22] Lihat misalnya: Russell Brown, "Rethinking Privacy", *Alberta Law Review Vol. 43 No. 3, (2006)*: 589-614, hlm. 592.

termasuk yang berkaitan dengan hal-hal kerahasiaan informasi diri. Ini sejalan dengan artikulasi Pasal 28H UUD 1945 yang menyebutkan, "Setiap orang berhak mempunyai hak milik dan hak milik tersebut tidak boleh diambil secara sewenang-wenang oleh siapapun". Konstruksi kepemilikan sebagaimana dimaksud mencakup pula kepemilikan berwujud immateriil, semisal, muatan 'nilai informatif' yang inheren dalam data.[23] Kedua, ketika data pribadi ditransmisikan secara sah oleh pemiliknya ke dalam sistem elektronik yang dikelola atau dimiliki pihak lain (*data user*), objek tersebut bisa beralih menjadi properti yang dapat dilekatkan kepemilikan-terbatas pihak pengendali. Di fase ini, paradigma data pribadi berubah; data pribadi yang terkoleksi (dengan syarat dan berdasarkan konsensualitas pemilik data) beralih menjadi milik Pengelola Sistem Elektronik sepanjang berdasarkan hal-hal yang diizinkan pemiliknya. Pembatasan itu penting karena menyangkut penghormatan hak-hak privasi individu *data subject* mengingat pemanfaatannya akan sekecil apapun menyimpan risiko. Sementara, yang ketiga, sewaktu dibutuhkan untuk kepentingan publik, informasi yang merupakan hasil olah atas data-data sebelumnya bisa menjadi milik publik, terutama untuk data-data umum yang disajikan secara teragregat. Misal, data-data statistik tentang demografi penduduk (jenis kelamin, kelompok usia, pekerjaan, dan seterusnya). Dalam paradigma yang terakhir, data bisa diakses lewat skema keterbukaan informasi publik untuk kepentingan siapa saja. Hal itu dikarenakan, berbeda dengan data pribadi yang bersifat individual, pada konteks data teragregat tidak ada isu privasi spesifik yang mencuat lantaran informasi ditampilkan secara populatif (pemaparan keseluruhan).

2.2. Aspek Hukum Privat

2.2.1. Data dalam Perspektif Hukum Benda

Dalam aktivitas ekonomi digital, data adalah properti. Meski tak secara spesifik disebut dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata), konstruksi hukum perdata Indonesia memperlakukan objek-objek seperti data sebagai 'benda'. Interpretasi deduktif dilakukan untuk menyimpulkan status kebendaannya mengingat hukum kodifikasi peninggalan kolonial Belanda itu memang belum mengenal konsep benda-benda elektronik. Konsekuensinya sebagai benda membuat pengaturan hukum benda buku ke-II KUHPerdata otomatis berlaku di sini. Pasal 499 KUHPerdata mengangkat pengertian benda sebagai: "segala sesuatu yang dapat menjadi hak milik".

Sudah dijelaskan sebelumnya, bahwa hak milik bisa juga melekat atas benda-benda materiil seperti informasi yang punya nilai berharga. Ada dua aspek kepemilikan yang muncul dan ini berkaitan pula dengan paradigma data. *Pertama*, data sebagai hak milik individu yang bersangkutan; dan *kedua*, hak milik bagi pihak lain ketika hak atas data itu diserahkan secara sukarela. Konsepnya agak mirip dengan pengaturan hak cipta dalam hukum kekayaan intelektual yang memiliki dua dimensi kepemilikan (*joint ownership*); pada suatu objek bisa melekat dua hak sekaligus: hak moral pada penciptanya dan hak ekonomis pada pihak yang diserahkan. Selanjutnya, KUHPerdata membedakan benda

[23] Pasal 28G UUD 1945 yang berbunyi: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan dan harta benda yang dibawa kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

menjadi 'benda bergerak'[24] dan benda tidak bergerak (terbatas pada objek benda seperti tanah, kapal laut dengan ukuran volume tertentu). Benda bergerak sendiri terklasifikasi jadi benda bergerak karena sifatnya dan benda bergerak karena ketentuan undang-undang.[25] Karena format fisiknya bisa dipindahtangankan dari satu pihak ke pihak lain, data merupakan bergerak. Konstruksi data sebagai konsep kebendaan juga ditekankan dalam undang-undang, misalnya, sebagai 'informasi elektronik' sebagaimana UU ITE.

Berdasarkan wujudnya, konsep benda dalam hukum perdata terbagi menjadi benda berwujud dan tidak berwujud.[26] Perihal data, ada keunikan tersendiri sebab 'informasi' sebagai benda pada dasarnya tidaklah berwujud. Informasi menampakan wujudnya ketika telah melalui pengolahan atau pendokumentasian tertentu, misalnya menjadi catatan tertulis atau dalam format-format elektronik. Lebih jauh, menurut Hasbullah, pentingnya pembedaan tersebut berkaitan dengan empat hal, yaitu penguasaan, penyerahan, daluwarsa, dan pembebanan.[27] Dalam konteks penguasaan, konsekuensi utama dari penggolongannya ke benda bergerak ini adalah melekatnya '*bezit'* sebagai titel yang sempurna.[28] Adapun yang dimaksud dengan bezit adalah kedudukan menguasai atau menikmati suatu barang yang ada dalam kekuasaan seseorang secara pribadi atau dengan perantaraan orang lain, seakan-akan barang itu miliknya sendiri.[29] Dan, dalam konsep hukum kebendaan, *bezit* diperlakukan sebagai titel kepemilikan bagi seseorang yang melakukan penguasaan fisik atas benda bergerak.[30] Dengan kata lain, ketika seseorang menguasai benda bergerak secara fisik, ia secara hukum diasumsikan sebagai pemiliknya.

Menggunakan hemat itu, pengelola sistem informasi, *server*, ataupun pemilik *database* merupakan pemegang *bezit.* Hal ini memberi keleluasaan bagi penguasa benda bergerak untuk menggunakan atau memanfaatkan benda di bawah penguasaannya untuk tujuan apapun. Tapi, yang patut jadi catatan penting di sini, *bezit* hanya bisa melekat ketika terjadi peralihan yang sah. Dan, tiap-tiap pemindahan benda bergerak mensyaratkan adanya penyerahan simbolis atau dalam istilah hukumnya '*levering'.*[31] Penyerahan itu sekaligus menandai penyerahan yuridis (peralihan hak) dan dimulainya titel *bezit*. Penyerahan ini, dalam konteks kegiatan pemrosesan data, biasanya berbentuk pengisian form submisi dan penginputan ke dalam database oleh pemilik data (atau biasa disebut proses pengumpulan). Selepas transmisi penginputan dilakukan, hukum 'mengasumsikan' telah terjadi *levering:* pemilik data telah secara hukum menyerahkan data-datanya pada pengelola sistem elektronik. Secara teoritis, adanya konsep benda bergerak berikut konsekuensi *bezit*-nya membuka peluang bagi pemanfaatan data secara eksploitatif demi

---

[24] Pasal 509 KUHPerdata: "Benda bergerak karena sifatnya bisa dipindah tangankan", dan Pasal 513 KUHPerdata, "Istilah barang bergerak, tanpa ada pengecualian, meliputi segala sesuatu yang menurut ketentuan-ketentuan di atas, dianggap bersifat bergerak."

[25] Pasal 511 KUHPerdata. Contohnya, hak-hak seperti hak pakai, piutang, dst.

[26] Pasal 503 KUHPerdata: "Ada barang yang bertubuh, dan ada yang tidak bertubuh."

[27] Freida Husni Hasbullah, *Hukum Kebendaan Perdata: Hak-Hak yang Memberi Kenikmatan, Jilid 1,* (Jakarta: Ind-Hill Co, 2005), hlm. 45-47.

[28] Berbeda dengan benda tidak bergerak seperti tanah yang titel kepemilikannya tak cukup didasarkan atas penguasaan saja, tapi juga harus ada pengakuan dari negara lewat proses pendaftaran. Lihat: Pasal 506 KUHPerdata.

[29] Pasal 529 KUHPerdata.

[30] Pasal 1977 KUHPerdata: "Bezit atas benda bergerak berlaku sebagai titel yang sempurna".

[31] Pasal 612 KUHPerdata: "penyerahan benda bergerak dapat dilakukan dengan penyerahan nyata. Dengan sendirinya penyerahan itu sekaligus penyerahan yuridis.

keuntungan sepihak pengumpul data. Oleh karena itu, kerangka proteksi atas data pribadi sebagai sebuah hukum menjadi semakin urgen. Dalam logika hukum perlindungan data pribadi, meski secara hak sudah terjadi peralihan, kewenangan pengelola atau penyelenggara sistem elektronik atas objek data yang diserahkan tidaklah mutlak dan tanpa batasan. Sekalipun melekat *bezit*, pada konten informasi inti yang diberikan oleh konsumen atau *user* tetap melekat hak perorangan (privasi pemilik data). Sehingga sifat kepemilikan dari pengelola data atas data yang dikoleksi hanya terbatas. Paralel, tiap-tiap penggunaannya untuk tujuan lain hanya bisa dilakukan dengan otorisasi dari pemilik data. Konstruksi logika hukum ini menjadi dasar pembuatan prinsip-prinsip hukum pelindungan data pribadi global. Artinya, di sini diperlukan aturan khusus (*lex specialis*) dalam ranah hukum telematika agar penyelenggara sistem elektronik yang melakukan pengelolaan dan pemanfaatan atas data-data tersebut hanya terbatas pada pemanfaatan yang diotorisasi oleh pemilik data. Status *bezit* atas data akan selalu dapat ditantang jika pemilik data (*data subject*) menilai penggunaannya dilakukan oleh pihak lain untuk tujuan-tujuan yang tidak sesuai atau dimanfaatkan tanpa itikad baik.

2.2.2. Data dari Aspek Hukum Perikatan

Selain kebendaan, konsep yang tak kalah penting untuk mengenali pengaturan data pribadi adalah ‘perikatan’. Perikatan terjadi karena adanya suatu hubungan hukum tertentu yang diatur undang-undang (contoh: jual-beli), atau tercipta atas dasar kesepakatan sadar (perjanjian) para pihak. Konsekuensi hukum dari suatu perikatan adalah berlakunya pengaturan undang-undang terhadap perbuatan spesifik (sedangkan apabila perikatannya lahir dari perjanjian, maka tiap-tiap kondisi yang telah disepakati mengikat para pihak sebagai hukum; dengan kata lain, bisa mengesampingkan ketentuan undang-undang). Lebih jauh, dalam konteks perjanjian, hukum perdata mengenal asas ‘kebebasan berkontrak’. Mengutip Subekti, siapa saja memiliki “kebebasan yang seluas-luasnya untuk mengadakan perjanjian yang berisi apa saja, asalkan tidak melanggar ketertiban umum dan kesusilaan”.[32] Termasuk dalam kebebasan itu adalah otonomi untuk mengatur objek apa yang ingin diperjanjikan (sepanjang bukan yang dilarang oleh hukum).

Setiap benda pada dasarnya bisa diperalihkan haknya. Tak terkecuali benda yang berupa data pribadi. Peralihan itu terjadi karena suatu hubungan hukum (perikatan) tertentu, misal, hubungan pengguna-penyedia jasa digital (konsumen-pelaku usaha), atau berdasarkan perjanjian atau bisa juga gabungan keduanya.[33] Dari perikatan itu, pengguna jasa alias konsumen aplikasi mendapatkan keuntungan dalam bentuk, misalnya, akses guna pada platform yang disediakan sementara penyedia jasa mendapat keuntungan dari pengumpulan data penggunanya. Namun demikian, mengingat dalam objek data pribadi melekat hak moral/privasi individu pemilik data, maka tiap-tiap hubungan hukum yang

[32] Subekti, *Hukum Perjanjian*, Cetakan ke-21, (Jakarta: Penerbit Intermasa, 2005), hlm. 13

[33] Misalnya, ketika seorang memutuskan untuk mendaftar dan menggunakan layanan digital. Ia secara simbolik telah melakukan perikatan. Dan, ketika yang bersangkutan menyetujui terms and condition, perikatan itu beranjak jadi perjanjian penggunaan jasa.

tercipta seputar pemrosesan atas data haruslah berbasis persetujuan dari pemilik data. Persetujuan (*consent*) sendiri sebenarnya hanya salah satu aspek dari perjanjian.[34]

Suatu perjanjian adalah sah apabila memenuhi unsur objektif maupun subjektif.[35] Pada tataran subjektif, para pihak harus (1) 'sepakat' dan juga (2) 'cakap'. Sepakat dalam hal ini berarti pemilik data maupun kolektornya harus sama-sama tahu konsekuensi hak dan kewajiban hukum dari perikatan yang dilakukan. Di samping itu, kesepakatan yang dimaksud juga tidak boleh didasarkan pada kekhilafan atau hal-hal yang disembunyikan. Inilah mengapa, dalam *best practice* pelindungan data pribadi, banyak dipersyaratkan *explicit consent*. Sementara, asas kecakapan hukum menuntut para pihak yang melakukan perikatan untuk mampu berhitung rasional atas konsensus yang diberikannya. Kecakapan diukur dari adanya kedewasaan (berbasis batasan usia) dan dari kemampuan kognitif (sehat secara kejiwaan atau tidak berada dibawah pengampuan).

Ukuran kecakapan menjadi penting mengingat pengguna internet yang datanya dikumpulkan tak hanya orang dewasa, tapi juga anak. Karena hukum mengasumsikan anak-anak tidak memiliki legitimasi untuk melakukan perbuatan hukum, maka data anak hanya bisa diambil ketika diotorisasi oleh orang tua atau walinya. Selanjutnya untuk syarat objektif, keabsahan perjanjian ditentukan berdasarkan (3) adanya hal tertentu yang diperjanjikan dan (4) sebab/kausa yang diperbolehkan undang-undang. Poin nomor tiga menekankan bahwa suatu perjanjian dengan kata lain tidak bisa dibuat tanpa objek sedang poin yang terakhir menegaskan bahwa hanya objek-objek yang bisa legal saja yang bisa diperjanjikan. Pemenuhan keempat syarat itu secara kumulatif menentukan keabsahan perjanjian sekaligus konsekuensi legalitas yang membuntut di belakang. Sebab, jika perikatan dibuat dalam kondisi mengandung cacat pada unsur subjektif, para pihak dapat membatalkannya; sementara jika kecacatan terletak pada unsur objektif, maka perjanjian menjadi batal demi hukum, atau dengan kata lain, diasumsikan tidak pernah ada.

2.3. Data dari Aspek Hukum Ekonomi

Konsekuensi dari data sebagai hak kebendaan adalah melekatnya nilai ekonomis disertai hak-hak turunannya. Praktis, ada setidaknya dua aspek ekonomi dari data: (1) nilai ekonomi secara langsung dan (2) tidak langsung. Elaborasi lebih rinci dipaparkan di bawah:

2.3.1. Nilai Ekonomi Langsung

Relasi antara perusahaan aplikasi dan penggunanya sebenarnya bersifat simbiosis: di satu sisi, pengguna diberi kemudahan dari fungsi dan manfaat aplikasi; tetapi di sisi lain operator data juga diuntungkan karena mengumpulkan data-data pengguna. Manfaat ekonomi langsung dari data bisa didapatkan dari kegiatan jual-beli atau monetasi data. Sementara, komodifikasi data bisa bersifat *direct*—dalam arti kumpulan data langsung dijual ke pihak ketiga, atau secara *indirect*—di mana hasil olahan data berbentuk informasi

[34] Hukum perdata mengakui dua jenis perjanjian: secara tertulis, yang seringkali dipersamakan dengan 'kontrak'; maupun perjanjian verbal. Akan tetapi, untuk kepentingan pembuktian, kontrak lebih diutamakan karena dalam format itu hak dan kewajiban para pihak lebih mudah dirujuk.

[35] Pasal 1320 KUHPerdata.

maupun pengetahuan dijual ke pihak ketiga. Ringkasnya, nilai ekonomi langsung dari data muncul karena dapat komodifikasi untuk kepentingan perdagangan.

Lebih jauh, pada praktiknya, dataset yang dikoleksi kerap dijual oleh perusahaan IT kepada perusahaan lain yang membutuhkannya. Terutama untuk perusahaan periklanan. Menurut Makarim, informasi pribadi merupakan suatu komoditas yang laku terjual, penjualan dan perdagangan informasi telah berkembang menjadi industri yang menghasilkan jutaan dolar.[36] Tentu tidak semua negara memperbolehkan penjualan data ini, karena adanya asas *purpose limitation*,[37] meski demikian, pada beberapa yurisdiksi negara yang belum memiliki hukum perlindungan data pribadi memadai, kegiatan jual-beli data sangat leluasa terjadi. Pun dalam negara yang sudah mengadopsi perlindungan data pribadi, praktik jual-beli data tetap marak dan beberapa perusahaan kolektor data cukup cerdik mengakali hal tersebut dengan membuat klausula pada bagian syarat dan kondisi (*terms and condition)* yang harus diterima oleh penggunanya: "bahwa data yang dikoleksi menjadi sepenuhnya milik pengelola data, dan pemilik data mengizinkan data tersebut dipergunakan untuk tujuan apapun, termasuk untuk diungkap ke pihak ketiga".

Sebagai komoditas, nilai ekonomi dari data terbilang cukup tinggi. Pada 2017, Institute of Director sebagaimana diwartakan oleh Katadata, memperkirakan pasar *big data* di Indonesia bisa mencapai US$41,77 juta atau setara Rp 556 miliar.[38] Nilai pasar tertinggi diproyeksikan untuk industri penyedia infrastruktur digital, yaitu sekitar US$15,43 juta dengan tingkat pertumbuhan rata-rata periode 2012–2017 mencapai 45,1 persen. Di bidang *marketing* terutama industri perbankan, jual beli data pribadi dilakukan untuk menjaring calon nasabah. Temuan investigasi Kompas (13/5/19) menyebut data pribadi yang kualitasnya bagus bisa dijual seharga Rp1 Juta untuk 50 data, atau Rp 200 ribu per data.[39] Data yang punya nilai jual tinggi biasanya dilengkapi dengan informasi perihal gaji dan kemampuan finansial dari Bank Indonesia dan Otoritas Jasa Keuangan.[40] Praktik penjualan data ini marak imbas dari sistem komisi yang diberikan bank kepada agen kartu kredit yang berhasil menjaring nasabah baru. "Jika datanya bagus, dari 50 ada peluang 30-40 orang di dalamnya bersedia mengajukan permohonan kartu kredit jenis platinum," aku sang informan.[41]

Transaksi serupa disinyalir terjadi juga pada media sosial. Hampir seluruh perusahaan media sosial berbagi data penggunanya kepada pihak ketiga yang biasanya dimanfaatkan oleh pengiklan. Dalam laman pCloud, Instagram didapuk jadi aplikasi yang

---

[36] Edmon Makarim, 'Kajian Aspek Hukum Perlindungan Data dan Hak Pribadi', dalam *Pengantar Hukum Telematika: Suatu Kompilasi Kajian,* (Depok: Badan Penerbit FHUI & Rajawali Pers, 2005), hlm. 185.

[37] Indonesia sendiri memperbolehkan penjualan sepanjang dengan persetujuan pemilik data. Lihat Pasal 26 ayat (1) UU ITE. "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

[38] "Berapa Nilai Pasar Big Data di Indonesia?", *katadata.co.id*, 13 Juni 2017, diakses dari https://bit.ly/3g3WNxH.

[39] Kompas, "Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial", *Harian Kompas*, 13 Mei 2019, dimuat juga secara daring di https://bit.ly/3v4lAWP.

[40] *Ibid.*

[41] *Ibid.*

paling banyak menyedot informasi pribadi pengguna, yakni hingga 79%.[42] Beberapa informasi yang diambil antara lain riwayat pembayaran, lokasi, info kontak, riwayat pencarian, dan informasi keuangan.

Menurut Saputri dalam wawancaranya dengan Detik, data-data itu dipakai oleh pengiklan untuk mengisi algoritma di platformnya, untuk melakukan personalisasi periklanan.[43] Semakin jelas profil data-data yang dikumpulkan akan semakin spesifik populasi target yang bisa ditemukan. Sementara, berbeda dengan perusahaan raksasa seperti Facebook dan Google yang menambang pendapatan dari periklanan pada platformnya langsung, perusahaan-perusahaan yang lebih kecil memanfaatkan penjualan data untuk mendapat insentif dari pihak ketiga. Malgieri dan Custers menyebut data seperti identitas pribadi individu, dalam format zip, memiliki harga jual rata-rata sebesar US$ 50 sen.[44] Angka tersebut dapat meningkat ketika data telah diolah terstruktur dalam format set data.[45] Karena nilai jualnya yang tinggi, penjualan juga tidak hanya terjadi secara legal. Jual beli data pribadi yang ilegal di *dark web*—istilah untuk situs-situs yang hanya bisa diakses lewat konfigurasi perangkat tertentu, jadi masalah turunan.

Tahun 2019 lalu, polisi menciduk seseorang berinisial C (32 tahun) karena menjual data nasabah dan data kependudukan melalui website *temanmarketing.com.*[46] Bahkan jumlah data yang didapatkannya mencapai jutaan: mencakup puluhan ribu nama lengkap, alamat, nomor telepon seluler, jutaan Nomor Induk Kependudukan (NIK), enam puluh ribu nomor kartu kredit, serta data pribadi lainnya. Data tersebut pun dijual mulai dari Rp 250 ribu hingga Rp 20 juta. Sedang pada 2020, salah satu *marketplace* terbesar di Indonesia, Tokopedia, ramai diberitakan mengalami kebocoran data setelah 91 juta data akun konsumennya dijual.[47] Baru-baru ini kejadian sama berulang, tapi kini kebocoran ditengarai berasal sistem data milik BPJS Kesehatan. Tak tanggung-tanggung, kali ini 279 juta data WNI dijual secara ilegal. Beberapa preseden ini adalah kasus yang kebetulan terlaporkan. Ini menunjukan betapa data merupakan komoditas emas yang paling diminati.

Selain diperjualbelikan, nilai ekonomi langsung dari data juga didapatkan dari hak-hak hukum turunannya. Sebagai sebuah aset kebendaan, data berikut servernya bukan tidak mungkin dijadikan jaminan hutang. Hal ini karena data, oleh hukum, diperlakukan sebagai hak kebendaan, dan hukum perdata mengonstruksikan tiap-tiap harta kekayaan milik seseorang dengan sendirinya menjadi jaminan umum bagi tiap-tiap perikatan hutang

---

[42] Andrea Lidwina, "Facebook, Medsos yang Kehilangan Kepercayaan Publik Tertinggi Persentase Hilangnya Kepercayaan Publik pada Perusahaan (2018)", *katadata.co.id*, 29 Januari 20201, diakses dari https://bit.ly/3ipwaF5.

[43] Soraya Novika, "Marak Kasus Jual Beli Data Pribadi, Dijual Ke Mana?", *detik.com*, 20 November 2020, diakses dari https://bit.ly/3ze6Zvd.

[44] Gianclaudio Malgieri, 'Pricing Privacy – the right to know the value of your personal data', *Computer Law & Security Review: The International Journal of Technology and Law Practice,* Vol. 34, Issue 2, (April 2019): 289-303.

[45] *Ibid.*

[46] Adi Briantika, "Polisi Tangkap Penjual Data Nasabah dan Kependudukan", *tirto.id*, 15 Agustus 2019, diakses dari https://bit.ly/34XCvQ4.

[47] CNN Indonesia, "Penelusuran 91 Juta Data Bocor Tokopedia, Dijual Rp74 Juta", *cnnindonesia.com*, 3 Mei 2020, diakses dari https://bit.ly/3w72Wi2.

yang dimilikinya.[48] Seumpama *Facebook* memiliki sejumlah hutang pada Bank ABC: segala aset miliknya baik fisik (misal, server) maupun digital (dataset seluruh penggunanya) secara hukum jadi jaminan bagi debitur dan ketika gagal bayar asset jaminan itu bisa beralih milik. Atau, dalam rezim jaminan khusus, data sebagai benda bergerak bisa digadaikan. Hal ini lantas memunculkan pertanyaan: dapatkah pihak penerima jaminan gadai itu nantinya menggunakan data-data yang berada di bawah penguasaannya tersebut mengingat ada faktor privasi pihak lain yang melekat dalam data-data itu. Praktik penggadaian data yang belakangan disebut ini rasanya hampir tidak pernah dilakukan oleh perusahaan pengelola sistem elektronik yang notabene padat dukungan modal. Namun, melihat preseden kasus penjualan data secara ilegal yang marak, fenomena penjaminan itu bukan tidak mungkin terjadi kedepannya.

2.3.2. Nilai Ekonomi Tidak Langsung

Nilai ekonomi tidak langsung dari data terletak dari manfaat data sebagai penunjang aktivitas produksi. Meski pada dasarnya data (mentah) saja sebenarnya tidak punya manfaat ekonomis yang signifikan, namun ketika diproses jadi informasi data seketika punya nilai guna. Sebagaimana telah disebut sebelumnya, kumpulan data pada skala dan volume yang besar akan membentuk *big data*, dan pada fase itu manfaat praksis dari data meluas meliputi juga, misalnya, (1) sebagai dasar untuk membuat keputusan; (2) sebagai dasar perencanaan, (3) sebagai acuan implementasi suatu kegiatan, (4) sebagai bahan evaluasi. Keempatnya memang tidak secara langsung memberi keuntungan moneter, tapi ketika diterapkan bisa jadi modal *know-how* yang membantu mengefisiensikan proses produksi lagi meningkatkan prospek penjualan. Perusahaan raksasa seperti Facebook, Google, Instagram memanfaatan *big data* yang mereka miliki untuk menjual layanan periklanan dan layanan pemasaran terprofil bagi pihak ketiga. Facebook, misalnya, pada tahun 2015 memiliki total keuntungan sebesar USD 17.93 miliar yang mayoritasnya berasal dari kegiatan periklanan. Pada tahun itu, total pengguna Facebook kurang lebih 1,59 miliar; maka secara rata-rata dapat dihitung, dari tiap-tiap penggunanya, platform buatan Zuckerberg cs itu menghasilkan sekitar USD10 keuntungan per periklanan tiap tahunnya atau sekitar satu dolar per bulan.[49]

Utamanya kegunaan *big data,* dalam konteks aktivitas ekonomi digital, adalah untuk memudahkan identifikasi demografi. Menurut Edmon, sekarang ini perusahaan rutin membayar ribuan dolar untuk mendapatkan informasi pribadi mengenai pelanggan perusahaan lain; oleh pembelinya, informasi tersebut akan membantu mereka dalam membuat strategi pemasaran sehingga dapat mengurangi biaya pemasaran karena produk dapat langsung ditawarkan kepada orang berdasarkan minat, kesukaan dan kepribadian mereka yang terungkap dalam informasi pribadinya.[50] Artinya, berbekal data konsumen yang terolah, perusahaan dapat membaca pola-pola pemasaran, permintaan dan penawaran. Bagi perusahaan, basis data akan membantu pemasaran menjadi tepat sasaran sekaligus di sisi lain mengefisiensi berbagai ongkos yang tak perlu. Dan, salah satu pemrosesan

[48] Pasal 1131 KUHPerdata: "Semua kebendaan si berutang, baik yang bergerak maupun yang tidak bergerak, baik yang sudah ada maupun yang baru akan ada di kemudian hari, menjadi tanggungan untuk segala perikatan perseorangan."

[49] Malgieri, 'Pricing Privacy..., hlm. 298.

[50] Makarim, *Pengantar Hukum Telematika…,* hlm. 185.

informasi untuk mengetahui temuan-temuan itu dilakukan dengan bantuan komputasi kecerdasan buatan.

Seiring perkembangan aktivitas ekonomi digital, lalu lintas pertukaran data menjadi semakin cepat. Hal ini tak lepas dari meningkatnya konsumsi *e-commerce* masyarakat Indonesia. Menurut Kemp, sampai 2019 saja, setidaknya ada 107 juta masyarkat Indonesia yang berbelanja lewat *e-commerce*, angka itu sudah menyentuh 40% dari total populasi Indonesia.[51] Di balik statistik itu, terdapat kumpulan data demografi konsumen yang mampu diolah untuk memperluas pemasaran sekaligus meningkatkan penjualan. Menurut McLean, algoritma dapat mempelajari aktivitas toko online untuk melihat dinamika pasar, semisal, bagaimana harga produk semestinya ditetapkan, pola konsumsi normal, tingkat penawaran dan permintaan terakhir. Tetapi mereka (kecerdasan buatan) juga dapat secara tidak sengaja "berinteraksi" dengan program lainnya terus menerus untuk mengawasi penetapan harga dari penjual lain dan mempelajari harga yang pas di pasar.[52] Dari situ, lanjut McLean, mereka mampu belajar bahwa cara-cara tersebut adalah hal yang terbaik untuk mencapai tujuan memaksimalkan keuntungan. Karakter robotik itu diterapkan pada industri perhotelan dan pariwisata, dan belakangan telah ramai diaplikasikan pada pasar modal atau pasar uang.

Bagi perusahaan *marketplace*, database yang berisikan informasi konsumennya merupakan aset strategis yang dapat di-valuasi tak terkecuali sebagai penyertaan saham. Konsekuensinya, ketika terjadi aksi korporasi seperti merger atau akuisisi, kepemilikan atas data juga beralih. Kasus merger antara dua perusahaan *unicorn* baru-baru ini, yaitu, Gojek (PT. Aplikasi Karya Anak Bangsa) dan Tokopedia (PT. Tokopedia), menyisakan isu penting seputar perlindungan data pribadi konsumen. Sebab, pasca penggabungan itu, data konsumen Gojek dengan sendirinya jadi terakumulasi dengan data konsumen Tokopedia untuk dimiliki bersama entitas usaha baru yang dibentuk (GoTo). Ini jadi masalah sebab tak semua konsumen Gojek adalah pengguna Tokopedia, begitu pun sebaliknya. Penyatuan kedua platform jadi satu wadah berpotensi melanggar asas 'otorisasi data' karena dalam skenario itu perusahaan bisa saling pakai atas data-data tersebut, padahal pemilik data bisa saja tidak menghendaki datanya direkam oleh salah satu dari kedua entitas tadi. Dengan kata lain, konteks tujuan spesifik dari pengumpulan dan pembatasan penyimpanan atas data berpotensi besar terlanggar.

2.4. Aspek Hukum Publik dari Data

Senada tapi tak seirama dengan para pelaku sektor privat, penyelenggara negara juga membutuhkan data-data pribadi masyarakat sebagai penunjang kegiatannya. Bedanya, jika sektor privat memanfaatkan data berdasarkan motif akumulasi keuntungan, sektor publik membutuhkan data lebih banyak untuk kepentingan penyelenggaraan fungsi pemerintahan. Prinsipnya, penyelenggaraan pemerintahan yang baik salah satunya harus akuntabel dan transparan sehingga kebutuhan akan data-data akurat semakin krusial karena bisa menyangkut hajat hidup orang banyak. Idealnya berbagai keputusan pemerintah dalam

---

[51] Simon Kemp, 'Digital 2020: Indonesia', *datareportal.com*, 18 February 2020, diakses dari https://datareportal.com/reports/digital-2020-indonesia.

[52] Graeme McLean, "Algoritma bantu pelaku bisnis online untuk tetapkan harga yang tinggi", theconversation.com, 18 Maret 2019, diakses dari https://bit.ly/3g4PyWe.

rangka kebijakan haruslah berbasis riset dan bukti data sehingga bukan hanya dapat dipertanggungjawabkan dalam tataran ilmiah, tapi juga mendukung terciptanya sistem teknokratis agar segala keputusan tidak spekulatif dan berujung merugikan publik.

Meski begitu, tantangan yang selama ini dihadapi di sektor pelayanan publik justru muncul karena terlalu otoritas terlalu banyak data: Kementerian yang satu punya data versinya sendiri dan kadang kala tidak sejalan dengan data temuan otoritas lainnya. Tidak adanya kesatuan data jadi penghambat dalam pengambilan-pengambilan keputusan penting di samping turut menambah beban untuk penyimpanan data. Beberapa upaya dilakukan untuk menyiasati persoalan sebelumnya, salah satunya dengan membuat kebijakan Satu Data yang diteken lewat Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres SDI) untuk mendorong terciptanya pusat data yang terpadu, mutakhir, bisa dipertanggungjawabkan, dan mudah dibagipakaikan.[53]

Relasi antara data dan penyelenggaraan negara terlihat pada aktivitas sederhana seperti pencatatan sipil. Data-data penduduk senantiasa dikelola dan disimpan untuk kepentingan administrasi kependudukan sehingga sewaktu dibutuhkan, baik individu maupun otoritas dan untuk kepentingan apapun itu, aktivitas bisa berjalan dengan bekal data-data dimaksud. Misalnya, pada sektor perpajakan, data pribadi seperti riwayat keuangan nasabah penyimpan di bank penting untuk mendeteksi ketaatan seseorang atas pajak. Direktorat Jenderal Pajak dapat meminta akses bagi bank BUMN untuk melacak riwayat pajak seseorang yang diduga bermasalah, dalam hal kepentingan perpajakan.[54] Negara juga membutuhkan data-data umum akurat untuk mengukur atau mengevaluasi kebijakannya. Semisal, untuk menentukan tingkat Produk Domestik Bruto (PDB) negaranya sebagai batu ukur pertumbuhan ekonomi—meski ada banyak perdebatan tentang penggunaan formula itu.[55] Kumpulan data pribadi, dalam kaitannya dengan aktivitas masyarakat, juga diperlukan guna merumuskan berbagai program dan rencana pembangunan ke depan: untuk mendeteksi demografi populasi, sebaran dan jangkauan komoditas pokok, besarnya serapan tenaga kerja.

Sebagian besar data publik yang bersifat statistik-strategis dikumpulkan lewat otoritas yang mengurusi kegiatan statistik, seperti Badan Pusat Statistik (BPS)[56] atau oleh lembaga lainnya dalam ranah fungsi pendataan tertentu. Dalam kerja-kerjanya, BPS bertanggung jawab untuk mengolah data dan metadata menjadi teragregat sehingga keluarannya bisa jadi rujukan informasi dalam mengambil kebijakan. Khusus hasil olahan data-data teragregat yang dikeluarkan BPS sendiri merupakan informasi publik yang dapat diakses siapa saja kecuali yang bersifat konfidensial atau menyangkut keamanan negara. Dalam tataran fungsi transparansi pula, data dibutuhkan untuk menjamin akses publik atas informasi yang jadi ritus penting demokrasi. Hal ini diatur dalam Undang-Undang tentang

---

[53] Indonesia, *Peraturan Presiden tentang Satu Data Indonesia,* Perpres Nomor 39 Tahun 2019, LN No. 112 Tahun 2019.

[54] Indonesia, *Peraturan Pemerintah Pengganti Undang-Undang tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan*, Perppu Nomor 1 Tahun 2017, LN No. 95 Tahun 2017, TLN No. 6051, Pasal 2 ayat 1 jo. Pasal 4.

[55] Kajian menarik tentang penolakan atas digunakannya PDB sebagai tolok ukur pertumbuhan, lihat: Lorenzo Fioramonti, Lisa Soerjadinata (trans), *Problem Domestik Bruto: Sejarah dan Realitas Politik di Balik Angka Pertumbuhan Ekonomi,* (Jakarta: Marjin Kiri Publisher, 2017).

[56] Lihat: Badan Pusat Statistik RI, "Tentang BPS: Tugas, Fungsi dan Kewenangan", *bps.go.id*, (n.d.). Tautan: https://bit.ly/3w5j0B7.

Keterbukaan Informasi Publik.[57] Yang dimaksud 'Informasi Publik' adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik.[58] Di situ data dibagi jadi dua jenis berdasarkan keterbukaan aksesnya, yakni data terbuka dan data tertutup (dikecualikan). Data yang bersifat tertutup menyangkut kegiatan-kegiatan seperti intelijen, kepentingan keamanan-pertahanan negara, informasi kemampuan kemiliteran, serta data yang pembukaannya berpotensi merugikan privasi perorangan.[59] Pengelolaan data pribadi oleh negara juga penting menyangkut pengendalian sosial, penegakan hukum, dan pertahanan dan keamanan negara. Dalam konteks pengendalian, proses datafikasi diperlukan guna, misalnya, memetakan sebaran risiko konflik sosial atau melacak keberadaan orang tertentu. Ringkasnya, fungsi sepenting intelijen tentu tidak bisa berjalan tanpa didukung adanya data dan informasi yang akurat. Namun, yang paling kontroversial adalah penggunaan data untuk kepentingan surveilans massa. Beberapa negara maju seperti Inggris Raya tak lama lalu dinyatakan oleh Komisi Uni Eropa telah melanggar hak privasi warga lantaran menerapkan kebijakan surveilans massa dengan alibi keamanan nasional.[60]

2.4.1. Otoritas yang Mengurusi Perlindungan Data Pribadi di Indonesia

Belum adanya satu payung hukum utama perlindungan data pribadi berkonsekuensi pada belum terbentuknya satu otoritas khusus yang spesifik mengemban tugas mengurus perlindungan data pribadi. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik sebagai rujukan utama regulasi tata kelola sistem elektronik pun masih melepaskan pengaturan tersebut untuk diregulasi secara mandiri (*self-regulation)* oleh penyelenggara sistem elektronik,[61] dengan beberapa standar keamanan dan keandalan turunan yang ditetapkan oleh lembaga sertifikasi independen.

Setidaknya ada tiga kementerian/lembaga yang secara kewenangan beririsan: *Pertama*, Kementerian Komunikasi dan Informasi (Kominfo) berwenang dalam ranah pengelolaan informasi dan komunikasi, termasuk informasi elektronik.[62] Dalam lalu lintas informasi, Kemkominfo juga berwenang untuk melakukan *take down* atas konten dan pemutusan akses informasi dalam hal konten-konten yang beredar di internet meresahkan dan/atau mengandung disinformasi. Pelaksanaan tugas itu dijalankan oleh unit kerja

---

[57] Indonesia, *Undang-Undang tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008, LN No. 61 Tahun 2008, TLN No. 4846.

[58] *Ibid.*, Pasal 1 angka 2.

[59] *Ibid.*, Pasal 17.

[60] Hugo Miller, "UK's Data Spying After Snowden Violated Privacy Rights", *bloomberg.com*, 25 Mei 2021, diakses dari https://bloom.bg/3ghnHkw.

[61] Lihat: Pasal 10 UU ITE jo. Pasal 1 angka 27 PP PSTE; Permenkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Objek yang disertifikasi bukan dokumen atau informasi elektronik melainkan kemampuan pelaku usaha menyelenggarakan sistem elektronik;

[62] Lihat: "Tugas dan fungsi", *kominfo.go.id*, (n.d.), diakses dari https://www.kominfo.go.id/tugas-dan-fungsi

Direktorat Aplikasi Informatika yang berada dalam struktur Kominfo.[63] Sebelumnya, ada Badan Regulasi Telekomunikasi Indonesia (BRTI) yang dibentuk berdasarkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang punya tugas berkoordinasi dengan Menkominfo dalam menyelenggarakan pengaturan di bidang keamanan telekomunikasi. Tapi, BRTI dibubarkan oleh Presiden Jokowi tahun 2019. Pasca UU ITE memperkenalkan konsep standarisasi sistem elektronik, otoritas seperti Badan Standarisasi Nasional (BSN) juga muncul dalam percaturan karena berwenang melakukan penilaian terhadap keamanan sistem informasi berdasarkan SNI ISO/IEC 27001,[64] meski sifatnya cenderung pasif atau berdasarkan inisiatif pemohon.

Kedua, dalam konteks keamanan siber, ada otoritas khusus, yaitu, Badan Sandi dan Siber Negara (BSSN). Presiden Jokowi membentuk BSSN lewat Peraturan Presiden Nomor 53 Tahun 2017 sebagaimana telah diubah dalam Perpres Nomor 113 Tahun 2018. Masalah proteksi atas data pribadi sebenarnya sangat erat kaitannya dengan urusan keamanan siber, namun, tidak jelas limitasi kewenangan antara lembaga baru ini dengan Kemenkominfo. Padahal, secara fungsi, BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber.[65] Meski demikian, patut menjadi catatan mengapa sampai dengan hari ini peran BSSN sebagaimana yang diharapkan belum terlihat; belum ada produk regulasi menonjol yang diterbitkan Lembaga ini sementara anggaran yang dikeluarkan negara untuk mendukung kerja-kerja BSSN terbilang cukup besar, dengan alokasi pagu anggaran sebesar Rp 1,5 Triliun untuk periode 2021.[66] Terlihat dari situs BSSN, sebenarnya lembaga ini telah membuat beberapa rancangan peraturan, salah satunya perihal sertifikasi keamanan situs, namun persoalan tarik-ulur kewenangan yang tumpang tindih dengan Kemkominfo jadi salah satu kendala.[67]

Ketiga, otoritas berbeda muncul ketika berbicara tentang dunia perbankan dan jasa keuangan. Otoritas Jasa Keuangan (OJK) jadi regulator dalam hal perlindungan data/informasi konsumen perbankan atau jasa keuangan. Misalnya, Pasal 2 POJK Nomor 1/POJK.07/2013 mengadopsi aturan terkait kerahasiaan dan keamanan data/informasi konsumen, salah satunya menyebutkan tentang data-data apa saja yang harus dijaga oleh penyedia jasa keuangan. Pemisahan kewenangan perlindungan data elektronik di ranah perbankan memang tak cuma terjadi di Indonesia. Amerika Serikat, misalnya, meletakkan tanggung jawab perlindungan data pribadi nasabah juga di bawah kendali otoritas pengawas keuangan. Meski begitu, peran aktif OJK yang diharapkan dalam melindungi data pribadi konsumen jasa keuangan juga dirasa belum maksimal. Terlihat, salah satu

---

[63] Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 6 Tahun 2018 Tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika Republik Indonesia.

[64] SNI ISO/IEC 27001:2013 adalah standar Sistem Manajemen Keamanan Informasi yang ditetapkan oleh BSN yang menjelaskan panduan dan syarat-syarat untuk membuat, menerapkan, melaksanakan, mengelola risiko, memelihara dan mendokumentasikan Sistem Manajemen Keamanan Informasi. Standar ini merupakan adopsi dari ISO/IEC 27001:2013 yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC).

[65] Pasal 2 Peraturan Presiden Nomor 53 Tahun 2017 tentang Satu Data Indonesia.

[66] BSSN, 'Raker dengan Komisi I DPR RI, BSSN: SNKS RI sebagai Langkah Nyata Kehadiran Negara di Ruang Siber', *bssn.go.id,* 3 Februari 2021, diakses dari https://bit.ly/2SKppTi.

[67] Steffani Dina, "Tumpang Tindih Tugas Badan Siber dengan Lembaga Lain", *kominfo.go.id,* 9 Januari 2018, diakses dari https://bit.ly/2RCjPCs.

kasus-kasus pelanggaran data pribadi yang paling sering dilaporkan menurut Lembaga Bantuan Hukum (LBH) Jakarta, justru datang dari sektor ini karena perusahaan *fintech* atau pinjaman online seringkali menyingkap informasi pribadi nasabah untuk kepentingan penagihan.[68] Salah satu kasus terakhir bahkan sampai memakan korban jiwa lantaran teror tak berkesudahan yang dilakukan oknum penagih.[69] Tak hanya OJK, Kemenkominfo juga punya tanggung jawab perihal penertiban pinjaman online ilegal yang menjadi salah satu penyebab maraknya pelanggaran data pribadi. Di luar ketiga otoritas sebelumnya, ada otoritas penegak hukum seperti kepolisian dan kejaksaan, yang juga jadi aktor penentu. Polri, misalnya, memiliki unit tersendiri yang mengurusi tentang kejahatan siber. Sayangnya, rincian prestasi yang diukir masih terbilang nihil. Kasus-kasus yang ditindaklanjuti masih terbatas pada kasus yang berdimensi tindak pidana ekonomi, semisal, pembobolan kartu kredit nasabah, namun belum mampu mengungkap kasus-kasus umum seperti jual-beli data pribadi illegal di mana kerugian materiil belum muncul.

2.5. Pentingnya Pelindungan Data dan Informasi Pribadi: Privasi, Keamanan dan Otonomi Individu

Data dan/atau informasi yang terkandung di dalamnya adalah bagian dari identitas seseorang. Karena itu, data bisa jadi penting karena menyangkut otonomi kebebasan seseorang. Pertimbangkan, contohnya, seorang penjahat yang cukup berbekal data-data umum, bisa melakukan *cloning* untuk melakukan penipuan lewat ponsel. Atau, berbekal informasi alamat tinggal, seseorang dapat melakukan teror ke tempat seseorang tinggal. Belum lagi faktor risiko lain mengingat Indonesia, dalam catatan Kaspersky, jadi salah satu target serangan siber *phishing*[70] paling empuk.[71] Oleh karena itu, memproteksi data, dengan kata lain, sama dengan memproteksi bagian fundamental dari hak asasi manusia.

Menelisik ke belakang, Warren dan Brandeis pertama kali mengangkat dan mengonseptualisasikan privasi atas informasi pribadi sebagai sebuah hukum dalam tulisannya di *Harvard Law Review* pada 1980.[72] Dasarnya, ketika itu konsep perlindungan hukum atas privasi masih terkonsentrasi pada hal-hal atau kerugian yang sifatnya fisik.[73] Warren berargumen, sejalan dengan diakuinya dimensi spiritual (intelektual, sensasi dan emosi, reputasi) dari otonomi seseorang, privasi perlu mengakui pula hal-hal implisit sebagai bagian di dalamnya.[74] Ini tak bisa dilepaskan dari meningkatnya aktivitas industri pers *vis-a-vis* otonomi pribadi, di mana informasi tentang kehidupan seseorang cenderung bebas dikapitalisasi dan dipublikasi walau bermuatan keliru (*wrongful publication*).[75]

---

[68] Vincent Fabian Thomas, "Pinjaman Online Kembali "Makan Korban", OJK Diminta Tak Bungkam", *tirto.id,* 12 Februari 2019, diakses dari https://bit.ly/3x6ifYz.

[69] Yayu Agustina Rahayu, "OJK Telusuri Kejadian Sopir Taksi Bunuh Diri Akibat Pinjaman Online', *merdeka.com,* 13 Februari 2019, diakses dari https://bit.ly/3cpjKcf.

[70] *Phising* adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan.

[71] CNN Indonesia, "Indonesia Jadi Salah Satu Negara Target Phishing', *cnnindonesia.com*, 1 Oktober 2019, diakses dari https://bit.ly/350GfAf.

[72] Samuel Warren dan Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, (Desember 1980): 193-220.

[73] *Ibid.*, hlm, 193.

[74] *Ibid.*, hlm. 194.

[75] *Ibid.*, hlm 196.

Eskalasi tersebut menimbulkan potensi cedera atas privasi seseorang, meski tak melulu bernilai materiil, tapi juga immaterial, misalnya dalam bentuk hilangnya kenyamanan diri.

Lebih jauh, menurut Bernal, seiring internet semakin terintegrasi ke dalam kehidupan kita, otonomi *online* menjadi semakin signifikan. Sejauh mana aktivitas online kita 'bebas' dalam banyak hal merupakan cerminan dari sejauh mana kehidupan offline kita bebas, dan keduanya menjadi terkait erat.[76] Jika aktivitas online kita dibatasi, dikontrol, atau terlalu dipengaruhi, akibatnya aktivitas 'kehidupan nyata' kita dapat dibatasi, dikontrol, dan terlalu dipengaruhi. Inilah sebabnya mengapa privasi sebagai pelindung utama otonomi daring, penting. Bukan hanya tentang internet, ini tentang hidup kita secara keseluruhan.[77] Terkait hal ini, Joinet, sebagaimana dikutip oleh Tsanacas menyebut: *"Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantages over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows."*[78]

Lebih lanjut, menurut Direktur Eksekutif SAFENet, Damar Juniarto, ada tiga motif pelanggaran data pribadi yang umum terjadi di Indonesia, yaitu ekonomi, politik, dan ancaman.[79] Argumentasi pertama yang kerap diutarakan terkait kerahasian data pribadi adalah terkait ancaman siber. Serangan siber seperti peretasan akun, pembobolan akun rekening, dan kejahatan sejenis diawali dengan adanya penggunaan data pribadi secara melawan hukum, baik itu berupa kebocoran ataupun kelalaian pemilik data. Dalam konteks ekonomi, sebagaimana telah dijelaskan di bagian sebelumnya, aktivitas jual-beli data pribadi secara legal dan ilegal kerap terjadi imbas dari potensi keuntungan yang besar. Dalam konteks politik, data pribadi penting untuk memonopoli peta kekuasaan, juga biasanya disebabkan adanya kebijakan surveilans dan alasan proteksionisme atas kepentingan nasional.

Selain itu, aspek fundamental yang menjadi basis kebutuhan perlindungan adalah tentang kenyamanan hidup dan privasi. Privasi merupakan hak asasi manusia di bidang sipil yang diatur dalam *International Covenant on Civil and Political Rights* sebagaimana telah diratifikasi Indonesia lewat Undang-Undang Nomor 11 Tahun 2005. Dalam konteks data pribadi, privasi meliputi hak untuk bebas dari gangguan, hak untuk tetap mandiri, dan hak untuk mengontrol peredaran dari informasi tentang seseorang, dalam hal pengumpulan, penyimpanan, penggunaan, dan penyingkapan data.[80] Seiring meningkatnya penyalahgunaan data, kewajiban penghormatan atas privasi daring meningkat dari ranah etis menjadi sebuah kewajiban hukum. Dalam kaitannya dengan itu, menurut Edmon, pada praktiknya seringkali terjadi kekeliruan dalam pengertian tentang privasi, kerahasiaan, dan keamanan.[81] Privasi dapat digolongkan ke dalam kerahasiaan tapi secara konsep ia lebih

---

[76] Bernal, *Internet Privacy Rights*..., hlm. 12

[77] *Ibid.*

[78] Demetri Tsanacas, 'The Transborder Data Flow in the New World Information Order: Privacy or Control', *Review of Social Economy,* Vol. 43, No. 3, 357-370, Taylor and Francis Group: 1985, doi: 10.1080/00346768500000037, hlm. 359.

[79] Cindy Mutia Anur, "Pelanggaran Data Pribadi di Indonesia Diperdagangkan Hingga Ancaman", *katadata.co.id*, 2 Agustus 2019, diakses dari https://bit.ly/34XOc9w.

[80] Alan F. Wenstin, hlm. 13.

[81] Edmon, *Pengantar Hukum Telematika*..., hlm. 162-163.

luas dari sekedar kerahasiaan. Kerahasiaan sendiri hanya dipermasalahkan setelah informasi diperoleh oleh pengguna data yang kemudian menimbulkan pertanggungjawaban atas keamanan penyimpanannya.[82] Di situ, timbul hubungan kepercayaan antara *data subjects* dan *data users*, yang menimbulkan suatu kewajiban pemeliharaan dan jaminan atas kerahasiannya, dari penyingkapan yang tidak sah kepada pihak ketiga.[83]

Di Indonesia sendiri, proteksi yang diberikan negara dirasa belum memadai. Contohnya nyatanya, ketika mengunduh aplikasi, konsumen sering melihat klausul dalam syarat dan ketentuan yang melampaui batas. *User* sering diminta untuk memberi otorisasi aplikasi ke dalam sistem gawai semisal galeri, kontak, pesan singkat, *email*, kamera, mikrofon bahkan konfigurasi perangkat.[84] Salah satu yang paling sering dilaporkan adalah aplikasi-aplikasi *financial technology* sejenis pinjaman online. Bukan hanya sekedar untuk verifikasi, penerobosan sistem itu sering kali digunakan oknum *collector* untuk meneror debitur. Celah ini jadi pintu masuk bagi pengumpulan data yang kerap tidak diketahui oleh pemiliknya. Ketika kemudian diketahui ada tindakan penyalahgunaan data, pemilik data pun akan merasa kesulitan dalam melakukan pelacakan sampai mana data-data pribadinya telah dipindahtangankan. Di sisi lain, pengelola aplikasi cenderung bersikap "*take it or leave it*", artinya, jika tidak setuju dengan syarat dan ketentuan penggunaan data pribadi, maka calon konsumen tidak perlu menggunakan aplikasinya.

Alasan yang mendasari semua ancaman ini adalah terdapat konflik dan perbedaan kepentingan terkait perlakuan atas data. Prioritas individu, pemerintah, dan bisnis berbeda, dan meskipun kepentingan dapat, dan memang, sesuai pada banyak poin (sekalipun ketiganya mendapat manfaat dari kemakmuran dan keamanan, misalnya), mereka tidak selalu cocok. Perbedaan kepentingan ini membuat pengguna (pemilik data) seringkali dikorbankan.[85] Dalam istilah yang sangat luas, pemerintah memiliki kepentingan keamanan dan stabilitas, yang terkadang dapat mengesampingkan keinginan dan kebutuhan individu atas privasi dan otonomi. Bisnis, di sisi lain, hanya memiliki satu minat utama: menghasilkan uang. Sektor privat dan pemerintah dapat mendukung kepentingan tersebut dengan mengumpulkan lebih banyak data; dengan mengetahui lebih banyak tentang orang dan aktivitas, minat, dan sebagainya. Kepentingan tersebut sah dan pada prinsipnya tidak bertentangan dengan hak dan kebutuhan individu. Namun, individu juga memiliki kepentingan yang kuat akan keamanan yang disediakan oleh pemerintah dan sektor bisnis yang berkembang. "Sering kali ada ketegangan yang dapat dan memang meluas ke dalam konflik yang sesungguhnya", sebut Bernal.[86] "Ketika bisnis atau pemerintah bertindak terlalu jauh, individu dapat dan memang menderita, dan terkadang juga memberontak. Itulah alasan utama gagasan tentang hak privasi internet yang dikemukakan di sini. Dengan mengartikulasikan hak-hak ini, tidak hanya individu yang dapat dibantu mengungkapkan keprihatinan mereka dan mengedepankan alasan mereka

---

[82] *Ibid.,* hlm. 163.
[83] *Ibid.*
[84] "Waspada Aplikasi Pinjam Uang Ambil Data Kontak dan Baca SMS di Ponsel", *kumparan.com*, 28 Juni 2018, diakses dari https://bit.ly/2RGB4mc.
[85] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy,* (London: Cambridge University Press, 2014), hlm. 14.
[86] *Ibid.*

untuk privasi, tetapi baik bisnis maupun pemerintah dapat menghindari melangkah terlalu jauh sejak awal.

Kehadiran prinsip-prinsip perlindungan data pribadi juga semakin krusial untuk meminimalisir penggunaan data yang tidak perlu. Sebab, pada banyak kasus, penyelenggara sistem elektronik kerap mengumpulkan data penggunanya secara berlebihan. Bukan hanya untuk mengkomodifikasi data-data lainnya, tapi juga, hasil dari pengolahan atas data-data itu kerap disodorkan kembali untuk mempengaruhi perilaku penggunanya, misalnya, untuk mendorong orang menjadi konsumtif. Hegemoni itu, sayangnya, terjadi tanpa disadari oleh korbannya. Aspek paternalistik dari pemanfaatan data ini menimbulkan eksploitasi baru yang bersifat laten sehingga diperlukan batasan-batasan sejauh mana data bisa dikumpulkan, berikut tujuan-tujuannya yang tidak boleh merugikan pemilik data pribadi.

2.6. Inisiatif Komunitas Internasional

Perkembangan privasi sebelumnya memunculkan inisiatif untuk mengonseptualisasikan perlindungan privasi data. Inisiatif perlindungan data pribadi sudah diawali sejak diinisiasikan dalam *OECD Guidelines on the Data Protection of Privacy and Transborder Flows of Personal Data* tahun 1980. Pada era tersebut, penggunaan teknologi informasi jelas belum semarak hari ini; di satu sisi risiko-risiko terhadap privasi mulai disadari, namun, dalam kerangka itu, filosofi yang diangkat masih berfokus pada upaya menunjang perdagangan bebas dengan semangat pemerataan globalisasi ekonomi. Hak-hak individu pemilik data, sebagai pihak terdampak dari aktivitas perdagangan, tertutup oleh isu perihal kepentingan ekonomi nasional. Kesepakatan dalam OECD tersebut ditindaklanjuti, salah satunya, oleh Uni Eropa dengan menciptakan Konvensi 108, satu tahun berselang.

Paralel dengan peningkatan penggunaan teknologi informasi, progres nyata dalam upaya proteksi di ranah operasional tersebut mulai terlihat dalam lima tahun ke belakang. Menurut Alvin Toh, ada beberapa perkembangan penting terkait proteksi atas data pribadi di level internasional dan regional dalam lima tahun ke belakang[87], diantaranya *APEC Cross-Border Privacy Rules* (2015), *European Union Guidelines on Data Protection Rules* (2018), *Convention 108+* (2018) dan *ISO 27701* (2019). Pertemuan APEC CBPR[88] menghasilkan kesepakatan model sertifikasi sistem bagi pelaku bisnis yang melakukan pengelolaan, pengumpulan, pemrosesan dan penggunaan data pribadi lintas batas negara. Pada intinya, perjanjian internasional ini menghasilkan prinsip-prinsip dasar berupa simplisitas, transparansi, biaya rendah, dan akuntabilitas terhadap APEC Economics.[89]

Dilanjutkan dengan *European Union (EU) Guidelines on Data Protection Regulation* (GDPR) tahun 2016. Meski bersifat regional, panduan ini menjadi salah satu yang paling banyak dirujuk dalam tata kelola data dan informasi. Hal tersebut dikarenakan GDPR memiliki keharusan bagi vendor pihak ketiga yang berelasi dengan pelaku usaha di

---

[87] Alvin Toh, 'Cross Border Trade and Regional Data Protection – An Operational Perspective', presentasi untuk Webinar Global Connect @SBF, "Cross-Border Trade & Data Flows", Singapura, 22 Juli 2020.

[88] Pertemuan ini merupakan kelanjutan dari APEC Privacy Framework yang disepakati dua puluh satu perwakilan Menteri anggota APEC bulan November 2004. Lebih jauh lihat: APEC, "Cross-Border Privacy Rules System: Policies, Rules, and Guidelines", (n.d.), diunduh dari https://bit.ly/3x3OFmz.

[89] *Ibid*, Artikel 49.

wilayah yurisdiksi Uni Eropa. Ada pula Convention 108+ tahun 2018[90], yang merupakan modernisasi dari Convention 108 tahun 1981 yang dibentuk Komisi Eropa. Konvensi ini telah diaksesi oleh beberapa negara non-Uni Eropa. Lalu, pada skala yang lebih luas lagi, ISO 27701 tahun 2019 menetapkan standar dalam bentuk *soft-law* terkait cara-cara sebuah organisasi mengumpulkan data dan mencegah penggunaan dan pembukaan data secara tidak terotorisasi. Dalam hal itu, berbeda dengan sedaftar perjanjian internasional sebelumnya yang inisiatif politik, standarisasi ISO 27701 bisa diaplikasikan oleh siapa saja.

Seluruh inisiatif tersebut bagaimanapun juga tidak cukup tanpa ditunjang oleh kerangka regulasi yang memadai di level nasional. Model sertifikasi keandalan sistem komputer yang diperkenalkan dalam APEC CBPR memang sebagian telah diadopsi Indonesia dalam UU ITE, meski demikian spesifik perihal penggunaan data pribadi belum banyak dibicarakan di level eksekutif. Pengesahan RUU Perlindungan Data Pribadi semakin urgen mengingat sejumlah agenda *Free Trade Agreement* (FTA) yang ditandatangani Indonesia di bidang kerja sama ekonomi digital mengarah pada keterbukaan platform digital, dan dengan sendirinya menambah faktor risiko mengingat kondisi pelindungan relatif rendah.[91]

[90] Council of Europe, *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, (June 2018), diunduh dari https://bit.ly/3g52sU7.

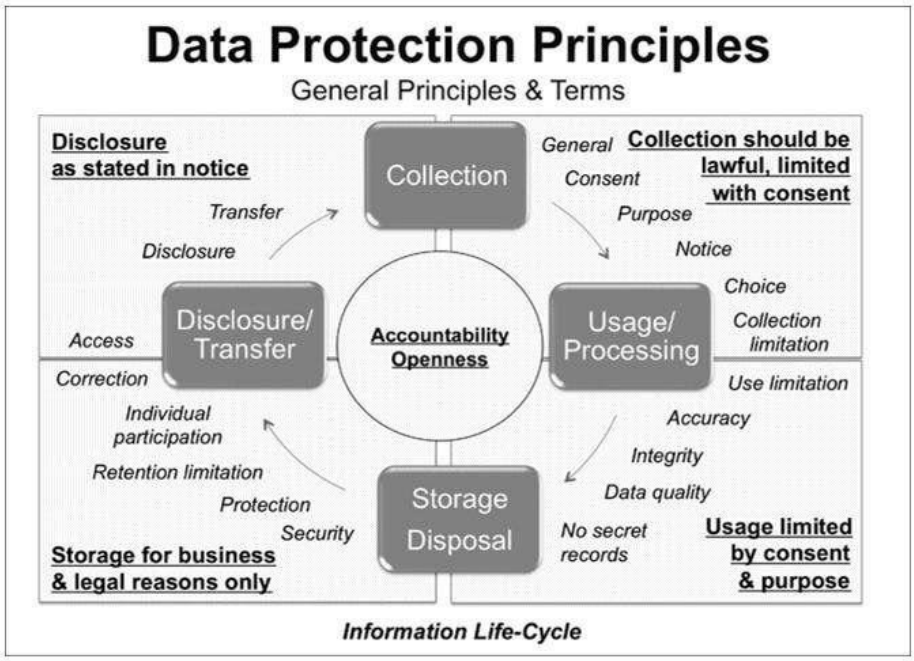
[91] Lihat: Indonesia for Global Justice, "Perlu Kebijakan Konsisten dalam Menghadapi Era Keterbukaan Platform Digital, *igj.or.id,* 6 Maret 2021, diakses dari https://bit.ly/3iw9yCK.

BAB 3
PERBANDINGAN KONSEP HUKUM PELINDUNGAN DATA PRIBADI

3.1. Prinsip-Prinsip Perlindungan Data Pribadi

Praktik lazim perlindungan atas data pribadi disusun berdasarkan siklus hidup informasi (*information life cycle*). Siklus tersebut terbagi menjadi pengumpulan (*collection*), penggunaan (*usage*), pembukaan (*disclosure*), dan penempatan (*storage*) atau disingkat dengan CUDS (Gambar 3.1.). Tiap-tiap tahap dalam siklus tersebut mensyaratkan perlakuan tertentu atas data maupun aksesnya sehingga tercipta perlindungan sebaik-baiknya. Kajian ini mengangkat tiga model pelindungan data pribadi yang dikenal, pertama di kawasan Uni Eropa, Amerika Serikat, dan Kanada. Perspektif Uni Eropa digunakan mengingat kawasan tersebut terbilang paling maju dalam konteks pengaturan PDP, sementara Amerika Serikat juga Kanada patut diperhitungkan karena menjadi negara asal mayoritas korporasi multinasional IT dunia.

Gambar 3.1.1 Konstruksi Siklus Hidup Data menurut GDPR



(Sumber: https://learn.lif.co.id/62101/)

3.2. GDPR Uni Eropa

Dalam konteks internasional, *best practice* yang paling banyak diadopsi adalah *European Union General Data Protection Rules* (GDPR). GDPR berlaku untuk tiap aktivitas 'pemrosesan' atas 'data pribadi', sebagian atau sepenuhnya, oleh pengendali data (*controller*) maupun prosesor, dengan cara otomatis yang merupakan bagian dari sistem pengarsipan (*filing system*) atau dimaksudkan untuk menjadi bagian dari sistem

pengarsipan.[92] 'Pemrosesan' berarti setiap operasi atau rangkaian operasi yang dilakukan pada data pribadi atau pada kumpulan data pribadi, baik dengan cara otomatis maupun tidak. Cakupan keberlakuannya membuat GDPR, meski secara *de facto* bersifat kebijakan regional, punya efek keberlakuan global—dikenal dengan sebutan 'Efek Brussel'.[93]

Dalam GDPR, menurut Bussche dan Voigt, pada dasarnya setiap perlakuan data akan dianggap sebagai pemrosesan; contohnya termasuk pengumpulan, pencatatan, pengorganisasian, penataan, penyimpanan dan penghapusan data.[94] Pemrosesan yang dimaksud mencakup pula secara manual (yang sepenuhnya dilakukan pengisian oleh manusia tanpa bantuan mesin/otomasi) dengan syarat bahwa data yang dimaksud akan diarsipkan ke dalam suatu sistem pengarsipan dan merupakan data terstruktur untuk kriteria spesifik.[95] Cakupan GDPR sengaja dibuat luas agar memastikan proteksi maksimal.

Lebih lanjut, dalam Artikel 4 GDPR, sebuah data dikategorikan sebagai 'data pribadi' ketika informasi yang tercakup berhubungan dengan pengenalan/identifikasi atau individu tertentu. Oleh karena itu, data bersifat pribadi jika identifikasi seseorang dimungkinkan berdasarkan data yang tersedia, artinya jika seseorang dapat dideteksi, secara langsung atau tidak langsung, dengan mengacu pada pengenal. Ini terjadi jika penugasan pada satu atau lebih karakteristik yang merupakan ekspresi dari identitas fisik, fisiologis, psikologis, genetik, ekonomi, budaya atau sosial.[96] Misalnya, nama seseorang, nomor identitas kependudukan, lokasi data, identitas daring (*IP address* dan/atau *cookies*).

Human Rights Watch, organisasi non-pemerintah pemantau perkembangan isu hak asasi manusia internasional, menjelaskan bahwa GDPR memberi masyarakat peningkatan pelindungan dari pengumpulan data yang tak perlu, penggunaan data dengan cara-cara yang tak diantisipasi sebelumnya, serta pembuatan keputusan algoritmis yang bias.[97] Di era digital dewasa ini, data pribadi secara intrinsik berhubungan dengan kehidupan pribadi dan hak asasi manusia seseorang; segala sesuatu yang dilakukan seseorang meninggalkan jejak digital yang dapat membeberkan informasi mendalam tentang pemikiran, keyakinan, pergerakan, asosiasi, dan kegiatan orang tersebut. Untuk itu, GDPR berupaya membatasi gangguan secara sewenang-wenang terhadap kehidupan pribadi seseorang yang dilakukan melalui data mereka, yang pada akhirnya turut melindungi hak asasi manusia dalam bentuk-bentuk lain.[98] Pemilik data dapat mengunduh dan melihat data yang dikumpulkan dari mereka, meminta koreksi, meminta agar data mereka dihapus dalam kasus-kasus tertentu, dan menarik persetujuan kelanjutan penggunaan data itu.

Selain itu, subjek pemilik data juga berhak menolak pemetaan profil atau *profiling* daring dan iklan bertarget, dan organisasi atau entitas kemudian harus

---

[92] Pasal 2 GDPR: "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

[93] Aoife White, "How the Brussels Effect Helps the EU Rule the World", *bloomberg.com*, 21 Maret 2020, diakses dari https://bloom.bg/3zgoyun.

[94] P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, (Springer International, 2017), hlm. 9.

[95] *Ibid*., hlm. 10.

[96] *Ibid.*, hlm. 11.

[97] Human Rights Watch, 'Peraturan Pelindungan Data Umum Uni Eropa', *hrw.org,* 6 Juni 2018, diakses dari https://www.hrw.org/id/news/2018/06/06/318734

[98] *Ibid.*

berhenti memproses data pribadi mereka kecuali apabila perusahaan dapat menunjukkan adanya "alasan berdasar dan meyakinkan" untuk melakukan pemrosesan data. Meski tak mendefinisikan apa yang dianggap sebagai "alasan berdasar dan meyakinkan," peraturan ini memang memberi hak mutlak bagi pengguna untuk menolak dan menghentikan pemasaran langsung melalui surel, panggilan telepon, maupun pesan teks.[99] Lalu, setelah data dikumpulkan, perusahaan harus lebih transparan dalam menyampaikan bagaimana data dibagikan dengan pihak lain. Dalam teorinya, ini berarti bahwa pengguna dapat mengetahui lebih lanjut tentang bagaimana pendekatan perusahaan terhadap *profiling* daring dan kemitraan dalam iklan bertarget, khususnya pihak-pihak yang menawarkan *web analytics*, periklanan, atau layanan media sosial.[100] Dalam implementasinya, GDPR sendiri mengusung tujuh prinsip dasar perlindungan data pribadi, antara lain:

3.2.1. Lawfulness, Fairness and Transparency

Prinsip legalitas, kepatutan, dan transparansi berlaku pada siklus pertama: perolehan dan pengumpulan data. Dalam wilayah pengumpulan data, ada beberapa isu yang penting yang terangkat, yakni, bagaimana suatu data dikumpulkan dan penggunaan data setelah pengumpulan. Prinsip terpenting pada saat data dikoleksi adalah keabsahan secara hukum (*lawfulness*); artinya, harus ada persetujuan (*consent)* dari pemilik data yang bersifat eksplisit.[101] Persetujuan itu dilakukan, misalnya, dengan menyediakan kolom ceklis syarat dan ketentuan (*terms and condition)* perihal kebijakan privasi yang dapat diakses oleh pengguna secara jelas dan dalam bahasa yang dimengerti, sebelum memutuskan untuk menggunakan suatu layanan. Lalu dilanjutkan dengan pemberian notifikasi atas data yang terkoleksi, lalu menyediakan pilihan alternatif bagi pengguna yang berkeberatan datanya dikumpulkan, serta adanya batas atau limitasi jenis data yang dikumpulkan. Artinya, tidak semua data bisa diambil oleh pengelola sistem elektronik.

Sementara dalam hal penempatan pengelola data wajib melaporkan ke pihak berwajib, dan semua pengguna harus diberitahu, apabila terdapat pembobolan data, yang kemungkinan besar mengakibatkan risiko tinggi terhadap hak dan kebebasan *data subject*.[102] Kewajiban itu menyangkut adanya akuntabilitas dan transparansi kondisi keamanan data yang dikendalikan oleh *data controller*.

3.2.2. Purpose Limitation

Pada siklus penggunaan data pribadi, operator harus terlebih dahulu menjelaskan tujuan spesifik (*purpose specification*) dari penggunaan data, serta menjelaskan bagaimana data pribadi seseorang digunakan, dibagikan, dan disimpan.[103] Sehingga, pada saat mendaftar akun untuk aplikasi yang akan digunakan, harus termuat keterangan akan digunakan untuk apa saja data user tersebut; dan tak hanya itu,

[99] *Ibid.*
[100] *Ibid.*
[101] Pasal 6 ayat (1) huruf a GDPR
[102] Pasal 33 dan 34 GDPR
[103] Pasal 13 GDPR

tujuannya pun harus pula bersifat relevan dan absah. Beberapa aplikasi seperti Google menjelaskan jika pengumpulan data diperlukan untuk memperbarui keandalan aplikasi, juga untuk kebutuhan periklanan sesuai preferensi konsumen. Ini berkaitan juga dengan prinsip pertama, bahwa *data subjects* harus mengetahui untuk apa data pribadinya digunakan. Data pribadi, dalam pengertian asas ini, hanya akan digunakan untuk alasan-alasan yang bersifat spesifik; di luar itu, penggunaannya menjadi illegal, dan dengan otomatis menimbulkan pertanggungjawaban *data controller*.

Dalam limitasi tujuan, alasan yang diajukan pun berlegitimasi. Maka, redaksi klasula pasal baku yang menyebut 'pemilik data akan tunduk pada tiap-tiap keputusan pemanfaatan data oleh kontroler' tidak dibenarkan. Pengecualian hanya berlaku untuk tujuan pengarsipan untuk kepentingan umum, penelitian ilmiah atau historis, dan kebutuhan statistik. Menurut Frenzel sebagaimana dikutip Busche, aspek penting dalam menentukan level dari tujuan pengumpulan data, salah satunya, adalah bahwa semakin banyak jumlah data subject yang terpengaruh dan semakin besar wilayah geografis atas pengumpulan data yang dituju maka semakin jelas spesifikasi tujuan yang perlu ditentukan mengingat *data subject* dari latar belakang kelompok usia atau budaya yang sangat berbeda sangat mungkin terpengaruh.[104] Prinsip ini jadi krusial bagi calon pengguna layanan digital, sebagai pertimbangan awal sebelum memutuskan untuk menggunakan atau tidak, dengan memperhitungkan potensi kerugian yang dialami dari pemanfaatan data pribadinya.

3.2.3. Data Minimization

Minimalisasi data berkaitan dengan prinsip sebelumnya (*purpose limitation*), bahwa pada intinya data yang dikumpulkan atau diproses oleh kontroler dibatasi pada data-data yang relevan dan mencukupi saja.[105] Contohnya, ketika meregistrasi akun sosial media, *user* hanya bisa diminta memasukan alamat *e-mail* dan informasi seputar identitas dasar seseorang dan perangkat tidak boleh meminta informasi lain, seperti, nomor rekening, jika memang tidak relevan dengan layanan yang disediakan. Limitasi ini juga menyangkut pula fungsi dari fitur *cookies* yang umumnya bekerja sebagai agen pengumpul data tanpa disadari berimplikasi pada privasi pengguna layanan.[106]

Lebih jauh, persoalan mengenai proses pengumpulan jadi sorotan penting, sebab tanpa adanya limitasi, upaya-upaya pengkomodifikasian data pribadi untuk kepentingan jual-beli data menjadi tak berbatas, dan hal tersebut tentu akan berujung merugikan pemilik data. Oleh karena itu, dalam praktik penyelenggaraan sistem elektronik, ketika mengoleksi data, kolektor harus mempertimbangkan beberapa konteks relevansi untuk meminimalisasi pengumpulan seperti: (a) berapa

---

[104] Voigt & Busche, The EU general…, hlm. 89.

[105] Pasal 5 ayat 1 huruf c: *"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*

[106] Tentang mekanisme kerja cookies dan dampaknya pada privasi data pribadi, lihat misalnya: 'How Website Cookies Affect Your Data Privacy', *dbswebsite.com*, (n.d.), diakses dari https://www.dbswebsite.com/blog/website-cookies-and-data-privacy/

lama data akan digunakan, (b) apakah individu mengetahui bahwa saya mengoleksi datanya, (c) apakah ada cara lain bagi kolektor untuk mendapatkan informasi tersebut tanpa harus mengoleksi data, dan (d) bagaimana saya merencanakan penggunaan atas data tersebut.[107] Kelima kriteria itu penting agar sebuah data pribadi yang diambil tidak menjadi penyingkapan sia-sia; atau berakhir sebagai komoditas dagang data konsumen.

3.2.4. Accuracy

Prinsip akurasi menyangkut hampir di semua tahapan siklus hidup informasi, namun yang paling utama tentu pada saat pengumpulan dan pemanfaatan. Akurat berarti data harus senantiasa merefleksikan realitas dan, jika dibutuhkan, dijaga keterkiniannya (*up-to-date*). Sorotan penting tentang akurasi terletak pada tahap pengumpulan dan penempatan; setiap data yang tidak akurat berkenaan dengan tujuan pemrosesan data harus seketika diambil upaya penghapusan oleh *data user*. 'Seketika' berarti pengelola data tidak boleh mengambil langkah-langkah penundaan yang tidak dibutuhkan dan segala bentuk penundaannya dianggap sebagai pelanggaran. Lalu, pemilik data harus diberikan kesempatan untuk memperbarui dan akses untuk mengubah data pribadinya yang dikumpulkan. Isu akurasi juga berkenaan dengan kewajiban penghapusan dan pembenaran data yang menjadi hak bagi *data subject* dalam rezim pelindungan data pribadi.

3.2.5. Storage Limitation

Data pribadi harus disimpan dalam bentuk yang memungkinkan identifikasi subjek data tidak lebih dari yang diperlukan untuk tujuan pemrosesan.[108] Data pribadi yang ditempatkan juga harus dilindungi oleh masa retensi tertentu yang tercantum dalam kebijakan retensi. Periode penyimpanan data pribadi, dengan demikian, akan dibatasi dengan '*strict minimum',* dalam arti, jika memungkinkan masa retensi dibuat sesingkat mungkin. Sementara, untuk memastikan batasan penyimpanan ini, batas waktu harus ditetapkan oleh pengontrol, untuk melakukan penghapusan atau peninjauan berkala. Maka, data pribadi yang dikumpulkan dan disimpan oleh kontroler tidak berarti menjadi miliknya selamanya. Setelah masa retensi itu selesai dan kontroler telah mengambil langkah pemusnahan, maka pada prinsipnya, jika terjadi kegagalan pelindungan atas data pribadi, kontroler tidak bisa dituntut pertanggungjawaban hukum atas kerugian; skenario sebaliknya berlaku ketika kegagalan terjadi pada masa retensi berlangsung.

3.2.6. Integrity and Confidentiality

Data pribadi akan diproses dengan cara yang memastikan keamanan data pribadi yang sesuai, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan dari kehilangan, kerusakan, atau kerusakan yang tidak

---

[107] 'What is Data Minimisation?', *experian.co.uk,* (n.d.), diakses dari https://www.experian.co.uk/business/glossary/data-minimisation/

[108] Art 5 GDPR.

disengaja, menggunakan tindakan teknis dan organisasi yang sesuai. Prinsip ini diterapkan oleh persyaratan organisasi untuk pemrosesan data di bawah GDPR.

Lebih jauh, beberapa kewajiban penting pengendali data yang diintroduksi dalam GDPR sebagaimana dirangkum Busche, dapat diringkas sebagai berikut:[109]

- Kewajiban untuk melaksanakan tindakan teknis dan organisasi; kepatuhan dapat, antara lain, ditunjukkan melalui kepatuhan pada *Code of Conduct* atau Mekanisme Sertifikasi yang disetujui; prosesor akan tunduk pada tingkat kewajiban keamanan yang sama dengan pengontrol, termasuk penggunaan teknik penyamaran, kewajiban untuk memastikan kerahasiaan, integritas, ketersediaan dan ketahanan layanan pemrosesan, kemampuan untuk memulihkan dan memulihkan akses ke data yang hilang dan evaluasi langkah-langkah keamanannya.
- kewajiban untuk menunjuk perwakilan di dalam UE sesuai dengan Art. 27 GDPR, jika prosesor berada di luar UE;
- kewajiban untuk menyimpan catatan kegiatan pemrosesan, Art. 31 poin 2 GDPR, akan tetapi, isi catatan ini kurang komprehensif dibandingkan dengan yang harus dipelihara oleh pengontrol; catatan tersebut harus disediakan untuk Otoritas Pengawas atas permintaan mereka
- kewajiban untuk bekerja sama dengan Otoritas Pengawas.
- kewajiban untuk menunjuk Petugas Perlindungan Data *(Data Protection Officer* atau DPO)[110] jika persyaratan hukum untuk kewajiban penunjukan terpenuhi.

Spesifik tentang poin terakhir, GDPR memerintahkan organisasi dengan kriteria tertentu, yang mengelola data pribadi untuk menunjuk 'Petugas Perlindungan Data'. Tugasnya antara lain bekerja menuju terciptanya kepatuhan terhadap semua undang-undang perlindungan data yang relevan, memantau proses tertentu, seperti penilaian dampak perlindungan data atau peningkatan kesadaran dan pelatihan karyawan untuk perlindungan data, serta berkolaborasi dengan pengawas pihak berwajib. Oleh karena itu, karyawan yang bertindak sebagai Petugas Perlindungan Data tidak boleh serta-merta diberhentikan atau dikenakan sanksi karena telah melaksanakan tugasnya.

Terlepas dari fungsi pengawasannya itu, perusahaan tetap bertanggung jawab untuk mematuhi undang-undang perlindungan data. Karenanya, perusahaan harus melibatkan Petugas Perlindungan Data dalam semua masalah yang berkaitan dengan perlindungan data pribadi 'dengan benar' dan 'tepat waktu'. Ketika Petugas Perlindungan Data ditunjuk, atasannya harus mempublikasikan data kontaknya, dan mengkomunikasikan data pengangkatan dan kontaknya kepada otoritas pengawas perlindungan data. Jika perusahaan secara sukarela menunjuk DPO, mereka juga harus mematuhi kriteria dan ketentuan yang diuraikan di atas. Kegagalan yang disengaja atau lalai untuk menunjuk Petugas

[109] Busche dan Axel, *Ibid.*

[110] Petugas Perlindungan Data atau *Data Protection Officer* (DPO) adalah mekanisme wajib yang diperkenalkan GDPR, bagi penyelenggara sistem elektronik yang melakukan pemrosesan data dengan kriteria tertentu, wajib memiliki petugas khusus yang bertanggung jawab khusus atas perlindungan data pribadi. Kriterianya antara lain: (1) jika organisasi mengumpulkan data pribadi yang bersifat sensitif; (2) badan-badan publik, dengan pengecualian bagi lembaga pengadilan; (3) atau jika perusahaan mengelola data yang berskala besar. Lihat Art. 37 dan 38 GDPR.

Perlindungan Data meskipun terdapat kewajiban hukum merupakan pelanggaran yang dapat dikenakan denda. Sanksi atas pelanggaran kewajiban yang dimuat dalam GPDR berupa denda; Pasal 83 ayat 4 mengatur bahwa denda sebesar EUR 100,000,000 atau hingga 4% dari penghasilan tahunan global dapat dikenakan terhadap prosesor data per pelanggaran. Kewajiban membayar denda ini tidak menghilangkan tanggung gugat dari data prosesor ketika diajukan tuntutan kompensasi oleh *data subject*. Skema denda ini memunculkan resistensi di kalangan pelaku industri khususnya di kawasan Eropa. Di sisi lain, Banyualam pada wawancara dengan *the Conversation* menyebut pendekatan yurisdiksi ekstra-teritorial ala GDPR diklaim tidak realistis dan akhirnya membuat skema denda sulit ditegakkan pada aktor-aktor di luar kawasan UE.[111] Sedangkan dalam konteks pengaturan transfer data ke luar Uni Eropa, GDPR memberlakukan restriksi bersyarat. Artinya, tidak ada kewajiban spesifik tentang lokalisasi data, tapi pemindahan lokasi penempatan data pribadi hanya bisa dilakukan sepanjang negara tujuan memiliki standar yang dinilai memadai, didasarkan adanya perjanjian internasional atau kontrak pengendali data, serta, yang terpenting, adanya persetujuan transfer dari pemilik data. Data Guidance mencatat per 2020 baru tiga belas negara di luar Uni Eropa yang secara formal diakui memiliki standar perlindungan data pribadi yang memadai oleh Komisi Eropa.[112] *Cross-border data flow* antara Uni Eropa dan ketiga-belas negara tersebut dapat leluasa dilakukan sementara yang lainnya harus melalui mekanisme otorisasi dan penilaian terlebih dahulu oleh komisi.

3.3. Perbandingan Praktik di Beberapa Negara

3.3.1. Perlindungan Data Pribadi di Amerika Serikat

Kontras berbeda dengan Uni Eropa, Amerika Serikat (AS) mengikuti pendekatan sektoral untuk perlindungan privasi data. Tidak ada undang-undang federal yang mencakup semuanya dan menjamin privasi serta perlindungan data pribadi; sebaliknya, undang-undang di tingkat federal terutama melindungi data dalam konteks sektor tertentu. Fakta ini cukup mengejutkan mengingat AS sendiri merupakan salah satu negara asal penyedia layanan digital terbesar di dunia. Istilah 'data pribadi' tidak spesifik dikenal dalam legislasi AS mengingat terminologi yang lebih sering digunakan adalah 'informasi pribadi'.[113] Terkait hal itu, definisi atas informasi pribadi pun tak seragam di satu regulasi dan lainnya; masalah ini muncul karena AS menggunakan sistem negara federal di mana masing-masing negara bagiannya memiliki otonomi untuk mengatur sendiri.

---

[111] Risky Banyualam dalam Andre Arditya dan Ingatius Raditya Nugraha, "RUU PDP RUU PDP masih memiliki banyak kekurangan dibandingkan standar internasional dalam melindungi data pribadi", theconversation.com, 29 Januari 2021, diakses dari https://bit.ly/3v83EdL.

Lihat juga: Benjamin Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives', *International Data Privacy Law,* Volume 9, Issue 2, (May 2019): 109–128.

[112] Data Guidance, 'International: EU-US cross-border...", *Ibid*.

"*The 13 countries that have received adequacy rulings to date are: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the U.S. for Privacy Shield-certified companies.*"

[113] Steven Chabinsky dan F. Paul Wittman, "USA: Data Protection Laws and Regulation 2020", iclg.com, 6 Juni 2020, (London: International Comparative Law Guides, 2020), diakses dari https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Di samping itu, istilah-istilah yang digunakan dalam GDPR seperti "processing", "controller", "processor", "sensitive personal data" juga belum diatur dalam legislasi Amerika Serikat.[114] Lebih jauh, berbeda dengan rezim proteksi data pribadi di kawasan Uni Eropa Eropa, AS mengandalkan kombinasi undang-undang di tingkat federal dan negara bagian, peraturan administratif, serta pedoman regulasi mandiri khusus industri.[115] Jaminan perlindungan privasi condong lebih sektoral dan terdapat di berbagai instrumen legislatif dan yurisprudensi. Undang-undang sebagaimana dimaksud hanya berlaku untuk sektor tertentu saja, seperti perawatan kesehatan, pendidikan, komunikasi, dan layanan keuangan atau, dalam kasus pengumpulan data online, untuk anak-anak.[116]

Berbeda dengan pendekatan perlindungan data Uni Eropa, yang didapuk mewakili standar emas perlindungan privasi, pendekatan dominan di AS didasarkan pada peraturan perlindungan konsumen. Karenanya, di Amerika Serikat, Federal Trade Commission (FTC), sebuah badan penegakan hukum independen yang bertugas melindungi konsumen, berperan aktif sebagai otoritas penegakan privasi utama. Namun, yurisdiksi FTC dibatasi terhadap pelanggaran privasi oleh organisasi yang dalam praktiknya terindikasi 'menipu' atau 'tidak adil'.[117] Undang-undang Privasi AS tidak secara khusus merupakan undang-undang tentang privasi data, melainkan sistem undang-undang perlindungan konsumen yang luas; cakupannya telah digunakan untuk melarang praktik yang tidak adil atau penipuan yang melibatkan kegiatan pengungkapan dan kelalaian prosedur keamanan untuk melindungi informasi pribadi.[118] FTC selaku otoritas mengambil posisi tegas bahwa kategori praktik penipuan ('*deceptive practice'* dalam istilahnya) termasuk juga, di antaranya, kegagalan perusahaan pengelola untuk menyediakan sistem keamanan atas informasi pribadi memadai, dan penggunaan metode pemasaran yang menipu (*deceptive advertising* dan *marketing methods*).[119]

Beberapa sektor perundang-undangan yang beririsan dengan perlindungan data pribadi di bawah supervisi FTC diantaranya terdiri dari:[120]

i. *Financial Services Modernization Act*

   Undang-undang ini mengatur tentang '*non-public personal information'*[121] ketika digunakan oleh entitas perusahaan jasa keuangan. Singkatnya, regulasi ini mengizinkan institusi jasa keuangan untuk dapat melakukan transfer informasi pribadi ke perusahaan lain sepanjang benar-benar dibutuhkan untuk aktivitas jasa keuangan. Informasi dapat dibagikan pula dengan agensi pelaporan kredit atau agensi regulator di bidang tersebut.

---

[114] *Ibid.*, sub-bab 2.1.

[115] Shawn Marie Boyne, "Data Protection in the United States: U.S. National Report", dalam Dario M. Vincente dan Sofia de V. Casimiro (Eds), *Data Protection in the Internet,* Ius Comparatum Global Studies in Comparative Law Volume 38, (Cham Switzerland: Springer Nature, 2020), hlm. 409.

[116] *Ibid.*

[117] Sotto dan Simposon, dalam *Ibid.*

[118] *Ibid.*, hlm. 411.

[119] Chabinsky dan Wittman,

[120] Boyne, Ibid., hlm. 412.

[121] *"Non-public personal information" means personally identifiable financial information that is provided by a consumer to a financial institution; resulting from a transaction with the consumer or from a service provided to the consumer; or otherwise obtained by the financial institution". Ibid.*

ii. *Health Insurance Portability and Accountability Act 1996*

Undang-undang ini memproteksi informasi pribadi yang dipegang dan dikelola oleh entitas yang berkaitan tentang penyelenggaraan kesehatan berikut riwayat pembayaran yang dilakukan nasabah. Regulasi ini mengenal istilah 'Informasi Kesehatan Elektronik', yaitu informasi yang terekam dan/atau ditransmisikan ke dalam suatu sistem pengarsipan elektronik. Ketentuan privasinya mengatur tentang pengumpulan dan penyingkapan informasi sementara dalam ketentuan keamanannya mengatur persyaratan kewajiban bagi perusahaan untuk melakukan pengamanan atas data-data tersebut. Departemen Kesehatan bertanggungjawab dalam menegakkan proteksi informasi spesifik pada bidang ini.

iii. *Controlling the Assault and Non-Solicited Pornography and Marketing Act*

Mengatur perihal pengumpulan dan penggunaan alamat surat elektronik (e-mail), juga setiap pertukaran pesan elektronik yang bersifat komersial berkaitan dengan periklanan dan promosi produk. Di sini, surel yang sifatnya komersial tersebut tidak boleh mengandung unsur pengelabuan (*non-deceptive sender*) dan *spam*; pengirim harus secara eksplisit meninggalkan kontak dan informasi lain menyangkut identifikasi. Ketentuan pidana dalam undang-undang ini yang disingkat sebagai CAN-SPAM memberi hukuman bagi pelanggarnya, salah satunya adalah pengumpul informasi alamat surel yang menggunakan skema spam berupa '*dictionary attack*'.[122]

iv. *The Fair Credit Reporting Act*

Produk legislasi ini mengatur perihal laporan kredit konsumen yang diselenggarakan oleh pihak pengguna, semisal kreditur dan perusahaan kartu kredit, serta pihak yang menyediakan layanan pelaporan. "Consumer Report" atau laporan konsumen adalah setiap komunikasi yang diterbitkan oleh agensi pelaporan konsumen (*consumer-reporting agency* atau CRA) berkaitan tentang riwayat hutang-piutang, penilaian kredit, kapasitas kredit, termasuk juga karakter dan informasi perihal reputasi umum yang digunakan untuk mengevaluasi kelayakan kredit konsumen atau jasa asuransi. CRA diwajibkan mengikuti serangkaian prosedur untuk menjamin tingkat akurasi informasi dan ketika data ditemukan tidak akurat, penyelenggara harus segera melakukan pembaruan atau koreksi.

v. *Electronic Communication Privacy Act*

Undang-undang tentang privasi komunikasi elektronik ini mengatur salah satunya tentang larangan intersepsi komunikasi elektronik secara melawan hukum. Tiap-tiap intersepsi diwajibkan mendapatkan otorisasi dari lembaga pengadilan dan dari pihak yang bersangkutan. Menurut ketentuan UU ini, seluruh penggunaan informasi yang didapatkan dari penyadapan tanpa didahului otorisasi adalah illegal. Lebih jauh,

[122] Federal Trade Commission, "CAN-SPAM ACT: A Compliance Guide for Business", ftc.gov, (Terakhir disunting Januari 2021), diakses dari https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

ketentuan dalam UU privasi komunikasi elektronik ini menggunakan istilah konten, yang merujuk pada "*information concerning substance, purport, or meaning*".[123]

vi. The Computer Fraud and Abuse Act

Aturan ini mencegah dan menghukum aktivitas berkenaan dengan peretasan, yang didefinisikan sebagai pengaksesan tak terotorisasi terhadap komputer yang terproteksi. Individu atau entitas dilarang untuk melampaui pengumpulan informasi melampaui cakupan akses resmi mereka. Sementara, yang dimaksud komputer terproteksi mencakup perangkat-perangkat yang digunakan oleh institusi keuangan, pemerintahan, dan yang digunakan untuk kegiatan perdagangan atau komunikasi resmi lintas negara. Kriteria kerugian (*damage*) yang dipakai adalah adanya dampak negatif pada integritas atau availabilitas suatu data, program, sistem, ataupun informasi.

Pendekatan yang dipilih dalam hal perlindungan data pribadi lebih banyak dalam inisiatif *self-regulation*. Artinya, upaya memaksimalkan proteksi atas data pribadi diserahkan ke kebutuhan masing-masing penyelenggara. Hal ini menciptakan polemik sebab Amerika Serikat berada dalam peringkat teratas perusahaan pengontrol data.[124] Sementara, dalam konteks transfer data lintas batas negara, sikap AS lebih cenderung proposisi terhadap data *free flow* mengingat pengaturannya hanya sebatas mendorong organisasi yang berbasis di negara tersebut untuk melakukan sertifikasi ke Departemen Perdagangan sebelum melakukan transfer data ke luar. Brown sebagaimana dikutip oleh Boyne, menyebut bahwa AS berkomitmen penuh pada prinsip *free and fair trade*, sehingga tidak memiliki banyak aturan khusus yang mengatur perihal transfer data ke luar negeri.[125] Kegiatan itu hanya dibatasi oleh prinsip "*basic fair information for notice*" dan larangan atas "*deceptive or unfair business practices*". Amerika Serikat juga tidak memiliki persyaratan yang mewajibkan lokalisasi server data, kecuali data yang digunakan oleh lembaga pemerintah tertentu.[126] Khusus dalam konteks kegiatan transfer data pribadi AS-UE, kedua otoritas mengaturnya secara bilateral lewat perjanjian internasional.

3.3.2. Perlindungan Data Pribadi di Kanada

Pengaturan pelindungan data pribadi di Kanada, hampir serupa dengan Amerika Serikat, juga terpecah dalam multi-level, bahkan tiap-tiap sektor publik di setiap provinsi dan teritorinya memiliki masing-masing regulasi perlindungan data pribadi. Perbedaannya terletak pada regulasi di sektor publik dan privat. Menurut Scassa, aturan federal yang berlaku perihal urusan perlindungan privasi adalah *Privacy Act;* juga *Freedom of Information and Protection of Privacy Act.*[127] Sementara, *Personal Information Protection and Electronic Documents Act* (PIPEDA) membahas perlindungan informasi pribadi yang

[123] Boyne, *Ibid*., hlm. 414.

[124] Beberapa yang kontra menilai bahwa kebijakan perdagangan perihal pembatasan cross-border akan menjadi beban dan berdampak serius pada pendapatan AS. Lihat: Rachel F. Fefer, 'Data Flows, Online Privacy, and Trade Policy', laporan untuk Congressional Research Service, (26 Maret 2020), diakses dari https://fas.org/sgp/crs/misc/R45584.pdf.

[125] *Ibid.,* hlm. 451.

[126] *Ibid.*

[127] Teressa Scassa, 'Data Protection and the Internet: Canada', dalam Vincente & Casemiro, *Data Protection in the Internet.., Ibid*., hlm. 55-56.

berada di tangan organisasi sektor swasta. Ada banyaknya regulasi perihal data pribadi, di tingkat federal maupun daerah, menyebabkan perlindungan data pribadi bisa tidak merata dari satu provinsi ke provinsi lain dan hingga 2020, ada tiga provinsi yang memiliki aturan tersendiri, antara lain, Quebec, Alberta, dan British Columbia. PIPEDA berlaku untuk pengumpulan informasi pribadi serta pengungkapannya dalam wilayah kegiatan komersial. Undang-undang ini berlaku untuk semua informasi pribadi yang dikumpulkan, digunakan, atau diungkapkan oleh sektor swasta yang diatur secara federal (misalnya, industri telekomunikasi dan maskapai penerbangan) serta semua aktivitas komersial sektor swasta yang melintasi perbatasan provinsi atau nasional.[128] Ini juga berlaku untuk semua pengumpulan, penggunaan, dan pengungkapan informasi pribadi murni intra-provinsi yang terjadi di provinsi yang belum memberlakukan undang-undang yang secara substansial mirip dengan PIPEDA.[129] Konteks privasi subjek data yang disinggung dalam muatan produk undang-undang tersebut diantaranya adalah hak untuk dilupakan (*the right to be forgotten*) dan hak atas penghapusan (*de-indexing*).[130] Namun, PIPEDA tidak berlaku pada data pribadi yang dikelola oleh partai politik karena dalam wilayah itu *Personal Information and Protection of Privacy Act* yang mengatur. Secara umum, perlindungan dasarnya terjamin dalam kitab undang-undang perdata di masing-masing wilayah provinsi di Kanda, yang memungkinkan bagi korban pelanggaran data pribadi untuk mengajukan gugatan.

Seperti di Amerika Serikat, Kanada menggunakan istilah ‘personal information’. Pada prinsipnya, Scassa menyebut, setiap undang-undang memiliki definisinya sendiri namun inti penting dari seluruhnya beririsan dalam pengertian ‘informasi pribadi’ sebagai informasi tentang individu yang teridentifikasi. “*Courts have generally interpreted this to mean that information is personal information if, on its own or when combined with other available information, it can lead to the identification of an individual.”.*[131] Beberapa data yang tercakup dalam informasi pribadi termasuk IP address (berdasarkan putusan Mahkamah Agung Kanada). Namun, legislasi di Kanada tidak membedakan antara data pribadi yang diproses secara daring maupun luring.

Selanjutnya, ada sepuluh prinsip *fair information* yang dikenal dalam perlindungan informasi pribadi dalam PIPEDA, yakni:[132]

a. Akuntabilitas (*accountability)*; bahwa organisasi bertanggungjawab sepenuhnya terhadap data-data yang berada di bawah kendalinya. Juga, harus menunjuk pihak penanggung jawab tertentu yang bertugas untuk memastikan kepatuhan terhadap pemenuhan prinsip-prinsip keadilan, serta membentuk desain program manajemen perlindungan privasi dalam pengelolaannya.
b. Mengidentifikasi tujuan (*identifying purposes),* yakni, tujuan pemanfaatan informasi pribadi harus diidentifikasi oleh organisasi sebelum maupun sesudah pengumpulan. Tujuan harus dijelaskan sejelas dan sesempit mungkin sehingga pengguna atau

[128] *Ibid.*, hlm. 56.
[129] *Ibid.*
[130] *Ibid.,* hlm. 62.
[131] *Ibid.*, hlm. 57.
[132] Office of the Privacy Commissioner of Canada, ‘PIPEDA Fair Information Principles’, priv.gc.ca, (Mei 2019), diakses dari https://bit.ly/3q3KJ2E.

subjek data dapat memahami bagaimana informasi mereka akan digunakan. Tujuan yang dimaksud, misalnya, untuk pembukaan rekening, penilaian kelayakan kredit, memproses layanan langganan, dst.

c. Persetujuan (*consent)*; bahwa untuk tiap-tiap informasi yang dikumpulkan, digunakan, dan dibuka harus berdasarkan pada persetujuan pemilik data. Caranya dengan menyediakan formulir lengkap yang menekankan poin penting seperti, 'informasi pribadi apa yang dikumpulkan dari pengguna', 'kepada siapa informasi tersebut akan dibagikan', 'apa risiko dari pengumpulannya', dst.
d. Pembatasan pengumpulan (*limiting collection)*; bahwa pengumpulan yang dilakukan oleh kontroler harus dibatasi seminim mungkin dengan batasan tujuan pengumpulan yang sebelumnya teridentifikasi. Selain itu, informasi yang dikumpulkan haruslah legal dan patut, dan data kontroler harus bersikap transparan perihal kebijakan pemrosesan informasi.
e. Pembatasan kegunaan, pembukaan, dan retensi (*limiting use, disclosure and retention*); bahwa kecuali ditentukan lain, setiap informasi pribadi yang diperoleh hanya dapat digunakan atau dibuka berdasarkan tujuan spesifik yang disetujui. Dalam konteks retensi, informasi pribadi harus dijaga selama mungkin sepanjang berkenaan dengan pemenuhan tujuan awalnya. Selain membatasi, data kontroler harus pula melakukan pengawasan akses dan menempuh tindakan yang sepatutnya ketika ditemukan akses yang tidak terotorisasi. Lalu, pengelola data harus memiliki pedoman kerja yang terukur mengenai masa retensi dan mekanisme pemusnahan informasi.
f. Keakuratan (*accuracy*); bahwa selain lengkap, informasi yang diterima haruslah akurat, terkini, untuk melayani tujuan pengumpulan serta pemanfaatannya. Untuk memastikan itu, penyedia layanan harus meminimalisasi penggunaan informasi yang keliru ketika pengambilan keputusan atas informasi individu, atau ketika melakukan pembukaan ke pihak ketiga, dengan memperhatikan kepentingan pemilik data.
g. Pengamanan (*safeguards*); setiap informasi pribadi harus terlindungi dengan sistem keamanan yang layak, terutama berkaitan dengan sensitivitas data. Pengamanan dimaksud mencakup terhadap pencurian, kehilangan, akses non-otorisasi, duplikasi, penggunaan dan modifikasi.
h. Keterbukaan (*openness)*; bahwa organisasi harus memberikan informasi mendetail terhadap kebijakan privasi yang dimilikinya, berikut praktik pengelolaan yang dilakukan, secara terbuka untuk umum dan tersedia kapan saja.
i. Akses individu (*individual access*); dalam hal terdapat permintaan, pemilik data bukan hanya harus terinformasikan perihal ketersediaan, penggunaan, dan pembukaan atas informasi pribadi mereka, tapi juga diberi akses terhadapnya. Subjek data harus bisa mengajukan keberatan jika ditemukan informasi yang tidak lengkap, tidak akurat, dan diberikan kesempatan untuk melakukan perubahan.
j. Keberatan atas kepatuhan (*challenging compliance*); di Kanada, hak untuk mengajukan keberatan atas kepatuhan diekstraksi jadi prinsip tersendiri. Intinya, individu pemilik data harus bisa menantang kepatuhan organisasi atas pemenuhan prinsip-prinsip di atas. Keberatan dapat diajukan ke alamat pihak yang ditunjuk oleh

kontroler untuk bertanggungjawab, semisal, Kepala Petugas Privasi (*Chief Privacy Officer)*, yang serupa dengan DPO dalam GDPR.

Selain itu, pada 2015, ketentuan kewajiban notifikasi perihal terjadinya kegagalan atau pelanggaran atas pelindungan informasi pribadi diperkenalkan.[133] Situasi kegagalan yang dimaksud tidak melulu harus sudah terjadi interupsi, namun meliputi tiap kondisi dimana patut diperkirakan suatu risiko secara beralasan meningkat, akibat adanya peristiwa eksternal maupun internal.

Perihal kebijakan penempatan data di luar teritori Kanada, PIPEDA pada dasarnya memperbolehkan dengan catatan bahwa organisasi yang bersangkutan bertanggung jawab secara hukum atas risiko yang kemungkinan muncul.[134] Pertanggungjawaban itu mencakup pula kewajiban menyediakan level proteksi yang minimal setara dengan apa yang ditetapkan dalam kebijakan privasi yang digunakan organisasi. Caranya, pada umumnya, dilakukan lewat kesepakatan kontraktual antara kontroler di Kanada dengan pihak prosesor di luar negeri. Aturan teknisnya pun tersedia dalam *Guidelines for Processing Personal Data Across Borders,* yang salah satunya mengharuskan kontroler untuk transparan menginformasikan pemilik informasi pribadi tentang perlakuan yang akan dibuat, termasuk peringatan akan konsekuensi hukum yang dapat dipahami pelanggan bahwa penempatan informasi miliknya di luar yurisdiksi dengan otomatis memberikan otoritas pemerintah atau penegak hukum di negara tujuan, akses terhadap data miliknya dalam hal dibutuhkan untuk kepentingan penegakan hukum di negara tersebut. Berbeda dengan sektor privat, pada aktivitas pengelolaan data sektor publik terdapat kebijakan lokalisasi data; artinya, entitas atau badan publik dilarang melakukan penempatan data atau transfer informasi pribadi warga negara Kanada di luar teritori Kanada.[135]

3.4. Sikap Indonesia dalam Perjanjian Internasional tentang Pengaturan Arus Data Lintas Negara

Sikap Pemerintah Indonesia terbaca dalam gestur proteksionis yang ditunjukan sepanjang pertemuan G20 Digital Economy Ministerial Meeting 2020. Pada pertemuan awal, isu kedaulatan belum banyak disoroti peserta. Momentum itu digunakan Indonesia untuk mengajukan inisiatif proposal prinsip perlindungan data, khususnya terkait isu arus data lintas negara.[136] Menteri Johnny G. Plate mengaku proposal itu didukung luas oleh negara-negara G20. Dalam pertemuan menyepakati kerangka ekonomi digital tersebut, isu *e-commerce* disepakati oleh forum untuk dilepaskan pada mekanisme WTO sementara pembangunan kerjangka kerja sama kepercayaan akan meliputi isu-isu seperti privasi, keamanan siber, dan lainnya. Prinsip pertama adalah *data free-flow with trust* (DFWT). Ini merupakan pemutakhiran dari prinsip yang sudah eksis sebelumnya dengan tambahan pada konsep 'trust'. Aspek trust di satu sisi menekankan adanya tanggung jawab etis penerima data di luar tanggung jawab hukum, bagi data yang ditempatkan di luar yurisdiksi suatu

---

[133] Scassa, *Data Protection and...*, hlm. 65.
[134] *Ibid.*, hlm. 74.
[135] *Ibid.*
[136] Kominfo, "5 Proposisi Indonesia soal Keamanan Data di Pertemuan G20", *kominfo.go.id,* 30 Juli 2020, diakses dari https://bit.ly/35xl9Kd.

negara, dengan catatan adanya penghormatan bagi perlindungan data pribadi menurut sistem hukum negara asal, selain juga isu pada konteks kekayaan intelektual.

Di sisi lain, dimasukkannya aspek *trust* ini relatif memperlunak kebijakan pelindungan data pribadi karena yang semestinya diatur tegas, lantaran kini jadi diserahkan untuk diputuskan lewat pendekatan dialog. Munculnya proposal ini tidak bisa dilepaskan dari intensi Indonesia yang menghendaki *data free flow* sebagai kegiatan ekonomi baru yang bernilai miliaran dolar.[137] Juga latar belakang Indonesia sebagai salah satu negara dengan masyarakat pengguna internet terbanyak. Prinsip kedua adalah resiprositas. Timbal balik diharapkan oleh Indonesia untuk tiap-tiap pembukaan atau transfer data lintas batas negara. Implementasinya dengan menetapkan standar minimal yang setara atau lebih tinggi dengan yang diatur dalam legislasi di dalam negeri. Namun, kesan timbal balik ini juga mencerminkan bahwa pemerintah Indonesia cenderung terbuka pada liberalisasi data.

[137] Nemo Ikram, "Indonesia Dukung Data Free-Flow, Bagaimana Keamanannya", *cyberthreat.id*, 9 Juni 2019, diakses dari https://bit.ly/3xy7kY1.

BAB 4
PEMETAAN REGULASI PERLINDUNGAN DATA PRIBADI DI INDONESIA

4.1. Pengantar

Seperti halnya di Amerika Serikat, peta regulasi perlindungan data pribadi di Indonesia tersebar di banyak undang-undang. Hal ini, salah satunya, dikarenakan Indonesia, belum memiliki satu acuan hukum perlindungan data pribadi di level legislasi nasional. Publik berharap banyak mengingat Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) kini telah masuk dalam salah satu agenda legislasi prioritas tahunan walaupun sudah cukup lama tidak kunjung selesai dibahas. Pada level konstitusi, Indonesia memiliki rujukan hukum yang mengakui privasi sebagai hak asasi manusia. Pasal 28G ayat (1) Undang-Undang Dasar 1945 menegaskan: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang mencakup hak asasinya." Meski demikian, spesifik dalam konteks data pribadi, Indonesia belum memiliki landas rujukan yang kuat.

Dalam konteks pengaturan aturan mengenai dokumen dan/atau informasi elektronik, Indonesia sejauh ini baru memiliki Undang-Undang Nomor 8 Tahun 2008 tentang Informasi dan Teknologi Informasi, sebagaimana sudah diubah dalam Undang-Undang Nomor 19 Tahun 2019 (UU ITE). Di situ memang telah sedikit diatur tentang kewajiban pengelola sistem elektronik menjaga kerahasiaan data, keamanan sistem, keharusan otorisasi dan kriteria keandalan lainnya terkait transaksi elektronik, juga kewajiban menghapus data atas permintaan pemiliknya. Ada pula aturan pidana yang melarang adanya intersepsi secara melawan hukum ke dalam sistem elektronik milik orang lain, atau biasa disebut *cyber-attack*. Tapi, sekalipun mengusung tema tentang regulasi di bidang informasi dan transaksi elektronik yang sangat dekat dengan konteks pengoleksian data oleh sistem, definisi 'data pribadi' dalam konteks elektronik belum dikenal dalam undang-undang ini. Data masih diperlakukan sebagai bagian dari 'informasi elektronik' yang dilindungi secara umum.

Menelusuri lebih jauh, definisi tentang 'Data Pribadi' bisa ditemukan dalam Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan ('UU Adminduk'). Data pribadi dijelaskan sebagai data perseorangan yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.[138] Meski telah mengenal istilah data pribadi, definisi tersebut sebenarnya belum konkret menjelaskan data sebagai sebuah objek digital mengingat konteks data yang dimaksud dalam UU Adminduk berbeda dengan data dalam relasinya sebagai komoditas digital. Meski demikian, dari rumusan ini kita dapat memperoleh gambaran awal bahwa (1) data pribadi bersifat perseorangan, (2) ia wajib disimpan, dirawat, dan dijaga kebenarannya, artinya data harus akurat dan ter-*update*; dan

[138] Pasal 1 angka 22 UU Nomor 24 Tahun 2013 tentang Administrasi Kependudukan.

yang terpenting (3) terjaga kerahasiaannya. Lebih jauh, definisi yang lebih memuaskan baru ditemukan di level peraturan pelaksana, yakni, Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik (PP PSTE) dan PP Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE). Di sini, 'Data Pribadi' diintroduksi sebagai "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.[139] Definisi ini pula yang diadopsi dalam RUU Perlindungan Data Pribadi yang saat ini pembahasannya sedang berlangsung. Sementara, pada tingkat Kementerian, ada Menteri Komunikasi dan Informatika pada 2016 juga sempat mengeluarkan Peraturan Menteri tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang meminjam definisi teknis dari Derivatif PDP Uni Eropa. Akan tetapi, persoalan seputar efektivitas implementasi muncul mengingat Peraturan Menteri memiliki cakupan yang bersifat sektoral (hanya pada lingkup aktivitas yang beririsan dengan tugas pokok dan fungsi internal kementerian) sedangkan aktivitas pemrosesan data pada kenyataannya menjadi sesuatu yang lintas sektoral.

Masih dalam sektor perdagangan, data sebagai komoditas juga disinggung dalam Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan (UU Perdagangan). Secara garis besar, UU Perdagangan mengatur objek perdagangan berupa barang dan jasa, termasuk ruang lingkup aktivitas perdagangan secara daring yang lekat dengan kegiatan pemrosesan data. Pasal 1 angka 5 UU Perdagangan mendefinisikan 'barang' sebagai setiap benda, berwujud maupun tidak berwujud, bergerak maupun tidak bergerak, yang dapat dihabiskan maupun tidak dapat dihabiskan, yang memiliki nilai kemanfaatan; dari definisi itu jelas bisa disimpulkan jika data termasuk sebagai obyek yang bisa diperdagangkan, tapi sejauh apa hal itu bisa diperdagangkan belum ada pengaturan yang jelas. Padahal, UU Perdagangan menegaskan bahwa undang-undang ini mengatur perdagangan yang diselenggarakan melalui Sistem Elektronik dan kerja sama perdagangan internasional. Ini terlihat dalam beberapa *Free Trade Agreement* yang ditandatangani pemerintah Indonesia, semisal *Regional Comprehensive Economic Partnership* ASEAN-RRT, yang salah satu poinnya adalah memudahkan transfer data antara negara anggota.[140]

Selain itu, data dan informasi juga beririsan dengan isu hukum kekayaan intelektual. Salah satu yang disoroti adalah perihal penggunaan metode analisis *big data* dalam pengambilan keputusan, dalam kaitannya dengan rezim rahasia dagang.[141] Undang-Undang Nomor 30 Tahun 2000 mendefinisikan 'Rahasia Dagang' sebagai 'informasi yang tidak diketahui oleh umum' di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik rahasia dagang. Data, informasi, maupun *big data* berikut teknik-teknik analisisnya punya irisan dengan definisi rahasia dagang karena nilai informasi yang dimilikinya dapat berguna bagi bisnis. Begitu pun dalam ranah hak cipta, Undang-Undang Nomor 19 Tahun 2002 tentang

---

[139] PP Nomor 71 Tahun 2019, Pasal 1 Angka 29.

[140] Lihat: ASEAN, 'Summary of the Regional Comprehensive Economic Partnership Agreement', *asean.org.*, 2020, diakses dari https://asean.org/storage/2020/11/Summary-of-the-RCEP-Agreement.pdf

[141] Lihat: Craig D'Souza, 'Big Data and Trade Secrets (A General Analysis)', *srrn.com*, (15 Januari 2019), diakses dari https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316328

Hak Cipta (sebelum diganti oleh Undang-Undang Nomor 28 Tahun 2014) menyebutkan bahwa *database* dapat dilekatkan perlindungan hak cipta. Pada penjelasan Pasal 12 UU Hak Cipta terdahulu menyebut *database* adalah kompilasi data dalam bentuk apapun yang dapat dibaca oleh mesin (komputer) atau dalam bentuk lain, yang karena alasan pemilihan atau pengaturan atas isi data itu merupakan kreasi intelektual. Perlindungan terhadap database diberikan dengan tidak mengurangi hak pencipta lain yang ciptaannya dimasukkan dalam database tersebut. Pada level peraturan pelaksananya, ada Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Transaksi Perdagangan Melalui Sistem Elektronik (PP TPMSE). Aturan tersebut mewajibkan Pengelola Sistem Elektronik (PSE) untuk memberi notifikasi tertulis kepada pemilik data dalam hal terjadi kegagalan pelindungan data pribadi.[142] Kegagalan yang dimaksud adalah terhentinya sebagian atau seluruh fungsi sistem elektronik yang bersifat esensial sehingga sistem elektronik tidak berfungsi sebagaimana mestinya.

Lebih jauh, secara umum pemetaan regulasi dipisahkan pada dua kategori, yaitu, regulasi inti dan regulasi penunjang. Di luar keduanya, regulasi dalam proses pembentukan seperti RUU PDP juga akan sedikit ditelaah untuk memberikan proyeksi ke depan dan komparasi. Sebuah aturan masuk dalam kategori regulasi inti karena berkaitan langsung dengan kegiatan tata kelola data pribadi dalam ranah siklus hidup informasi. Sementara, aturan dikatakan regulasi penunjang jika muatannya bersifat pendukung aktivitas ekonomi digital. Masing-masing kategori tersebut dipecah ke dalam dua tingkatan, yakni, tingkat undang-undang dan tingkat peraturan pelaksana. Adapun elaborasinya sebagai berikut:

4.2. Regulasi Inti

4.2.1. Tingkat Undang-Undang

Undang-Undang Hak Asasi Manusia (UU HAM)[143]

Prinsip dasar pelindungan privasi dalam kerangka penghormatan atas hak asasi manusia diletakan dalam UU Nomor 39 Tahun 1999 tentang HAM sebagai aturan turunan dari Pasal 28G ayat (1) Konstitusi. Proteksi atas data pribadi, sebagaimana disebut pada bagian terdahulu, masuk ke dalam ranah pelindungan atas privasi. Secara umum, norma inti perihal pelindungan privasi diatur dalam Pasal 29 ayat (1) UU HAM, yang berbunyi: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya." Sebagai bagian dari otonomi pribadi, informasi terkait diri pribadi yang berwujud dalam data dapat interpretasikan termasuk dalam lingkup privasi pasal ini. Proteksi tersebut kemudian dikuatkan lagi dengan Pasal 30 UU HAM bahwa, "setiap orang berhak atas rasa aman dan tenteram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu."

Meski demikian, konteks pengaturan terkait data pribadi belum disebut secara khusus. Pada Pasal 21 UU HAM, keutuhan pribadi baik yang berada dalam dimensi rohani maupun jasmani, tidak boleh menjadi 'objek penelitian' tanpa persetujuan darinya. Untuk

---

[142] Pasal 4 PP TPMSE.

[143] Indonesia, *Undang-Undang tentang Hak Asasi Manusia*, UU Nomor 39 Tahun 1999, LN Nomor 165 Tahun 1999, TLN Nomor 3886.

mengaitkan konteks proteksi data pribadi sebagai bagian dari privasi pada UU HAM, frasa 'objek penelitian'[144] perlu dimaknai dan diletakan pada konteks yang lebih luas luas. Jika dikaitkan dengan konteks pemrosesan data, termasuk di dalamnya penganalisisan dan pengolahan data/informasi pribadi, merupakan bagian yang beririsan langsung dalam suatu proses 'penelitian' pada umumnya.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)[145]

Aturan spesifik tentang perlindungan tata kelola sistem elektronik berikut pengaturan tentang informasi pribadi baru diatur separuhnya dalam UU ITE. Undang-undang tersebut diinisiasikan sejak 2005 namun akhirnya baru berhasil disahkan oleh Pemerintah dan DPR pada tahun 2008. Sepanjang perjalanannya UU ITE telah mengalami perubahan sekali pada 2016 dan selama itu pula telah menyita banyak perhatian publik lantaran implementasinya lebih banyak berfokus pada kebebasan berekspresi di internet; dibandingkan dengan esensi objektifnya guna mengurus perihal pengamanan transaksi digital.

Beberapa bab yang diatur dalam UU ITE diantaranya tentang Informasi, Dokumen dan Tanda Tangan Elektronik (Bab III); Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik (Bab IV); Transaksi Elektronik (Bab V); Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi (Bab VI); Perbuatan yang Dilarang (Bab VII); dan Peran Pemerintah dan Masyarakat (Bab IX); serta ketentuan Pidana (Bab XI). Meski diklaim kontraproduktif, namun pada bagian penjelasannya Undang-Undang ini mulai mengadopsi konsep privasi, yang kemudian disebut sebagai hak pribadi, sebagai dasar pelindungan data pribadi meski belum spesifik terakomodir dalam substansinya.[146]

Di samping itu, perlu dicermati juga bahwa penggunaan istilah 'Penyelenggara Sistem Elektronik' dalam UU ITE sejatinya bersifat umum dan luas; bukan hanya mencakup aktivitas pemrosesan data, tapi juga kegiatan pemberian layanan-layanan transaksi berbasis digital. Hal ini membuat urgensi perihal materi muatan pelindungan data pribadi semakin terasa karena belum secara adekuat terkandung dalam substansi UU ITE.
Dalam ketentuan umumnya, ada beberapa terminologi kunci yang diperkenalkan UU ITE, di antaranya:

- 'Informasi Elektronik' adalah satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.[147] Dari rumusan ini, data pribadi pengguna merupakan bagian dari informasi elektronik.

---

[144] *Ibid.*, Penjelasan Pasal 21 UU Nomor 39 Tahun 1999 tentang HAM: "Yang dimaksud dengan "menjadi objek penelitian" adalah kegiatan menempatkan seseorang sebagai yang dimintai komentar, pendapat atau keterangan yang menyangkut kehidupan pribadi dan data-data pribadinya serta direkam gambar dan suaranya."

[145] Indonesia, *Undang-Undang tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, UU No. 19 Tahun 2016, LN Nomor 251 Tahun 2016, TLN Nomor

[146] Lihat: *Ibid.*, Penjelasan Pasal 26 ayat (1).

[147] *Ibid.,* Pasal 1 angka 1.

- ‘Transaksi Elektronik’ adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.[148]
- ‘Dokumen Elektronik’ adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.[149] Berdasarkan rumusan ini, data pribadi pengguna yang tersimpan dalam format tertentu secara hukum menjadi dokumen elektronik.
- ‘Sistem Elektronik’ adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.[150] Rumusan ini secara tidak langsung menjelaskan bahwa aktivitas pemrosesan data pribadi secara terkomputerisasi adalah bagian dari kegiatan berbasis Sistem Elektronik.
- ‘Penyelenggara Sistem Elektronik’ adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.[151]
- ‘Pengirim’ adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.[152] Pemilik data pribadi yang mengirimkan data miliknya untuk diproses masuk dalam definisi subjek pengirim.
- ‘Penerima’ adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.[153] Pengendali data, dengan demikian, masuk dalam definisi penerima.

Spesifik tentang pengaturan keandalan sistem serta perlindungan data pribadi dalam UU ITE dielaborasikan dalam Tabel 4.2.1.1 di bawah.

Tabel 4.2.1.1 Pemetaan Substansi Pelindungan Data dalam UU ITE

No	Pasal (Ayat)	Redaksi	Wilayah Siklus Informasi	Konteks Prinsip Pengaturan	Catatan
1	15 (1)	Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab	*Storage*	*Security;*	-

[148] *Ibid.,* Pasal 1 angka 2.
[149] *Ibid.,* Pasal 1 angka 4.
[150] *Ibid.,* Pasal 1 angka 5.
[151] *Ibid.,* Pasal 1 angka 6A.
[152] *Ibid.,* Pasal 1 angka 18.
[153] *Ibid.,* Pasal 1 angka 19.

		terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.			
2	16 (1)	Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan; b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut; c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut; d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.	*Collection, Usage, Disclosure, Storage*	*Accuracy; Security & Confidentiality; Purpose Specification; Lawfulness, Fairness, and Transparency* .	Secara normatif sudah sesuai dengan GDPR di mana terdapat kewajiban operator untuk memberi notifikasi pada *data subjec*t. Selain itu, huruf (d) juga mendukung adanya *purpose specification*.
3	22	Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.	*Collection*	*Accuracy (Accessibility)*	Akses terhadap perubahan data dan informasi berguna menjaga tingkat akurasi dan kebaruan data.

4	26 (1)	Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi[154] seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.	*Usage*	*Lawfulness, Fairness, and Transparency*	Sesuai GDPR, perlu jadi catatan tentang penafsiran unsur 'ditentukan lain.'
5	26 (2)	Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.	*Usage*	*Accountability*	Hak gugat bagi subjek data terhadap kerugian termasuk atas pelanggaran privasi. Salah satu bentuk pelanggaran privasi, berdasarkan *best practice*, adalah penggunaan data untuk tujuan di luar yang diinformasikan di awal.
6	26 (3)*	Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.	*Storage & Disposal*	*Data Minimization;*	Penghapusan hanya berdasarkan permintaan *data subject,* sementara dalam GDPR penghapusan data yang tidak relevan didorong jadi inisiatif proaktif operator.
7	30 (1) jo. 46 (2)	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun [...] dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)	*Usage*	*Security*	Pidana untuk akses ilegal terhadap sistem elektronik secara fisik. Pasal ini berlaku tidak spesifik pada perolehan informasi.

[154] Penjelasan Pasal 26 ayat (1) UU Nomor 19 Tahun 2016: "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut: (a) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. (b) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai. (c) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

8	30 (2) jo. 46 (2)	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik [...] dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).	*Disclosure*	-	Spesifik untuk akses ilegal yang tujuannya mengambil informasi elektronik.
9	30 (3) jo. 46 (3)	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan [...] dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).	*Usage*	*Security & Confidentiality*	Berbeda dengan Pasal 30 ayat 1 yang bisa dilakukan secara fisik, aturan ini mengacu pada akses ilegal lewat peretasan jarak jauh jarak jauh.
10	35 jo. 51 (1)	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik [...] dipidana penjara paling lama 12 tahun dan denda paling banyak Rp 12 miliar.	*Storage & Disposal; Collection; Usage; Disclosure*	*Confidentiality & Security*	Secara umum norma pasal ini melindungi *data user* dari ragam serangan siber.
11	40 (2a)*	Pemerintah wajib melakukan pencegahan, penyebarluasan, dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.	*Storage Disposal (Data / Content Blocking)*	*Lawfulness*	Kewajiban diletakan menjadi inisiatif Pemerintah. Kontras berbeda dengan pedoman GDPR di mana pemerintah hanya sebagai regulator, bukan *decision maker*.
12	40 (2b)*	Dalam melakukan pencegahan, Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem			

		Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum			

*UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008

Hasil telaah terhadap materi muatan UU ITE menunjukan bahwa pengaturan pada level undang-undang tersebut belum cukup memadai untuk menunjang perlindungan data pribadi dalam standar GDPR. Sekalipun muatannya mengatur tentang lalu lintas informasi elektronik dan tanggung gugat penyelenggara sistem elektronik atas kegagalan sistemnya, namun belum adanya satu pun materi muatan pengaturan terkait *cross-border data flow* berikut kewajiban-kewajiban yang spesifik dalam pelindungan data pribadi membuat urgensi pembentukan suatu undang-undang khusus terkait privasi data menjadi tak terhindarkan. Aturan-aturan yang dimaksud sebelumnya bukan tidak ada, namun lebih banyak diatur pada level peraturan teknis, yang tentu saja mempunyai konsekuensi keberlakuan yang berbeda dengan aturan di level undang-undang.

4.2.2. Tingkat Peraturan Pelaksana

Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)[155]

Aturan ini merupakan pelaksana lebih lanjut dari UU ITE sebelumnya khususnya terkait sertifikasi elektronik, berikut juga subjek-subjek Penyelenggara Sistem Elektronik (PSE) yang dalam pelaksanaannya bertindak pula sebagai *data operator*. PP Nomor 71 Tahun 2019 tentang PSTE ini merupakan pengganti atas PP Nomor 82 Tahun 2012 sebelumnya. Patut menjadi catatan, pada PP PSE ini terdapat perubahan kebijakan terkait lokalisasi data elektronik strategis.[156] Jika sebelumnya PSTE lingkup publik wajib menempatkan di Indonesia, kini penempatan di luar Indonesia dimungkinkan dalam kondisi tidak ada teknologi penyimpanan yang mendukung di Indonesia. Di samping itu, lewat peraturan ini pemerintah memperkenalkan klasifikasi data berdasarkan risiko; data terdiri dari data berisiko rendah, tinggi, dan strategis. Hanya terhadap data-data 'strategis' saja—menyangkut kepentingan sektor publik[157] atau dikelola oleh PSE lingkup publik, yang penyimpanannya harus ditempatkan di wilayah Indonesia.[158]

Dirjen Aptika Kominfo, salah satu pihak perancang revisi PP PSTE menyebut data elektronik strategis sebagai "...data-data yang dibiayai oleh APBN, dana publik, dan sejenisnya...".[159] Pendekatan ini berbeda dengan PP sebelumnya, yang mewajibkan pula

---

[155] Indonesia, *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP Nomor 71 Tahun 2019, LN Nomor 185 Tahun 2019, TLN Nomor 6400.

[156] *Ibid*, Pasal 20.

[157] *Ibid.,* Pasal 99 ayat 2: "Instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi [..] meliputi: (a) sektor administrasi pemerintahan; (b) sektor energi dan sumber daya mineral; (c) sektor transportasi; (d) sektor keuangan; (e) sektor kesehatan; (f) sektor teknologi informasi dan komunikasi; (g) sektor pangan; (h) sektor pertahanan; dan (i) sektor lain yang ditetapkan oleh Presiden"

[158] Jonathan Patrick, "PP PSTE Atur Data Digital Publik Wajib Disimpan di Indonesia", *cnnindonesia.com*, 5 November 2019, diakses dari https://bit.ly/3zxSdzC.

[159] *Ibid.*

PSE lingkup privat yang menjalankan fungsi pelayanan publik berdasarkan UU Pelayanan Publik,[160] untuk memiliki *data center* di Indonesia.[161] Perubahan kebijakan lokalisasi data ini sempat memancing kritik dari beberapa pihak lantaran dianggap menghilangkan kedaulatan Indonesia atas data.[162] Lagipula, menurut Direktur Eksekutif Masyarakat Telekomunikasi (Mastel), Arki Rifazka, pasca berlakunya PP PSTE terbitan tahun 2012 sebelumnya, sudah banyak pelaku usaha yang menghabiskan banyak dana untuk membangun pusat data di Indonesia sehingga penghilangan kewajiban lokalisasi data bagi sektor privat dalam PP PSTE terbaru dianggap tidak konsisten dan cenderung merugikan.[163]

Hal ini juga disayangkan akan berdampak pada keberlanjutan bisnis para pelaku usaha *data center* lokal yang akan semakin kalah saing dengan pelaku usaha dari luar.[164] Pendapat berbeda diutarakan oleh Asosiasi Game Indonesia, bahwa kebijakan lokalisasi data di Indonesia memang sulit dilakukan mengingat pasar internet bersifat global, dan karenanya, mayoritas pengembang dalam industri itu lebih memilih penempatan data di luar negeri dibandingkan di Indonesia karena fasilitas keamanan yang lebih mendukung.[165] Pada PP ini, dengan kata lain, pemerintah tampak mulai berubah haluan pada upaya meliberalisasi restriksi penempatan data untuk menunjang tumbuh kembang industri teknologi informasi.

Lebih lanjut, materi muatan dalam Peraturan Pemerintah ini meliputi diantaranya, (1) kategori Penyelenggara Sistem Elektronik; kewajiban Penyelenggara Sistem Elektronik; penghapusan dan/atau penutupan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan; penempatan Sistem Elektronik dan Data Elektronik; pengawasan penyelenggaraan Sistem Elektronik; penyelenggaraan Agen Elektronik; Penyelenggaraan Transaksi Elektronik; penyelenggaraan Sertifikasi Elektronik. Beberapa pengertian umum yang dimuat dalam aturan ini namun tidak diatur dalam UU ITE, antara lain:

- ‘Perangkat Keras’ adalah satu atau serangkaian alat yang terhubung dalam Sistem Elektronik.
- ‘Perangkat Lunak’ adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik.

---

[160] Indonesia, Undang-Undang tentang Pelayanan Publik, UU No. 25 Tahun 2009, Pasal 1 angka 2: “Penyelenggara pelayanan publik yang selanjutnya disebut Penyelenggara adalah setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan undang-undang untuk kegiatan pelayanan publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik.” Lihat juga, Pasal 5 ayat 4 huruf c: “[...] penyediaan jasa publik yang pembiayaannya tidak bersumber dari anggaran pendapatan dan belanja negara atau anggaran pendapatan dan belanja daerah [...], tetapi ketersediaannya menjadi misi negara yang ditetapkan dalam peraturan perundang-undangan.”. Maka, sektor telekomunikasi tercakup dalam ruang lingkup pelayanan publik.

[161] Indonesia, Pasal 3 ayat (2) jo. Pasal 17 PP Nomor 82 Tahun 2012.

[162] “Poin-poin yang dianggap ancam kedaulatan RI di PP PSTE”, *cnnindonesia.com*, 7 November 2019, diakses dari https://bit.ly/35I7T5H.

[163] Oktarina P. Sandhy, “PP 71 Dinilai Tak Pro Industri Data Center Lokal”, *cyberthreat.id,* 1 November 2019, diakses dari https://cyberthreat.id/read/3628/PP-71-Dinilai-Tak-Pro-Industri-Data-Center-Lokal

[164] *Ibid.*

[165] Kontan, “Asosiasi Game: Kewajiban Data Center di Indonesia Sulit Diterapkan”, *kontan.co.id,* 26 November 2018, diakses dari https://bit.ly/3gIpxei.

- ‘Uji Kelaikan Sistem Elektronik’ adalah suatu rangkaian proses penilaian secara objektif terhadap setiap komponen Sistem Elektronik, baik dilakukan secara mandiri dan/atau dilakukan oleh institusi yang berwenang dan berkompeten.
- ‘Data Pribadi’ adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.
- ‘Data Elektronik’ adalah data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi.

Aturan ini mengkategorikan PSE menjadi dua lingkup, yakni, lingkup publik dan privat. PSE Lingkup Publik adalah penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau institusi yang ditunjuk oleh Instansi Penyelenggara Negara,[166] kecuali otoritas pengatur dan pengawas sektor keuangan.[167] Sementara, PSE Lingkup Privat adalah penyelenggaraan Sistem Elektronik oleh Orang, Badan Usaha, dan masyarakat.[168] Dengan demikian, termasuk dalam PSE Lingkup Privat adalah PSE yang memiliki portal, situs, atau aplikasi dalam jaringan internet yang dipergunakan untuk menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau perdagangan barang dan/atau jasa, layanan transaksi keuangan; pengiriman materi atau muatan digital berbayar melalui jaringan data baik dengan cara unduh melalui portal atau situs; pengiriman lewat surat elektronik, atau melalui aplikasi lain ke perangkat pengguna.

Selain itu, PSE Lingkup Privat juga mencakup penyedia layanan komunikasi (termasuk pesan singkat, panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial); layanan mesin pencari (*search engine*), layanan penyediaan Informasi Elektronik yang berbentuk tulisan, suara, gambar, animasi, musik, video, film, dan permainan atau kombinasi dari sebagian dan/atau seluruhnya; dan pemrosesan Data Pribadi untuk kegiatan operasional melayani masyarakat yang terkait dengan aktivitas Transaksi Elektronik.[169] Sejauh ini PP PSTE menjadi produk hukum positif yang paling komprehensif, meski tidak seutuhnya, mengadopsi GDPR sebagaimana terlihat dalam ketentuan Pasal 14 hingga 21. Sedangkan dalam konteks pengaturan terkait pemrosesan data, PP PSTE mengadopsi konsep siklus hidup informasi. Tahapan yang disebutkan terdiri dari:[170]

a. perolehan dan pengumpulan;
b. pengolahan dan penganalisisan;
c. penyimpanan;
d. perbaikan dan pembaruan;
e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau

[166] Indonesia, PP Nomor 71 Tahun 2019..., Pasal 1 angka 5
[167] *Ibid.*, Pasal 2 ayat 4.
[168] *Ibid.*, Pasal 1 angka 6.
[169] *Ibid.,* Pasal 2 ayat 5.
[170] *Ibid.,* Pasal 14 ayat (2).

f. penghapusan atau pemusnahan.

Catatan pada huruf (f), pembentuk peraturan sengaja melepaskannya sebagai wilayah pemrosesan sendiri, meski dalam GDPR pemusnahan dan penghapusan tersebut masuk dalam bagian pengaturan perihal penyimpanan *storage*. Lebih lanjut, pemetaan prinsip perlindungan data pribadi dalam PP PSTE terhadap GDPR dapat dielaborasikan dalam tabel 4.2.2.1 di bawah ini.

Tabel 4.2.2.1 Pemetaan Substansi Pelindungan Data dalam PP PSTE

No	Pasal (Ayat)	Redaksi	Lingkup Siklus Informasi	Konteks Prinsip Pengaturan	Catatan
1	3	Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.	Pemrosesan Data Secara Keseluruhan	*Security & Confidentiality*	Mengacu pada perangkat. Mengkompilasikan asas *liability, security,* dan *confidentiality* sekaligus. Pada GDPR, masing-masing asas dielaborasikan dalam pasal tersendiri.
2	4	Sepanjang tidak ditentukan lain undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan; b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam penyelenggaraan Sistem Elektronik tersebut; c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam	Pemrosesan Data secara Keseluruhan	*Lawfulness, Transparency; Accountability and Accessibility;*	Merupakan penjabaran lebih lanjut tentang aspek keandalan dan kemutakhiran perangkat sistem elektronik. Karena merupakan standar minimal, maka pendekatan ini berlaku sebagai *benchmark* untuk mengukur keandalan. PSE dapat menerapkan standar lebih tinggi.

		penyelenggaraan Sistem Elektronik tersebut; d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan Sistem Elektronik tersebut; dan e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.			
3	5 (2)	Penyelenggara Sistem Elektronik wajib memastikan Sistem Elektroniknya tidak memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sesuai dengan ketentuan perundang-undangan.	*Disclosure*	*Lawfulness; Accountability*	Fokus utamanya pada konten, tapi berada dalam ranah penyingkapan informasi.
4	7 (1) & (2)	Perangkat Keras yang digunakan oleh Penyelenggara Sistem Elektronik harus: a. memenuhi aspek keamanan, interkonektivitas dan kompatibilitas dengan sistem yang digunakan; […] Pemenuhan terhadap persyaratan sebagaimana dimaksud harus dilakukan melalui sertifikasi atau bukti-bukti sejenis lainnya.	*Storage;*	*Integrity and Confidentiality*	-
5	8	Perangkat Lunak yang digunakan oleh Penyelenggara Sistem Elektronik harus: a. terjamin keamanan dan keandalan operasi sebagaimana mestinya; dan b. memastikan keberlanjutan layanan.	*Storage*	*Integrity and Confidentiality*	-
6	9 (1)	Pengembang yang menyediakan Perangkat Lunak yang khusus	(Perangkat Lunak)	*Security*	Mengatur tentang kewajiban

		dikembangkan untuk Penyelenggara Sistem Elektronik Lingkup Publik wajib menyerahkan kode sumber dan dokumentasi atas Perangkat Lunak kepada Instansi atau institusi yang bersangkutan.			penerapan *Source Code*[171] atas software yang digunakan oleh PSE Badan Publik. Institusi yang bersangkutan dalam hal ini adalah pemerintah namun terdapat pengecualian dalam hal tidak tersedianya institusi tersebut, bisa diserahkan ke pihak ketiga yang terpercaya.
7	10 (1)	Tenaga ahli yang digunakan oleh Penyelenggara Sistem Elektronik harus memiliki kompetensi di bidang Sistem Elektronik atau Teknologi Informasi.	Pemrosesan Data secara Keseluruhan	*Accountability and Liability*	Ketentuan ini mengadopsi konsep *Data Protection Officer* (DPO) dalam GDPR. Namun, tidak dijelaskan kualifikasi PSE seperti apa yang wajib menggunakan DPO.
8	11 (1)	Penyelenggara Sistem Elektronik harus menjamin: tersedianya perjanjian tingkat layanan; (a) tersedianya perjanjian keamanan informasi terhadap jasa layanan Teknologi Informasi yang digunakan; (b) dan keamanan informasi dan sarana komunikasi internal yang diselenggarakan.	*Collection*	*Lawfulness, Fairness, and Transparency*	Perjanjian tingkat layanan mencerminkan adanya persetujuan (*consent)* atas penggunaan data, semisal, lewat *terms and condition* yang harus di-ceklis oleh *data subject*.
9	11 (2)	Penyelenggara Sistem Elektronik... harus menjamin setiap komponen dan keterpaduan seluruh Sistem Elektronik beroperasi sebagaimana mestinya.	*Storage*	*Integrity and Confidentiality*	Dimaksudkan agar user maupun kontroler dapat mengakses lokasi simpan dan

[171] *Source Code* atau kode sumber dijelaskan dalam bagian Penjelasan Pasal 8 ayat 1 PP PSTE, yaitu: "Suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami orang."

10	12	Penyelenggara Sistem Elektronik harus menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan.	*Storage*	*Accountability and Liability*	Tidak diatur standar tata kelola risiko yang andal. Bandingkan dengan GDPR yang mewajibkan PSE segera melaporkan ke pihak berwajib.
11	13	Penyelenggara Sistem Elektronik harus memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap Sistem Elektronik.	*Storage*	*Accountability and Liability*	Menjamin bahwa riwayat perlakuan atas data senantiasa terekam dan bisa dipertanggungjawabkan.
12	14 (1)	Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi meliputi: a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik Data Pribadi; b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya; c. pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi; d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi; e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan	Pemrosesan Data Secara Keseluruhan	Seluruh Prinsip GDPR	Pasal ini mengadopsi ketujuh prinsip tata kelola data dalam GDPR. Pemrosesan Data Pribadi sebagaimana dimaksud meliputi: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan f. dan/atau penghapusan atau pemusnahan

		pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi; f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan g. pemrosesan Data Pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan			
13	14 (3)	Pemrosesan Data Pribadi harus memenuhi ketentuan adanya persetujuan yang sah dari pemilik Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan kepada pemilik Data Pribadi.	*Collection*	*Lawfulness, Fairness and Transparency; Purpose Specification.*	Sesuai dengan GDPR: bahwa pengumpulan harus didasarkan atas persetujuan eksplisit dari *data subject.*
14	14 (4)	…Pemrosesan Data Pribadi harus memenuhi ketentuan yang diperlukan untuk: a. pemenuhan kewajiban perjanjian dalam hal pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan pemilik Data Pribadi pada saat akan melakukan perjanjian; b. pemenuhan kewajiban hukum dari pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; c. pemenuhan pelindungan kepentingan yang sah (vital interest) pemilik Data Pribadi; d. pelaksanaan kewenangan pengendali Data Pribadi berdasarkan ketentuan peraturan perundang-undangan;	*Collection; Usage*	*Lawfulness, Fairness and Transparency; Purpose Specification*	Tidak diatur mekanisme mengenai opsi alternatif bagi *data subject* yang tidak setuju.

		e. pemenuhan kewajiban pengendali Data Pribadi dalam pelayanan publik untuk kepentingan umum; dan/atau f. pemenuhan kepentingan yang sah lainnya dari pengendali Data Pribadi dan/atau pemilik Data Pribadi.			
15	14 (5)	Jika terjadi kegagalan dalam pelindungan terhadap Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut.	*Storage; Disclosure;* (*Breach of Data*)	*Security*	Notifikasi kepada data subject sudah sesuai GDPR. Namun, dalam hal pembobolan data, GPDR mewajibkan PSE melaporkan ke pihak berwajib selain menotifikasi *user*.
16	15 (1) & (2)	Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan. Kewajiban penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan sebagaimana dimaksud terdiri dari: penghapusan (*right to erasure*); dan pengeluaran dari daftar mesin pencari (*right to delisting).*	*Storage; Disclosure*	*Storage Limitation; Data Minimization ;*	Penegasan bahwa kewajiban penghapusan data tidak relevan jadi tanggung jawab PSE. Berbeda dengan UU ITE yang normanya bersifat non-imperatif.
17	16 (1)	Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang dilakukan penghapusan (*right to erasure*) sebagaimana dimaksud dalam terdiri atas Data Pribadi yang: a. diperoleh dan diproses tanpa persetujuan pemilik Data Pribadi; b. telah ditarik persetujuannya oleh pemilik Data Pribadi; c. diperoleh dan diproses dengan cara melawan hukum;	*Disposal*	*Lawfulness, Fairness, and Transparency; Storage Limitation; Purpose Specification ; Data Minimization*	Elaborasi lebih lanjut dari Pasal 15. Catatan atas huruf (b), PP PSE tidak menjelaskan adanya mekanisme penarikan persetujuan.

		d. sudah tidak sesuai lagi dengan tujuan perolehan berdasarkan perjanjian dan/atau ketentuan peraturan perundang-undangan; e. penggunaannya telah melampaui waktu sesuai dengan perjanjian dan/atau ketentuan peraturan perundang-undangan; dan/atau f. ditampilkan oleh Penyelenggara Sistem Elektronik yang mengakibatkan kerugian bagi pemilik Data Pribadi.			
18	17 (1) & (2)	Penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang dilakukan pengeluaran dari daftar mesin pencari (*right to delisting*) dilakukan berdasarkan penetapan pengadilan. Permohonan penetapan penghapusan Informasi Elektronik dan/atau Dokumen Elektronik kepada pengadilan negeri setempat dilakukan oleh orang yang bersangkutan sebagai pemilik Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.	*Disposal*		Ini merupakan bagian dari komponen hak privasi dalam bentuk *right to be forgotten*. Ketentuan *delisting* semestinya tak perlu melalui peradilan karena cenderung membebeani *data subject*. Namun dapat dipahami karena asumsi hukum dari pengaturan ini adalah bahwa pengumpulan data sudah diajukan berdasarkan *consent* dan perjanjian baku pengumpulan data.
19	18 (1) & (2)	Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan, yang paling sedikit memuat ketentuan mengenai: a. penyediaan saluran komunikasi antara	*Storage & Disposal*	*Data Minimisation*	-

		Penyelenggara Sistem Elektronik dengan pemilik Data Pribadi; b. fitur penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang memungkinkan pemilik Data Pribadi melakukan penghapusan Data Pribadinya; dan c. pendataan atas permintaan penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan.			
20	19 (1) & (2)	Penyelenggara Sistem Elektronik harus menerapkan tata kelola Sistem Elektronik yang baik dan akuntabel, yang paling sedikit memenuhi persyaratan: a. tersedianya prosedur atau petunjuk dalam penyelenggaraan Sistem Elektronik yang didokumentasikan dan/atau diumumkan dengan bahasa, informasi, atau simbol yang dimengerti oleh pihak yang terkait dengan penyelenggaraan Sistem Elektronik tersebut; b. adanya mekanisme yang berkelanjutan untuk menjaga kebaruan dan kejelasan prosedur pedoman pelaksanaan; c. adanya kelembagaan dan kelengkapan personel pendukung bagi pengoperasian Sistem Elektronik sebagaimana mestinya; d. adanya penerapan manajemen kinerja pada Sistem Elektronik yang. diselenggarakannya untuk memastikan Sistem Elektronik beroperasi sebagaimana mestinya; dan	Setiap Siklus Pemrosesan Data	*Accountability*	-

		e. adanya rencana menjaga keberlangsungan penyelenggaraan Sistem Elektronik yang dikelolanya.			
21	21 (1) & (2)	Penyelenggara Sistem Elektronik Lingkup Privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia. Dalam hal Sistem Elektronik dan Data Elektronik dilakukan pengelolaan, pemrosesan, dan/atau penyimpanan di luar wilayah Indonesia, Penyelenggara Sistem Elektronik Lingkup Privat wajib memastikan efektivitas pengawasan oleh Kementerian atau Lembaga dan penegakan hukum.	*Storage; Disclosure*	*Security; Accountability*	Aturan ini beririsan dengan *Cross-Border Data Flow.* Patut jadi catatan bagaimana database di luar yurisdiksi Indonesia tersebut bisa diawasi mengingat beberapa negara melarang adanya otoritas *non-data controller* dari luar untuk mengakses database di negaranya.
22	22	Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik.	*Collection; Usage; Storage;*	*Transparency; Accuracy*	Riwayat audit untuk keperluan penegakan hukum, penyelesaian sengketa, verifikasi, pengujian.
23	24 (1)	Penyelenggara Sistem Elektronik wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian.	Seluruh Tahap Siklus Pemrosesan Data	*Security; Accountability*	Tidak menyangkut salah satu tahapan pemrosesan data, melainkan pada pengelolaan perangkat sistem elektronik secara umum dan keseluruhan.
24	24 (2)	Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.			
25	24 (3)	Dalam hal terjadi kegagalan	*Storage;*	*Security;*	Ketentuan ini mirip

		atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara Sistem Elektronik wajib mengamankan Informasi Elektronik dan/atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait.	*Disclosure (Breach)*	*Accountability; Transparency*	dengan Pasal 14 ayat (5) namun spesifik mewajibkan pelaporan ke aparat penegak hukum.
26	26	Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keotentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan. Dalam penyelenggaraan Sistem Elektronik yang ditujukan untuk Informasi Elektronik dan/atau Dokumen Elektronik yang dapat dipindahtangankan, Informasi Elektronik dan/atau Dokumen Elektronik harus unik serta menjelaskan penguasaan dan kepemilikannya.	*Storage*	*Confidentiality; Accuracy; Accessibility*	Menegaskan bahwa data yang dikumpulkan harus bisa teridentifikasi agar bisa sewaktu-waktu diakses kembali oleh subjek data.
27	29	Penyelenggara Sistem Elektronik wajib menyampaikan informasi kepada Pengguna Sistem Elektronik paling sedikit mengenai: a. identitas Penyelenggara Sistem Elektronik; b. objek yang ditransaksikan; c. kelaikan atau keamanan Sistem Elektronik; d. tata cara penggunaan perangkat; e. syarat kontrak; f. prosedur mencapai kesepakatan; g. jaminan privasi dan/atau pelindungan Data Pribadi;	*Collection*	*Transparency; Security; Accountability*	Norma ini umumnya berlaku di setiap siklus pemrosesan data, namun paling krusial sebelum pengumpulan.

		dan h. nomor telepon pusat pengaduan.			
28	30 (1) & (2)	Penyelenggara Sistem Elektronik wajib menyediakan fitur sesuai dengan karakteristik Sistem Elektronik yang digunakannya. Fitur sebagaimana dimaksud paling sedikit berupa fasilitas untuk: a. melakukan koreksi; b. membatalkan perintah; c. memberikan konfirmasi atau rekonfirmasi; d. memilih meneruskan atau berhenti melaksanakan aktivitas berikutnya; e. melihat informasi yang disampaikan berupa tawaran Kontrak Elektronik atau iklan; f. mengecek status berhasil atau gagalnya Transaksi Elektronik; dan g. membaca perjanjian sebelum melakukan Transaksi Elektronik.	*Collection; Usage; Storage;*	*Accuracy; Accessability ; Transparency*	Karakteristik disesuaikan dengan sistem elektronik yang digunakan. Misal, penyedia marketplace harus menempatkan fitur pembatalan jika transaksi yang dibuat pengguna mengalami kekeliruan.

Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) [172]

Spesifik dalam konteks perdagangan melalui sistem elektronik, pelindungan data pribadi diatur dalam PP PMSE. Aturan tentang PDP hanya muncul dalam dua pasal yang diakomodir Bab XI tentang Perlindungan Data Pribadi (Pasal 58-59), dari total 82 pasal yang diatur PP ini. Konstruksi PP PMSE menegaskan bahwa data pribadi sebagai hak milik orang yang bersangkutan: "Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau Pelaku Usaha yang bersangkutan."[173] Dimasukkannya frasa 'pelaku usaha yang bersangkutan' sebagai pemilik sebenarnya problematik, sebab dengan begitu pelaku usaha selaku pengendali data diasumsikan dapat memanfaatkan data-data yang dikumpulkan untuk kepentingan yang bertentangan dengan privasi subjek data.

Lebih jauh, ketentuan pada ayat selanjutnya mengatur bahwa setiap pelaku usaha [dalam sistem elektronik] yang memperoleh data pribadi wajib bertindak sebagai pengemban amanat dalam menyimpan dan menguasai data pribadi sesuai dengan

[172] Indonesia, *Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik*, PP Nomor 80 Tahun 2019, LN Nomor 222 Tahun 2019, TLN Nomor 6420.

[173] *Ibid.*, Pasal 58 ayat (1).

ketentuan peraturan perundang-undangan.[174] Berdasarkan bagian penjelasan yang tersedia, yang dimaksud 'pengemban amanat' sesuai ketentuan hukum mengharuskan pengendali data hanya menggunakan data sesuai peruntukannya—atau sejalan dengan asas *purpose limitation*. Selanjutnya, Pasal 59 ayat 1 disebutkan bahwa pelaku usaha wajib menyimpan data pribadi sesuai standar pelindungan atau praktik bisnis yang berkembang, namun artikulasi ini pun agak membingungkan mengingat standar pelindungan umumnya mengacu pada regulasi positif, sementara praktik bisnis bisa bersifat supranasional. Pada penjelasannya, standar praktik bisnis umum yang dimaksud mengacu pada GDPR dan APEC *Privacy Frameworks*.[175] Pelindungan data pribadi pada PP PMSE dapat dijabarkan pada tabel di bawah.

Tabel 4.2.2.2 Pementaan Regulasi PDP Pada PP PMSE

No	Redaksi Pengaturan	Siklus Pemrosesan Data	Relevansi Asas dengan GDPR
1	Data pribadi harus diperoleh secara jujur dan sah dari pemilik data pribadi yang bersangkutan disertai dengan adanya pilihan dan jaminan adanya upaya pengamanan dan pencegahan kerugian pemilik data tersebut.[176]	*Collection*	*Lawfulness, Fairness, and Transparency; Integrity and Confidentiality; Security*
2	Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang dideskripsikan secara spesifik dan sah serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut.[177]	*Usage*	*Purpose Specificaton;*
3	Data pribadi yang diperoleh harus layak, relevan, dan tidak terlalu luas dalam hubungannya dengan tujuan pengolahannya sebagaimana disampaikan sebelumnya kepada pemilik data.[178]	*Collection; Usage*	*Data minimation*
4	Data pribadi harus akurat dan harus selalu *up-to-date* dengan memberikan kesempatan kepada pemilik data untuk memutakhirkan data pribadinya.[179]	*Storage*	*Accuracy; Accessibility*
5	Data pribadi harus diproses sesuai dengan tujuan perolehan dan peruntukannya serta tidak boleh dikuasai lebih lama dari waktu yang diperlukan.[180]	*Usage; Storage*	*Purpose limitation;*
6	Data pribadi harus diproses sesuai dengan hak subyek pemilik data sebagaimana diatur dalam peraturan perundang-undangan.[181]	*Usage*	*Lawfulness*

[174] *Ibid.,* Pasal 58 ayat (2).
[175] Lihat Penjelasan Pasal 58 ayat (2).
[176] *Ibid.,* Pasal 59 ayat (2) huruf a.
[177] *Ibid.*, Pasal 59 ayat (2) huruf b.
[178] *Ibid.,* Pasal 59 ayat (2) huruf c.
[179] *Ibid.,* Pasal 59 ayat (2) huruf d.
[180] *Ibid.,* Pasal 59 ayat (2) huruf e.
[181] *Ibid.,* Pasal 59 ayat (2) huruf f.

7	Pihak yang menyimpan data pribadi harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran atau mencegah setiap kegiatan pemrosesan atau pemanfaatan data pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi tersebut.[182]	*Storage*	*Integrity & Confidentiality; Security; Accountability*
8	Data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia.[183]	*Disclosure*	
7	Dalam hal pemilik data pribadi menyatakan keluar, berhenti berlangganan atau berhenti menggunakan jasa dan sarana PMSE, maka pemilik data pribadi berhak meminta Pelaku Usaha untuk menghapus seluruh data pribadi yang bersangkutan.[184]	*Storage/Disposal*	*Accessability; Storage Limitation*
8	Pelaku usaha yang melanggar ketentuan Pasal 59 ayat (1) [kewajiban menyimpan data pribadi sesuai standar dan praktik bisnis yang berkembang] dikenai sanksi administratif oleh Menteri.[185] Sanksi administratif yang dimaksud berupa:[186] a. Teguran tertulis; b. Dimasukan dalam daftar prioritas pengawasan; c. Dimasukan dalam daftar hitam; d. Pemblokiran sementara layanan; e. Pencabutan izin usaha;	*Storage*	*Accountability* [Pengenaan sanksi administratif]

Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permen Kominfo PDPSE)[187]

Spesifik dalam hal PDP Permen Kominfo Nomor 20 Tahun 2016 mencakup seluruh perlindungan dalam tiap siklus informasi antara lain, (a) perolehan, pengumpulan, (b) penganalisisan penyimpanan, (c) penampilan, pengumuman, (d) pengiriman, penyebarluasan, dan pemusnahan.[188] Peraturan Menteri ini juga memberikan tambahan

[182] *Ibid.,* Pasal 59 ayat (2) huruf g.
[183] *Ibid.,* Pasal 59 ayat (2) huruf h.
[184] Ibid., Pasal 59 ayat (3).
[185] *Ibid.*, Pasal 80 ayat (1).
[186] *Ibid.*, Pasal 80 ayat (2).
[187] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik*, Permen Kominfo Nomor 20 Tahun 2016, Berita Negara Nomor 1829.
[188] *Ibid.*, Pasal 2 ayat (1). Spesifik dalam siklus informasi tersebut, sistematika peraturan ini dibagi menjadi beberapa bagian. Tentang perolehan dan pengumpulan (*collection*) diatur pada bagian Kedua; bagian ketiga mengatur tentang pengolahan dan penganalisisan (*usage*); bagian keempat mengatur tentang

definisi seputar hukum PDP yang sebelumnya tidak diatur dalam PP maupun UU ITE, antara lain:

- 'Data Perseorangan Tertentu' adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.[189]
- 'Pemilik Data Pribadi' adalah individu yang padanya melekat Data Perseorangan Tertentu.

Terlihat di sini ada perbedaan definisi Data Pribadi dalam Permen Kominfo PDPSE dengan PP PSE. 'Data Pribadi', dalam konteks Permen ini, merujuk pada tiap data yang merupakan 'data perseorangan tertentu', yang artinya tidak spesifik pada data yang terkumpul dalam sistem elektronik. Perbedaan tadi membuat definisi PDP jadi tidak sinkron dalam satu regulasi dengan lainnya.

Lebih jauh, *beleid* ini juga menetapkan beberapa asas terkait perlindungan data pribadi yang baik, yakni:[190]

a. Asas penghormatan terhadap data pribadi sebagai privasi;
b. Asas kerahasiaan; bahwa data pribadi bersifat rahasia sesuai persetujuan[191] dan/atau berdasarkan ketentuan peraturan perundang-undangan;
c. Asas konsensualitas (berdasarkan persetujuan);
d. Asas relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
e. Asas kelaikan Sistem Elektronik yang digunakan;
f. Asas iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi;
g. ketersediaan aturan internal pengelolaan perlindungan Data Pribadi;
h. tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna;
i. Asas kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi; dan
j. Asas keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.

Dari aspek substansinya, terlihat kiblat politik pembuat Permen Kominfo PDPSE mengadopsi model PDP Uni-Eropa dalam GDPR berikut Derivatif PDP sebelumnya. Sementara, Pasal 26 Permen Kominfo PDPSE menegaskan diadopsinya konsep hak individu atas data pribadi, yakni:

"Pemilik Data Pribadi berhak:
a. atas kerahasiaan Data Pribadinya;

---

penyimpanan (*storage*); bagian kelima tentang penampilan, pengumuman, pengiriman, pembukaan, dst (*disclosure*); dan bagian keenam tentang penghapusan (*disposal*).

[189] *Ibid.*, Pasal 1 angka 2.

[190] *Ibid.*, Pasal 2 ayat (2).

[191] *Ibid.*, Pasal 1 angka 4 Permen Kominfo PDP SE mendefinisikan 'Persetujuan' sebagai pernyataan secara tertulis baik secara manual dan/atau elektronik yang diberikan oleh Pemilik Data Pribadi setelah mendapat penjelasan secara lengkap mengenai tindakan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan serta kerahasiaan atau ketidakrahasiaan Data Pribadi.

b. mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri;
c. mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
d. mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan
e. meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan."

Sementara, pengguna (*data user*) berkewajiban untuk (a) menjaga kerahasiaan data pribadi yang diperoleh, dikumpulkan, diolah dan dianalisisnya; (b) menggunakan data pribadi sesuai dengan kebutuhan pengguna saja; (c) melindungi data pribadi beserta dokumen yang memuat data pribadi dari tindakan penyalahgunaan; (d) bertanggung jawab atas data pribadi yang terdapat dalam penguasaannya, baik penguasaan secara organisasi yang menjadi kewenangannya maupun perorangan, jika terjadi tindakan penyalahgunaan.[192] Lebih jauh, beberapa substansi pasal yang penting dalam *beleid* ini dapat ditabulasikan sebagai berikut:

Tabel 4.2.2.3 Pemetaan Regulasi Permen Kominfo PDPSE

No	Pasal (Ayat)	Redaksi	Siklus Informasi	Prinsip yang Diatur	Catatan
1	3	Perlindungan Data Pribadi dalam Sistem Elektronik dilakukan pada proses: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. penampilan, pengumuman, pengiriman, penyebarluasan, dan/atau pembukaan akses; dan e. pemusnahan.	Seluruh tahap pemrosesan data	-	Mengadopsi derivatif PDP UE; Sudah sesuai dengan wilayah konsentrasi pengaturan di GDPR. Seluruh proses a hingga e untuk selanjutnya disebut 'pemrosesan data'.
2	4	Sistem Elektronik yang digunakan untuk pemrosesan data wajib tersertifikasi.		*Security*	Pengaturan teknis tentang sertifikasi diatur dalam Peraturan BSSN.
3	5 (1)	Setiap Penyelenggara Sistem Elektronik harus mempunyai aturan internal perlindungan		*Lawfulness, Fairness, Transparency*	PSE harus memiliki aturan internal terkait pemrosesan data pada

[192] *Ibid.,* Pasal 27.

		Data Pribadi untuk melaksanakan pemrosesan.		*; Integrity & Confidentiality*	masing-masing tahapan siklus hidup informasi.
4	5 (2)	Setiap Penyelenggara Sistem Elektronik harus menyusun aturan internal perlindungan Data Pribadi sebagai bentuk tindakan pencegahan untuk menghindari terjadinya kegagalan dalam perlindungan Data Pribadi yang dikelolanya.		*Security; Accountability*	PSE pada prinsipnya harus punya mekanisme mitigasi. Kebijakan ini umumnya disebut '*privacy policy*'.
5	6	Penyelenggara Sistem Elektronik yang melakukan pemrosesan data wajib menyediakan formulir persetujuan dalam Bahasa Indonesia untuk meminta Persetujuan dari Pemilik Data Pribadi yang dimaksud.	*Collection*	*Lawfulness, Fairness, and Transparency (Consent)*	Asas konsensualisitas jadi basis pengumpulan. Jika Pemilik Data Pribadi merupakan orang yang termasuk dalam kategori anak, pemberian Persetujuan dilakukan oleh orang tua atau wali dari anak yang bersangkutan.[193]
6	7 (1)	Perolehan dan pengumpulan Data Pribadi oleh Penyelenggara Sistem Elektronik harus dibatasi pada informasi yang relevan dan sesuai dengan tujuannya serta harus dilakukan secara akurat.		*Purpose Limitation*	Dalam ayat 2 pasal ini menyebut bahwa Instansi Pengawas dan Pengawas Sektor dapat menentukan informasi yang relevan dan sesuai dengan tujuannya.
7	8 (1) & (2)	Dalam memperoleh dan mengumpulkan Data Pribadi, Penyelenggara Sistem Elektronik harus menghormati Pemilik Data Pribadi atas Data Pribadinya yang bersifat privasi. Penghormatan terhadap Pemilik Data Pribadi atas Data Pribadi yang bersifat privasi sebagaimana dimaksud dilakukan melalui		*Confidentiality; Accessibility.*	Rumusan ayat (1) agak membingungkan sebab Data Pribadi memang bersifat privasi. Pengulangannya membuat redaksinya terkesan kalimat informatif. Penggunaan kata 'harus' juga tidak ideal, semestinya 'wajib' karena topik

[193] *Ibid.*, Pasal 37.

		penyediaan pilihan dalam Sistem Elektronik untuk Pemilik Data Pribadi terhadap: a. kerahasiaan atau ketidakrahasiaan Data Pribadi; dan b. perubahan, penambahan, atau pembaruan Data Pribadi.			yang diangkat adalah privasi. Meski demikian, pasal ini menegaskan bahwa data adalah hak individu yang lekat pada *data subject*. Ketersediaan pilihan sebagaimana dimaksud tidak berlaku jika peraturan perundang-undangan telah secara tegas menyatakan Data Pribadi yang secara khusus untuk beberapa elemennya dinyatakan bersifat rahasia.
8	9 (1) & (2)	Perolehan dan pengumpulan Data Pribadi oleh Penyelenggara Sistem Elektronik wajib berdasarkan Persetujuan atau berdasarkan ketentuan peraturan perundang-undangan. Pemilik Data Pribadi yang memberikan Persetujuan dapat menyatakan Data Perseorangan Tertentu miliknya bersifat rahasia.		*Lawfulness (Consent)*	Pada praktiknya tak banyak PSE yang memberi opsi kepada pengguna untuk memilih status data pribadi bersifat rahasia. Semestinya dibuat aturan lebih lanjut perihal perlakuan yang harus dilakukan kolektor ketika subjek data mendeklarasikan datanya rahasia.
9	10	Data Pribadi yang diperoleh dan dikumpulkan secara langsung harus diverifikasi ke Pemilik Data Pribadi. Data Pribadi yang diperoleh dan dikumpulkan secara tidak langsung harus diverifikasi berdasarkan hasil olahan berbagai sumber data. Sumber data dalam perolehan dan pengumpulan Data Pribadi sebagaimana dimaksud harus memiliki dasar hukum yang sah.		*Transparency ; Accuracy*	Tidak disebut metode verifikasinya seperti apa. Bisa jadi, cukup notifikasi ke *data subject* lewat. Lalu, tingkat legalitas pengumpulan data perlu dicermati sebab jika hanya berbasis pada *asas konsensualitas* data subjek bisa saja berada dalam posisi tawar rendah (*take it or leave it position*).

10	11	Sistem Elektronik yang digunakan untuk menampung perolehan dan pengumpulan Data Pribadi harus memiliki kemampuan interoperabilitas dan kompatibilitas, serta menggunakan perangkat lunak (*software)* yang legal.		*Lawfulness; Security*;	
11	12	Data Pribadi hanya dapat diolah dan dianalisis sesuai kebutuhan Penyelenggara Sistem Elektronik yang telah dinyatakan secara jelas saat memperoleh dan mengumpulkannya. Pengolahan dan penganalisisan Data Pribadi dilakukan berdasarkan Persetujuan.	*Usage*	*Data Minimization*;	Ketentuan ini tidak berlaku jika Data Pribadi yang diolah dan dianalisis tersebut berasal dari Data Pribadi yang telah ditampilkan atau diumumkan secara terbuka oleh Sistem Elektronik untuk pelayanan publik.[194]
12	14	Data Pribadi yang diolah dan dianalisis harus telah diverifikasi keakuratannya.		*Accuracy*	Hanya data yang akurat yang bisa dimanfaatkan.
13	15 (1)	Data Pribadi yang disimpan dalam Sistem Elektronik harus Data Pribadi yang telah diverifikasi keakuratannya.	*Storage*	*Accuracy*	Dalam siklus GDPR, prinsip akurasi terletak pada tahap *usage/processing*, bukan *storage.*
	15 (2)	Data Pribadi yang disimpan dalam Sistem Elektronik harus dalam bentuk data terenkripsi.		*Security;*	
14	15 (3)	Data Pribadi wajib disimpan dalam Sistem Elektronik sesuai dengan (a) ketentuan peraturan perundang-undangan yang mengatur kewajiban jangka waktu penyimpanan Data Pribadi pada masing-masing Instansi Pengawas dan Pengatur Sektor; Atau (b) *paling singkat 5 (lima) tahun* jika belum terdapat ketentuan peraturan perundang-undangan yang		*Storage Limitation*	Pengaturan jangka waktu penyimpanan saat ini adalah 5 (lima) tahun mengingat belum adanya regulasi spesifik tentang itu. Selama masa waktu penyimpanan itu, jika terjadi pelanggaran, PSE harus bertanggung jawab.

[194] *Ibid.*, Pasal 13.

		secara khusus mengatur untuk itu.			
15	16	Jika Pemilik Data Pribadi tidak lagi menjadi Pengguna, Penyelenggara Sistem Elektronik wajib menyimpan Data Pribadi tersebut sesuai batas waktu terhitung sejak tanggal terakhir Pemilik Data Pribadi menjadi Pengguna.		*Security of Processing*	Tidak ada penjelasan bagaimana seseorang dikatakan berhenti menjadi pengguna PSE
16	17	Pusat data (*data center*)[195] dan pusat pemulihan bencana (*disaster recovery center*)[196] Penyelenggara Sistem Elektronik *untuk pelayanan publik* yang digunakan untuk proses perlindungan Data Pribadi *wajib ditempatkan dalam* wilayah negara Republik Indonesia.		*Storage Limitation*	Lokalisasi data untuk PSE lingkup Publik wajib berada di wilayah teritori Indonesia.
17	18	Penyimpanan Data Pribadi dalam Sistem Elektronik harus dilakukan sesuai dengan ketentuan mengenai prosedur dan sarana pengamanan Sistem Elektronik.	*Storage*	*Integrity & Confidentiality*	Diatur dalam PP PSE
18	19	Jika waktu penyimpanan Data Pribadi telah melebihi batas waktu sebagaimana dimaksud dalam Pasal 15 ayat (2), Data Pribadi dalam Sistem Elektronik dapat dihapuskan, kecuali Data Pribadi tersebut masih akan dipergunakan atau dimanfaatkan sesuai dengan tujuan awal perolehan dan pengumpulannya.	*Storage / Disposal (& Usage)*	*Storage Limitation*	Pengecualian dalam aturan ini membuatnya tidak konsisten dengan konsepsi masa retensi. Semestinya inisiatif penghapusan dilakukan segera setelah masa waktu retensi berakhir.

[195] Pusat data (*data center*) merupakan suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data [Pasal 17 ayat (2) Permen Kominfo PDPSE].

[196] Pusat pemulihan bencana (*disaster recovery center*) merupakan suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat bencana yang disebabkan oleh alam dan/atau manusia [Pasal 17 ayat (3) Permen Kominfo PDPSE]

19	20	Jika Pemilik Data Pribadi meminta penghapusan Data Perseorangan Tertentu miliknya, permintaan penghapusan tersebut dilakukan sesuai dengan ketentuan peraturan perundang-undangan	*Storage / Disposal*	*Accessibility; Lawfulness*	Hak atas pengapusan (*the right to be forgotten*)
20	21	Menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan/atau membuka akses Data Pribadi dalam Sistem Elektronik hanya dapat dilakukan: a. atas Persetujuan kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; dan b. setelah diverifikasi keakuratan dan kesesuaian dengan tujuan perolehan dan pengumpulan Data Pribadi tersebut.	*Disclosure / Transfer*	*Lawfulness (Consent); Purpose Limitation; Accuracy;*	Keharusan ini termasuk pula kegiatan *disclosure* yang dilakukan antar Penyelenggara Sistem Elektronik, antar Penyelenggara Sistem Elektronik dan Pengguna, atau antar Pengguna
21	22 (1) & (2)	Pengiriman Data Pribadi yang dikelola oleh Penyelenggara Sistem Elektronik pada instansi pemerintah dan pemerintahan daerah serta masyarakat atau swasta yang berdomisili di dalam wilayah negara Republik Indonesia ke luar wilayah negara Republik Indonesia harus: a. berkoordinasi dengan Menteri atau pejabat/lembaga yang diberi wewenang untuk itu; dan b. menerapkan ketentuan peraturan perundang-undangan mengenai pertukaran Data Pribadi lintas batas negara. Koordinasi sebagaimana dimaksud berupa: a. melaporkan rencana	*Disclosure / Transfer*		Mengatur tentang mekanisme *cross-border data transfer*. Disebut pada ayat 1 huruf (b) harus taat pada ketentuan peraturan perundang-undangan terkait PDP, namun aturan spesifik terkait hal itu saat ini belum tersedia. Penggunaan istilah 'koordinasi' dengan otoritas menjelaskan bahwa Kementerian tidak berwenang melakukan penolakan atau pemberian keputusan atas cross-border data transfer. Aturan ini berbeda dengan RUU PDP yang menyediakan beberapa opsi kriteria transfer data, terutama persetujuan dari pemilik data.

		pelaksanaan pengiri-man Data Pribadi, paling sedikit memuat nama jelas negara tujuan, nama jelas subjek penerima, tanggal pelaksanaan, dan alasan/tujuan pengiriman; b. meminta advokasi, jika diperlukan; dan c. melaporkan hasil pelaksanaan kegiatan			
22	23 (1) & (2)	Untuk keperluan proses penegakan hukum, Penyelenggara Sistem Elektronik wajib memberikan Data Pribadi yang terdapat dalam Sistem Elektronik atau Data Pribadi yang dihasilkan oleh Sistem Elektronik atas permintaan yang sah dari aparat penegak hukum berdasarkan ketentuan peraturan perundang-undangan. Data Pribadi sebagaimana dimaksud merupakan Data Pribadi yang relevan dan sesuai dengan kebutuhan penegakan hukum.	*Disclosure / Transfer*		Perlu dibuat peraturan pelaksana yang mengelaborasi data-data apa saja yang masuk kriteria relevan untuk penegakan hukum guna membatasi akses data yang non-relevan. Ini penting sebab dalam konteks penegakan hukum otoritas kerap meminta bukti sebanyak-banyaknya.
23	24 (1) & (2)	Penggunaan dan pemanfaatan Data Pribadi yang ditampilkan, diumumkan, diterima, dan disebarluaskan oleh Penyelenggara Sistem Elektronik harus berdasarkan Persetujuan. Penggunaan dan pemanfaatan Data Pribadi sebagaimana dimaksud […] harus sesuai dengan tujuan perolehan, pengumpulan, pengolahan, dan / atau penganalisisan Data Pribadi.	*Disclosure / Transfer, Usage*		Ketentuan ini sejatinya terletak di bagian *disclosure*, namun redaksinya terdengar mengatur soal *usage* dari pihak ketiga. Sebagai catatan, model persetujuan yang diberikan seperti apa. Apakah cukup persetujuan di awal untuk berlaku pada tiap tahap pemrosesan, atau pada tiap-tiap tahap perlu persetujuan sendiri-sendiri?
24	25 (1)	Pemusnahan Data Pribadi dalam Sistem Elektronik	*Storage/ Disposal*	*Storage Limitation*	

		hanya dapat dilakukan jika: a. telah melewati ketentuan jangka waktu penyimpanan […] berdasarkan Peraturan Menteri ini atau sesuai dengan ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing Instansi Pengawas dan Pengatur Sektor untuk itu; atau b. atas permintaan Pemilik Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.			
25	25 (2)	Pemusnahan sebagaimana dimaksud […] harus menghilangkan sebagian atau keseluruhan dokumen terkait Data Pribadi, […] elektronik maupun nonelektronik yang dikelola oleh Penyelenggara Sistem Elektronik dan/atau Pengguna sehingga […] tidak dapat ditampilkan kembali dalam Sistem Elektronik kecuali Pemilik Data Pribadi memberikan […] yang baru.		*Data Minimization*	
	35 (3) & (4)	[Dalam konteks Pengawasan] Menteri berwenang meminta data dan informasi dari Penyelenggara Sistem Elektronik dalam rangka perlindungan Data Pribadi. Permintaan data dan informasi sebagaimana dimaksud […] dapat dilakukan secara berkala atau sewaktu-waktu apabila diperlukan	*Disclosure*	*Accountability and Liability*	Aturan ini ini rentan membuka peluang terjadinya pelanggaran privasi atas data pribadi, padahal sudah disebutkan bahwa tiap-tiap pengumpulan data wajib otorisasi *data subject*.

Sementara perihal mekanisme sanksi terhadap pemrosesan data tanpa hak dan melanggar *beleid* ini, Permen Kominfo PDPSE mengadopsi pendekatan administratif berupa peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, atau pengumuman di

situs dalam jaringan.[197] Pendekatan kebijakan ini berbeda dengan GDPR yang secara tegas menggunakan sistem denda. Lebih jauh, ada beberapa aturan lain yang diatur namun tidak ter tabulasi di atas, seperti penyelesaian sengketa,[198] peran serta masyarakat,[199] pengawasan,[200] dst.

Peraturan Menteri Komunikasi dan Informatika tentang Penyelenggaraan Sistem Elektronik Lingkup Privat (Permen Kominfo PSE-LP)[201]

Permen Kominfo PSE-LP diterbitkan untuk menggantikan Permenkominfo Nomor 14 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, dan Permenkominfo Nomor 36 Tahun 2014 tentang . Sesuai namanya, *beleid* ini mengatur beberapa aspek perihal kewajiban PSE lingkup privat. *Pertama*, kewajiban pendaftaran bagi PSE lingkup privat (PSE-LP). Artinya, hanya PSE yang terdaftar saja yang dapat menyediakan layanannya di Indonesia. Adapun yang dimaksud PSE-LP adalah perusahaan penyedia layanan aplikasi termasuk sosial media seperti Instagram, Facebook, dst. *Kedua*, penjatuhan sanksi administrasi dan normalisasi. *Ketiga*, kewajiban PSE lingkup privat terhadap *user generated content*, dan kewajiban penyelenggara komputasi awan (*cloud computation*). *Keempat*, dan yang belakangan merupakan paling kontroversial dikritisi, kewajiban pemutusan akses dan pemblokiran konten. Peraturan ini awalnya diwacanakan akan berlaku sejak akhir Mei 2021, namun mengalami penundaan hingga akhir Desember 2021.[202] Penundaan itu dilakukan lantaran sistem pendaftaran milik Kemkominfo belum memadai.

Lebih jauh, berbeda dengan format tabulasi sebelumnya, dalam Permen Kominfo PSE-LP pengaturannya tidak secara spesifik dapat dipetakan berdasarkan siklus pemrosesan informasi mengingat pengartikulasian normanya bersifat acak. Sehingga, pemetaan regulasinya hanya dapat dilakukan berdasarkan aspek asas atau prinsip yang dikenal dalam praktik PDP. Adapun beberapa norma penting dalam Permen Kominfo PSE-LP yang memiliki irisan dengan pengaturan proteksi privasi adalah sebagai berikut:

Tabel 4.2.2.4 Pemetaan Regulasi Permenkominfo PSE-LP

No	Pasal (Ayat)	Redaksi	Relevansi Prinsip	Catatan
1	2 (1) & (2)	Setiap PSE Lingkup Privat wajib melakukan pendaftaran. SE Lingkup Privat sebagaimana dimaksud […] meliputi: a. Penyelenggara Sistem Elektronik *yang*	*Lawfulness*	Pendaftaran platform menyangkut aspek legalitas. Ini diperlukan agar platform yang memberi layanan terawasi oleh otoritas

[197] Pasal 36 ayat (1) Permen Kominfo PDPSE.
[198] Pasal 29 sampai 33 Permen Kominfo PDPSE.
[199] Pasal 34 Permen Kominfo PDPSE.
[200] Pasal 35 Permen Kominfo PDPSE.
[201] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Penyelenggaraan Sistem Elektronik Lingkup Privat*, Permen Kominfo Nomor 5 Tahun 2020, Berita Negara Nomor 1376 Tahun 2020.
[202] Novina P. Besari, "Sistem Tak Siap, Pendaftaran Aplikasi ke Kominfo Diundur", *cnbcindonesia.com*, 24 Mei 2021, diakses dari https://bit.ly/3qEmo49.

		diatur atau diawasi oleh Kementerian atau Lembaga berdasarkan ketentuan peraturan perundang-undangan; dan/atau b. Penyelenggara Sistem Elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet yang dipergunakan untuk: i. menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau perdagangan barang dan/atau jasa; ii. […] layanan transaksi keuangan; iii. pengiriman materi atau muatan digital berbayar melalui jaringan data baik dengan cara unduh melalui portal atau situs, pengiriman lewat surat elektronik, atau melalui aplikasi lain ke perangkat Pengguna Sistem Elektronik; iv. […] layanan komunikasi meliputi namun tidak terbatas pada pesan singkat, panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial; v. layanan mesin pencari, layanan penyediaan Informasi Elektronik yang berbentuk tulisan, suara, gambar, animasi, musik, video, film, dan permainan atau kombinasi dari sebagian dan/ atau seluruhnya; dan/atau vi. pemrosesan Data Pribadi untuk kegiatan operasional melayani masyarakat yang terkait dengan aktivitas Transaksi Elektronik.		Kominfo. Permohonan pendaftaran tersebut diajukan kepada Menkominfo melalui *online single submission*.[203] Beberapa informasi terkait gambaran umum pengoperasian Sistem Elektronik ('SE') terdiri dari:[204] a. nama SE; b. sektor SE; c. URL website; d. Sistem nama domain dan/atau *IP address*; e. Deskripsi model bisnis; f. Deskripsi singkat fungsi SE dan proses bisnis; g. *Keterangan data pribadi yang diproses;* h. Keterangan lokasi pengelolaan, pemrosesan, dan atau penyimpanan SE dan data elektronik; i. Keterangan jaminan bahwa PSE-LP akan melaksanakan kewajiban pemberian akses dalam rangka pengawasan dan penegakan hukum.
2	2 (3)	Kewajiban melakukan pendaftaran bagi PSE Lingkup Privat dilakukan *sebelum Sistem Elektronik mulai digunakan* oleh Pengguna Sistem Elektronik	*Lawfulness*	Kewajiban registrasi pra-operasi. Proses pendaftaran diakhiri dengan pemberian tanda daftar PSE-LP yang diterbitkan oleh Menteri Kominfo.[205]
3	3 (1)	Kewajiban PSE Lingkup Privat		Dari rumusan pasal ini,

[203] Pasal 3 Permen Kominfo PSE-LP
[204] Lihat: Pasal 3 ayat (4) Permen Kominfo PSE-LP.
[205] Pasal 6 ayat (1) Permen Kominfo PSE-LP

		melakukan pendaftaran […] juga berlaku untuk PSE Lingkup Privat yang didirikan menurut hukum negara lain atau yang berdomisili tetap di negara lain tetapi: (a) memberikan layanan di dalam wilayah Indonesia; (b) melakukan usaha di Indonesia; dan/atau (c) Sistem Elektroniknya dipergunakan dan/atau ditawarkan di wilayah Indonesia.		diketahui hampir seluruh jenis PSE-LP wajib melakukan pendaftaran di Indonesia. Persoalannya, bagaimana dengan PSE-LP luar negeri yang hanya menyediakan produk untuk impor, semisal, situs-situs yang dikelola secara perseorangan, dan tidak memiliki populasi pengguna sebanyak perusahaan aplikasi pada umumnya? Ini patut dicermati sebab ada konsekuensi pembukaan akses dan tidak semua PSE-LP bersedia karena dilarang oleh hukum di negara asal.
4	7 (2)	Dalam hal PSE Lingkup Privat tidak melakukan pendaftaran sebagaimana dimaksud pada ayat (1) huruf a, Menteri memberikan sanksi administratif berupa Pemutusan Akses terhadap Sistem Elektronik (*access blocking*).		Kebijakan ini tidak punya efek regulatif sebab pemblokiran akses tetap dapat ditembus menggunakan VPN. Pendekatan denda lebih ideal.
5	9 (1) & (2)	PSE Lingkup Privat bertanggung jawab atas penyelenggaraan Sistem Elektronik dan pengelolaan Informasi Elektronik dan/atau Dokumen Elektronik di dalam Sistem Elektronik secara andal, aman, dan bertanggung jawab. PSE Lingkup Privat wajib menyediakan petunjuk penggunaan layanan dalam bahasa Indonesia […].	*Accountability; Lawfulness, Fairness, and Transparency*	
6	9 (3)	PSE Lingkup Privat wajib memastikan: a. Sistem Elektroniknya tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang; dan b. Sistem Elektroniknya tidak memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.	*Security; Integrity and Confidentiality*	Rumusan pasal ini membebani PSE-LP secara aktif memonitor dan memfilter konten-konten yang diunggah penggunanya. Beberapa pihak berkeberatan karena pendekatan ini membuat kebebasan dan privasi digital berkurang, di samping

				menciptakan model penyensoran pra-publikasi.[206]
7	13 (1) & (2)	PSE Lingkup Privat wajib melakukan Pemutusan Akses (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 9 ayat (4). Kewajiban melakukan Pemutusan Akses […] termasuk Pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dapat memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.	*Accountability*	Permohonan *take down* dapat diajukan oleh masyarakat, Kementerian atau Lembaga, Aparat Penegak Hukum; dan/atau lembaga peradilan.[207] Konten yang bersifat mendesak dalam hal: (a) terorisme; (b) pornografi anak; atau (c) konten yang meresahkan masyarakat dan mengganggu ketertiban umum Permohonan disampaikan melalui situs web, aplikasi, surat (e-mail atau surat non-elektronik).[208]
8	25 (1) & (2)	[Dalam konteks penegakan hukum] PSE Lingkup Privat harus menunjuk paling sedikit seorang Narahubung yang berdomisili di wilayah Indonesia yang bertugas untuk memfasilitasi permintaan akses terhadap Sistem Elektronik dan/atau Data Elektronik yang disampaikan oleh Kementerian atau Lembaga. Narahubung […] menerima permintaan akses terhadap Sistem Elektronik dan/atau Data Elektronik dari Narahubung yang telah ditetapkan oleh Kementerian atau Lembaga dan disampaikan kepada PSE Lingkup Privat	*Accountability*	Dalam GDPR narahubung yang dimkaksud adalah Petugas Perlindungan Data (DPO). Tidak dijelaskan apakah yang dimaksud pada PP ini adalah staf sejenis DPO.
9	15 (6)	PSE Lingkup Privat yang diperintahkan melakukan Pemutusan Akses *(take down)* […] wajib melakukan pemutusan […] terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang paling	*Accountability*	Jika tidak dilaksanakan, Menteri dapat melakukan Pemutusan Akses lewat penyedia layanan internet (ISP).

[206] Human Rights Watch, "Indonesia: Tangguhkan dan Revisi Permenkominfo No. 5 Tahun 2020", *hrw.org*, 21 Mei 2016, para. 5, diakses dari https://www.hrw.org/id/news/2021/05/21/378764

[207] Pasal 14 ayat (1) Permen Kominfo PSE-LP

[208] Pasal 14 ayat (2) PDP SE.

		lambat 1 x 24 jam setelah surat perintah […] diterima.		
10	15 (8)	Permohonan Pemutusan Akses *(take down)* terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang bersifat mendesak […]. PSE Lingkup Privat wajib melakukan Pemutusan Akses *(take down)* […] sesegera mungkin tanpa penundaan paling lambat 4 (empat) jam setelah peringatan diterima	*Accountability*	Kebijakan kontroversial mengingat penentuan indikasi konten terlarang atau tidaknya cenderung sepihak.
11	15 (10) & (11)	[Dalam konteks permohonan penghapusan konten oleh masyarakat] PSE Lingkup Privat *User Generated Content* yang tidak melaksanakan Pemutusan Akses (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang […] dikenakan sanksi administratif berupa denda yang besarannya sesuai dengan ketentuan peraturan perundang-undangan mengenai penerimaan negara bukan pajak.	*Accountability*	Sanksi sebagaimana dimaksud disampaikan melalui surat teguran yang diberikan kepada PSE Lingkup Privat untuk setiap 1 x 24 jam untuk ketentuan sebagaimana dimaksud pada ayat (6) dan 1 x 4 jam untuk ketentuan sebagaimana dimaksud pada ayat (8) dengan maksimal surat teguran yang diberikan sebanyak 3 (tiga) kali.

Jika ditelaah dari beberapa pasal di atas yang dimuat di atas, terjadi perubahan pendekatan yang digunakan Pemerintah, dari privasi menuju ke pendekatan berbasis ketertiban umum (proteksionisme). Praktis karena perubahan itu, standar yang digunakan dalam Permen Kominfo PSE-LP menjadi kontradiktif terhadap Permen PDPSE yang notabene telah mengadopsi rumusan GDPR dengan cukup baik. Hal yang patut menjadi catatan adalah Pengadilan HAM Eropa pada 25 Mei 2021 memutuskan bahwa upaya surveilans massa berikut intersepsi digital sebagaimana dipraktikkan oleh Pemerintah Inggris dan beberapa negara lainnya di Uni Eropa, merupakan pelanggaran berat atas hak privasi dan kebebasan berekspresi, sekalipun otoritas berlindung pada dalih *safeguards*.[209]

Peraturan Badan Sandi dan Siber Negara (BSSN) tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

Sebagai otoritas yang ditugasi melakukan pengamanan ruang siber, Peraturan BSSN Nomor 8 Tahun 2020 memperkenalkan mekanisme penilaian mandiri (*self-assessment*) oleh PSE, guna menilai keandalan keamanan perangkat sistem elektronik yang digunakan. Penilaian ditetapkan berdasarkan kategori risiko dampak rendah, tinggi, dan strategis.

[209] Privacy International, "UK Mass Interception Laws Violates Human Rights and Fight Continues…", *privacyinternational.org*, 26 Mei 2021, diakses dari https://bit.ly/3dioa5t.

Peraturan ini menarget pada PSE Lingkup Publik dan Lingkup Privat, termasuk yang penyedia situs, jaringan, portal atau aplikasi yang melakukan pemrosesan data pribadi.[210] Lebih jauh, peraturan ini juga memberi kewajiban kepada penyelenggara sistem elektronik dari ketiga kategori sebelumnya untuk menerapkan standar SNI ISO/IEC 27001[211], yang merupakan standar Sistem Manajemen Keamanan Informasi yang ditetapkan Badan Standardisasi Nasional.

Tabel 4.2.2.5 Kategori Sistem Elektronik dalam Peraturan BSSN Pengamanan Sistem Pengamanan PSE

Pasal (Ayat)	Klasifikasi	Kriteria
6 (1)	Strategis	Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara
6 (2)	Tinggi	Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.
6 (3)	Rendah	Yang tidak termasuk kriteria sedang dan strategis.

Peraturan ini juga secara spesifik menarget keamanan perlindungan data pribadi, namun bedanya dengan Permen PDPSE sebelumnya adalah peraturan ini lebih mengatur ihwal tentang keandalan perangkat, bukan pada proses pemrosesan data. Kriteria keandalan untuk mengetahui klasifikasi sistem elektroniknya diatur pada Lampiran II Nomor 1.6 hingga 1.9, yang dirumuskan lewat penilaian atas beberapa *benchmark* yang ditetapkan kemudian diberi bobot nilai, yakni:

> [1.6] Data pribadi yang dikelola Sistem Elektronik:
> a. Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya.
> b. Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha.
> c. Tidak ada data pribadi.
>
> [1,7] Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi:
> a. Sangat Rahasia.
> b. Rahasia dan/ atau Terbatas.
> c. Biasa.
>
> [1.8] Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi:
> a. Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik.
> b. Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung.
> c. Proses yang hanya berdampak pada bisnis perusahaan.
>
> [1,9] Dampak dari kegagalan Sistem Elektronik:
> a. Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan

[210] Pasal 5 ayat (2) Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik.
[211] *Ibid.*, Pasal 9.

keamanan negara.
b. Tidak tersedianya layanan publik dalam 1 propinsi atau lebih.
c. Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih.

Jika PSE memenuhi kriteria standar yang ditetapkan pada Peraturan BSSN ini, maka akan diterbitkan Sertifikat Manajemen Pengamanan Informasi (SMPI).[212]

4.3. Regulasi Penunjang

Regulasi penunjang bagi aktivitas ekonomi digital tersebar luas dalam pelbagai sektor, mulai dari perdagangan hingga kependudukan. Kemkominfo sendiri dalam Siaran Pers tanggal 17 Mei 2019 menyebut "…terdapat paling tidak 30 regulasi yang mengatur mengenai perlindungan data, dalam kaitannya dengan hak asasi manusia, pertahanan keamanan, kesehatan, administrasi kependudukan, keuangan dan perbankan, serta perdagangan dan perindustrian". [213] Maka, mengingat jumlah sektor yang sangat banyak itu, pemetaan regulasi pada kajian ini tidak akan secara spesifik menyebutkan satu per satu regulasi tersebut, namun hanya memaparkan beberapa peraturan sektoral yang tersedia. Beberapa sektor yang dapat disoroti antara lain namun tidak terbatas pada:

4.3.1. Sektor Bisnis

Pada sektor bisnis, setidaknya ditemukan tujuh peraturan perundang-undangan di tingkat UU hingga Peraturan Menteri yang menjadi regulasi penunjang pelindungan data pribadi.

Tabel 4.3.1.1 Pemetaan Regulasi Penunjang Sektor Bisnis

No	Regulasi	Konteks Pengaturan	Cakupan	Catatan
1	UU No. 7 Tahun 2014 tentang Perdagangan[214]	'Barang' adalah setiap benda, baik berwujud maupun tidak berwujud, baik bergerak maupun tidak bergerak, baik dapat dihabiskan maupun tidak dapat dihabiskan, dan dapat diperdagangkan, dipakai, digunakan, atau dimanfaatkan oleh konsumen atau Pelaku	1. Kegiatan perdagangan termasuk yang dilakukan lewat medium daring atau *e-commerce*.[215] 2. Perdagangan lintas batas negara melalui kerja sama perdagangan	Data masuk dalam definisi benda sehingga bisa jadi komoditas dagang karena memiliki nilai kemanfaatan dan dapat diperdagangkan (sepanjang disepakati oleh data subjek). Sementara, pemrosesan data termasuk ke dalam aktivitas jasa, termasuk di dalamnya

[212] Pasal 28 Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik.

[213] Kementerian Komunikasi dan Informasi, "Pernyataan BRTI Mengenai Praktik Jual Beli Data Pribadi", Siaran Pers, *kominfo.go.id*, (17 Mei 2019), diakses dari https://bit.ly/3xZOeKz.

Untuk kajian lebih lengkap tentang ke-tiga puluh UU dimaksud lihat: Wahyudi Djafar dkk, *Pelindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia,* Seri Internat dan HAM, (Jakarta: ELSAM, 2016).

[214] Indonesia, *Undang-Undang tentang Perdagangan*, UU No. 7 Tahun 2014, LN No. 45 Tahun 2014, TLN Nomor. 5512.

[215] *Ibid.,* Pasal 4 ayat (1) huruf e.

		Usaha.[216] 'Jasa' adalah setiap layanan dan unjuk kerja berbentuk pekerjaan atau hasil kerja yang dicapai, yang diperdagangkan oleh satu pihak ke pihak lain dalam masyarakat untuk dimanfaatkan oleh konsumen atau Pelaku Usaha.[217]	internasional.[218] 3. Penyedia layanan *e-commerce* wajib menyediakan data secara akurat dan benar.	pengolahan data untuk kebutuhan periklanan. Data tidak termasuk ke dalam kriteria barang ynag secara spesifik dilarang ekspor dalam Pasal 2 ayat (1) Permendag No. 44/2012 tentang Barang Dilarang Ekspor.
2	UU No. 30 Tahun 2000 tentang Rahasia Dagang	Rahasia Dagang' sebagai informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik rahasia dagang.	1. Rahasia dagang bisa dilisensikan.	Tidak adanya pembatasan terkait informasi seperti apa membuat teknik-teknik analisis atas data maupun *big data* dapat dilekati dengan proteksi rahasia dagang yang dilindungi kerahasiaannya dan memiliki nilai ekonomis.
3	UU No. 19 Tahun 2002 tentang Hak Cipta[219] (sebelum diganti UU No. 28 Tahun 2014)	'Database' adalah kompilasi data dalam bentuk apapun yang dapat dibaca oleh mesin (komputer) atau dalam bentuk lain, yang karena alasan pemilihan atau pengaturan atas isi data itu merupakan kreasi intelektual. Data pribadi yang tertuang ke dalam karya cipta, semisal, fotografi, dapat menjadi objek hak cipta.	1. Pembagian jenis hak dalam hak cipta, yakni, hak moral dan hak ekonomi. 2. Dalam wilayah HAKI, hak moral melekat pada subjek data pribadi, sementara hak ekonomi dapat menjadi properti kontroler.	Database dapat dilekatkan perlindungan hak cipta, namun ketentuan ini dihapuskan pada UU Hak Cipta yang baru. Data pribadi, seperti wajah seseorang, yang dituangkan dalam bentuk potret/foto, dapat dilekati hak cipta.
4	UU No. 8 Tahun 1999 tentang Perlindungan Konsumen[220]	'Konsumen' adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri	1. Kewajiban transparansi pelaku usaha untuk menjelaskan produk yang	Penyedia layanan daring untuk kepentingan profit (PSE-LP) tergolong sebagai pelaku usaha. Sementara, masyarakat

[216] *Ibid.*, Pasal 1 angka 5.
[217] *Ibid.*, Pasal 1 angka 6.
[218] *Ibid.,* Pasal 4 ayat (1) huruf i.
[219] Indonesia, *Undang-Undang tentang Hak Cipta*, UU No. 19 Tahun 2002, LN No. 85 Tahun 2002.
[220] Indonesia, *Undang-Undang tentang Perlindungan Konsumen*, UU No. 8 Tahun 1999, LN No. 22 Tahun 1999, TLN No. 3821.

		sendiri, keluarga, orang lain, maupun makhluk hidup lain dan tidak untuk diperdagangkan.[221] 'Pelaku usaha' adalah setiap orang perseorangan atau badan usaha, baik yang berbentuk badan hukum maupun bukan badan hukum yang didirikan dan berkedudukan atau melakukan kegiatan dalam wilayah hukum negara Republik Indonesia, baik sendiri maupun bersama-sama melalui perjanjian penyelenggaraan kegiatan usaha dalam berbagai bidang ekonomi.[222]	ditawarkan secara jelas. 2. Larangan bagi pelaku usaha untuk membuat klausula baku yang melepaskan tanggung jawab pelaku usaha. 3. Kewajiban pelaku usaha untuk bertanggungjawab atas risiko yang dialami konsumen. 4. Kewajiban pelaku usaha periklanan atas kerugian yang dialami akibat iklan yang dibuat.	pengguna aplikasi termasuk ke dalam definisi konsumen.
5	UU No. 8 Tahun 1997 tentang Dokumen Perusahaan[223]	'Dokumen perusahaan' adalah data, catatan dan atau keterangan yang dibuat dan atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya, baik tertulis di atas kertas atau sarana lain maupun terekam dalam bentuk corak apapun yang dapat dilihat, dibaca dan didengar	1. Mengatur perihal penyimpanan, pemindahan, dan pemusnahan dokumen perusahaan. 2. Dokumen perusahaan terdiri dari dokumen keuangan dan dokumen lainnya. 3. Dokumen lainnya terdiri dari setiap data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen keuangan.[224] 4. Kewajiban	Data yang diproses tercakup ke dalam kategori 'dokumen lainnya'. Pemindahan dokumen perusahaan dari unit pengolahan ke unit kearsipan di lingkungan perusahaan tersebut dilakukan berdasarkan keputusan pimpinan perusahaan yang pelaksanaannya disesuaikan dengan kebutuhan perusahaan yang bersangkutan.[225]

[221] *Ibid.,* Pasal 1 angka 2.
[222] *Ibid.*, Pasal 1 angka 3.
[223] Indonesia, *Undang-Undang tentang Dokumen Perusahaan*, UU No. 8 Tahun 1997, LN No. 18 Tahun 1997, TLN No. 3674.
[224] *Ibid.*, Pasal 4.
[225] *Ibid.*, Pasal 17.

			pemusnahan dokumen perusahaan.	
6	PP Nomor 5 Tahun 2020 tentang Sistem Informasi Perdagangan [226]	'Sistem Informasi Perdagangan' adalah tatanan, prosedur, dan mekanisme untuk pengumpulan, pengolahan, penyampaian, pengelolaan, dan penyebarluasan data dan/atau informasi perdagangan yang terintegrasi dalam mendukung kebijakan dan pengendalian perdagangan.[227] 'Data Perdagangan' adalah fakta yang ada yang berupa tekstual atau spasial baik terstruktur maupun tidak terstruktur terkait dengan kegiatan perdagangan yang dapat dijadikan dasar untuk menyusun Informasi Perdagangan.[228]	Data perdagangan bersifat terbuka, kecuali ditentukan lain oleh Menteri.[229] Pelaku Usaha dan/atau pelaku usaha yang berkedudukan di luar wilayah Negara Republik Indonesia [...] wajib memberikan Data Perdagangan dan atau Informasi Perdagangan kepada Menteri.[230]	Penegasan data teragregat di bidang perdagangan sebagai informasi yang terbuka bagi publik.
7	PP No. 80 Tahun 2019 tentang Transaksi Perdagangan Melalui Sistem Elektronik (PP TPMSE)[231]	Mewajibkan Pengelola Sistem Elektronik (PSE) untuk memberi notifikasi tertulis kepada pemilik data dalam hal terjadi kegagalan pelindungan data pribadi.[232]	Kegagalan yang dimaksud adalah terhentinya sebagian atau seluruh fungsi sistem elektronik yang bersifat esensial sehingga sistem elektronik tidak berfungsi sebagaimana mestinya.	Pertanggungjawaban PSE dalam bentuk tanggung gugat atas kerugian kegagalan sistem elektronik yang dialami konsumen.

[226] Indonesia, P*eraturan Pemerintah tentang Sistem Informasi Perdagangan*, PP No. 5 Tahun 2020, LN No. 9 Tahun 2020, TLN No. 6458.
[227] *Ibid.*, Pasal 1 angka 1.
[228] *Ibid.*, Pasal 1 angka (2).
[229] *Ibid.*, Pasal 4 ayat (2).
[230] *Ibid.*, Pasal 8 ayat (2).
[231] Indonesia, *Peraturan Pemerintah tentang Transaksi Perdagangan Melalui Sistem Elektroni*k, PP No. 80 Tahun 2019, LN No. 222 Tahun 2019, TLN No. 6420.
[232] *Ibid.*, Pasal 4 PP.

7	Peraturan Menteri Perdagangan Nomor 50 Tahun 2020 tentang Perizinan Usaha Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan Melalui Sistem Elektronik[233]	'Iklan Elektronik' adalah informasi untuk kepentingan komersial atas Barang dan/atau Jasa melalui Komunikasi Elektronik yang dimuat dan disebarluaskan kepada pihak tertentu baik yang dilakukan secara berbayar maupun yang tidak berbayar.[234] Dalam rangka pembinaan, data dan/atau informasi perusahaan dan kegiatan usaha Pelaku Usaha sebagaimana dimaksud dalam Pasal 36 disampaikan kepada Menteri melalui Direktur Jenderal PDN.[235] Jenis data dan/atau informasi perusahaan dan kegiatan usaha Pelaku Usaha dapat berupa data individual dan/atau granular.[236]	1. *E-commerce* asing wajib punya kantor perwakilan di Indonesia. Bertujuan untuk memberikan jaminan perlindungan konsumen Indonesia apabila ada *dispute* antara konsumen dengan *seller*. 2. Ada sanksi administratif bagi yang melanggar.	Dalam konteks periklanan, Iklan Elektronik tunduk pada ketentuan peraturan perundang-undangan di bidang penyiaran, perlindungan atas privasi dan data pribadi, perlindungan Konsumen, dan tidak bertentangan dengan prinsip persaingan usaha yang sehat.

4.3.2. Sektor Perbankan dan Jasa Keuangan

Sebagai salah satu industri yang paling marak menggunakan sistem elektronik dan melakukan pemrosesan data pribadi, sektor perbankan menjadi pencetak regulasi perihal pelindungan data pribadi terbanyak. Mengingat tidak mungkin seluruhnya ditabulasikan, maka Tabel 4.3.2.1 di bawah hanya mengelaborasikan empat produk perundang-undangan pada sektor tersebut yang menjadi rujukan utama norma pelindungan data pribadi di bidang perbankan. Diantaranya UU Perbankan, Peraturan OJK tentang Perlindungan Konsumen Sektor Jasa Keuangan, Peraturan BI tentang Perlindungan Konsumen BI, Peraturan BI tentang Sistem Pembayaran

Tabel 4.3.2.1 Pemetaan Regulasi Penunjang di Sektor Perbankan

No	Regulasi	Konteks Pengaturan	Cakupan	Catatan

[233] Indonesia, P*eraturan Menteri Perdagangan tentang Perizinan Usaha Periklanan, Pembinaan dan Pengawasan Pelaku Usaha dalam Perdagangan Melalui Sistem Elektronik*, Permendag No. 50 Tahun 2020, LN No. 498 Tahun 2020.
[234] *Ibid.*, Pasal 1 angka 21.
[235] *Ibid.*, Pasal 37 ayat (1).
[236] *Ibid.*, Pasal 37 a yat (2).

1	UU No. 10 Tahun 1998 tentang Perbankan[237]	'Rahasia Bank' adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.[238] Dalam rangka tukar menukar informasi antar bank, direksi bank dapat memberitahukan keadaan keuangan nasabahnya kepada bank lain.[239]	1. Bank dilarang memberikan keterangan yang tercatat pada bank tentang keadaan keuangan dan hal-hal lain dari nasabahnya, yang wajib dirahasiakan oleh bank menurut kelaziman dalam dunia perbankan.[240] 2. Pengecualian dilakukan dalam hal perpajakan, dan kepentingan penegakan hukum. 3. Sanksi bagi pelanggar rahasia bank sebesar Rp 2 Milyar rupiah.	Segala sesuatu yang berkaitan dengan simpanan nasabah bersifat rahasia. Tapi, dalam rezim hukum rahasia bank ada perbedaan antara data pribadi dan data simpanan nasabah. Definisi rahasia bank dalam UU No. 10 Tahun 1998 lebih umum jika dibandingkan UU sebelumnya.
2	Peraturan Otoritas Jasa Keuangan No. 1/POJK.7/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan[241]	Perlindungan konsumen [Jasa Keuangan] menerapkan prinsip kerahasiaan data atau informasi konsumen.[242]	1. Pelaku Usaha Jasa Keuangan wajib menginformasikan kepada Konsumen setiap perubahan manfaat, biaya, risiko, syarat, dan ketentuan yang tercantum dalam dokumen dan/atau perjanjian mengenai produk dan/atau layanan Pelaku Usaha Jasa Keuangan. 2. Dalam hal Konsumen tidak menyetujui perubahan terhadap	Perihal perlindungan data nasabah diatur lebih lanjut dalam Surat Edaran No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen. Pelaku Usaha Jasa Keuangan (PUJK), termasuk bank, wajib melindungi data dan atau informasi pribadi konsumen dan melarang dengan cara apapun untuk memberikan data dan atau informasi pribadi konsumen kepada pihak

[237] Indonesia, *Undang-Undang tentang Perubahan atas Undang-Undang Perbankan*, UU No. 10 Tahun 1998, LN No. 182 Tahun 1998, TLN No. 3790.

[238] *Ibid,* Pasal 1 angka 28.

[239] *Ibid.*, Pasal 44.

[240] *Ibid.*, Pasal 40.

[241] Indonesia, *Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen Sektor Jasa Keuangan*, POJK No. 1/POJK.7/2013, LN No. 118 Tahun 2013, TLN No. 5431.

[242] *Ibid.*, Pasal 2 huruf e. Dalam penjelasannya disebutkan: "Yang dimaksud dengan "kerahasiaan dan keamanan data/informasi Konsumen" dalam huruf ini adalah tindakan yang memberikan perlindungan, menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen, serta hanya menggunakannya sesuai dengan kepentingan dan tujuan yang disetujui oleh Konsumen, kecuali ditentukan lain oleh peraturan perundang undangan yang berlaku."

			persyaratan produk dan/atau layanan […] Konsumen berhak memutuskan produk dan/atau layanan tanpa dikenakan ganti rugi apapun.	ketiga. Data dan atau informasi konsumen yang wajib dirahasiakan dalam SE OJK tersebut termasuk data perseorangan, seperti nama, alama, tanggal lahir, umur, nomor telepon, dan/atau nama ibu kandung.
3	Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia[243]	Penyelenggara wajib menjaga kerahasiaan dan keamanan data dan/atau informasi konsumen.[244] Kewajiban menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen [...] sesuai dengan ketentuan peraturan perundang-undangan.[245] Dalam hal Penyelenggara bekerja sama dengan pihak lain untuk mengelola data dan/atau informasi konsumen, Penyelenggara wajib memastikan pihak lain tersebut menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen.	Guna menjaga kerahasiaan dan keamanan data dan/atau informasi konsumen, Penyelenggara wajib memiliki:[246] a. fungsi yang bertanggung jawab terhadap perlindungan data dan/atau informasi Konsumen; b. sistem informasi yang andal untuk mendukung pelaksanaan perlindungan data dan/atau informasi Konsumen; dan c. mekanisme dan prosedur mengenai perlindungan data dan/atau informasi Konsumen.	Selain menjamin kerahasian dan keamanan, Penyelenggara [Sistem Pembayaran] wajib menyediakan layanan khusus kepada Konsumen dengan kebutuhan khusus. Penyelenggara wajib mengelola dan menatausahakan data dan/atau informasi konsumen secara akurat, terkini, dan jelas.
4	Peraturan Bank Indonesia Nomor 22/23/2020	Dalam pemrosesan data dan/atau informasi terkait Sistem Pembayaran, Penyedia Jasa Pembayaran		Aturan ini mengadopsi prinsip-prinsip umum perlindungan privasi dalam pemrosesan data.

[243] *Ibid.*
[244] Indonesia, *Peraturan Bank Indonesia tentang Pelindungan Konsumen Bank Indonesia*, PBI Nomor 22/20/PBI/2020, LN No. 299 Tahun 2020, TLN No. 6605, Pasal 30 (1).
[245] *Ibid.*, Pasal 30 ayat (2)
[246] *Ibid.*, Pasal 30 ayat (3).

	tentang Sistem Pembayaran[247]	(PJP), Penyedia Infrastruktur Pembayaran (PIP), dan/atau pihak yang bekerja sama dengan PJP dan PIP wajib:[248] a. menerapkan prinsip perlindungan data pribadi termasuk memenuhi aspek persetujuan Pengguna Jasa atas penggunaan data pribadinya; b. memenuhi mekanisme pemrosesan data dan/atau informasi terkait Sistem Pembayaran yang ditetapkan oleh Bank Indonesia, termasuk mekanisme pemrosesan melalui infrastruktur data dan infrastruktur Sistem Pembayaran Bank Indonesia; c. memenuhi mekanisme pemanfaatan infrastruktur data pihak ketiga yang ditetapkan oleh Bank Indonesia; d. menerapkan manajemen risiko siber dalam penyelenggaraan Sistem Pembayaran, termasuk standar keamanan sistem informasi; dan e. memenuhi ketentuan peraturan perundang-undangan.		

4.3.3. Sektor Pelayanan Publik

Pengaturan perihal perlindungan data pribadi di sektor pelayanan publik tersebar di beberapa undang-undang sektoral. Tujuh diantaranya termuat namun tidak terbatas dalam Tabel 4.3.3.1 di bawah.

[247] Indonesia, *Peraturan Bank Indonesia tentang Sistem Pembayaran*, PBI No. 22/23/2020, LN No. 311 Tahun 2020, TLN No. 6610.

[248] *Ibid*., Pasal 107.

Tabel 4.3.3.1 Regulasi Penunjang Sektor Pelayanan Publik

No	Regulasi	Konteks Pengaturan	Cakupan	Catatan
1	UU No. 9 Tahun 2017 tentang Penetapan Perppu No. 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan[249]	Akses informasi keuangan untuk kepentingan perpajakan meliputi akses untuk *menerima dan memperoleh informasi keuangan* dalam rangka pelaksanaan ketentuan peraturan perundang-undangan.[250] Ketentuan rahasia bank dalam Pasal 41 UU Perbankan tidak berlaku sepanjang untuk kepentingan perpajakan.[251]	Direktur Jenderal Pajak berwenang mendapatkan akses informasi keuangan untuk kepentingan perpajakan dari lembaga jasa keuangan yang melaksanakan kegiatan di sektor perbankan, pasar modal, perasuransian, lembaga jasa keuangan lainnya, dan/atau entitas lain yang dikategorikan sebagai lembaga keuangan *sesuai standar pertukaran informasi keuangan* berdasarkan *perjanjian internasional* di bidang perpajakan.[252]	Pengecualian rahasia bank juga berlaku dalam rangka tukar menukar informasi antar bank. Direksi bank dapat memberitahukan keadaan keuangan nasabahnya kepada bank lain.
2	UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik[253]	'Informasi' adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi	Prinsipnya, setiap orang berhak untuk memperoleh informasi publik. Namun, Informasi Publik yang tidak dapat diberikan oleh Badan Publik […] antara lain: (c) informasi yang berkaitan dengan hak-hak pribadi.[254]	Informasi Publik yang apabila dibuka dan diberikan dapat membuka rahasia pribadi merupakan informasi yang dikecualikan. Beberapa diantaranya adalah:[255] 1. Riwayat dan kondisi anggota keluarga; 2. riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis

[249] Indonesia, *Undang-Undang tentang Penetapan Peraturan Pemerintah Nomor 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan*, UU No. 9 Tahun 2017, LN No. 190 Tahun 2017, TLN No. 6112.

[250] *Ibid.*, jo. Pasal 1 Perppu No. 1 Tahun 2017.

[251] *Ibid.*, jo. Pasal 8 angka 2 Perppu No. 1 Tahun 2017.

[252] *Ibid.*, jo. Pasal 2 ayat (1) Perppu No. 1 Tahun 2017.

[253] Indonesia, *Undang-Undang tentang Keterbukaan Informasi Publik*, UU No. 14 Tahun 2008, LN No. 61 Tahun 2008, TLN No. 4846.

[254] *Ibid.*, Pasal 6 ayat 3.

[255] Ibid., Pasal 17 huruf h.

		secara elektronik maupun nonelektronik.[256] 'Informasi Publik' adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik.[257]		seseorang 3. kondisi keuangan, aset, pendapatan, dan rekening bank seseorang; 4. hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang; dan/atau 5. catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.
3	UU No. 24 Tahun 2013 tentang Administrasi Kependudukan [258]	'Data Pribadi' adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.[259] 'Data Kependudukan' adalah data perseorangan dan/atau data agregat yang terstruktur sebagai hasil dari kegiatan Pendaftaran Penduduk dan Pencatatan Sipil.[260] Data agregat meliputi himpunan data perseorangan yang berupa data kuantitatif dan data kualitatif.[261]	Data Kependudukan terdiri atas data perseorangan dan/atau data agregat Penduduk.[262] Data perseorangan diatur dalam Pasal 58 ayat (2) huruf a hingga ee, diantaranya termasuk tanda tangan, sidik jari, iris mata, cacat fisik/mental, dst. Setiap orang yang tanpa hak menyebarluaskan Data Kependudukan […] dan Data Pribadi […] dipidana dengan pidana penjara paling lama 2 tahun	Mengatur perihal data agregat yang merupakan pengolahan lebih lanjut dari data kependudukan. Berbeda dengan data pribadi yang melekat hak privasi individu, data agregat menjadi hak publik. Besaran denda yang diatur relatif sangat kecil, dan tidak sebanding dengan nilai ekonomi dari aktivitas jual beli data.

[256] *Ibid*., Pasal 1 angka 1.
[257] *Ibid.*, Pasal 1 angka 2.
[258] Indonesia, *Undang-Undang tentang Perubahan atas UU Administrasi Kependudukan*, UU No. 24 Tahun 2013, LN No. 232 Tahun 2013, TLN No. 5475.
[259] *Ibid.*, Pasal 1 angka 22.
[260] *Ibid.*, Pasal 1 angka 9.
[261] *Ibid*, Pasal 58 ayat 3.
[262] *Ibid.*, Pasal 58 ayat 1.

			dan/atau denda paling banyak Rp25.000.000,00 (dua puluh lima juta rupiah).[263]	
4	UU No. 43 Tahun 2009 tentang Kearsipan[264]	'Arsip' adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, Lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara.[265]	Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila arsip dibuka untuk umum dapat mengungkapan rahasia atau data pribadi.[266]	Mengatur perihal pelaksanaan kearsipan yang dilakukan organisasi non-pemerintah.
5	UU No. 36 Tahun 1999 tentang Telekomunikasi[267]	'Telekomunikasi' adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik Iainnya.[268]	Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.[269]	Data sebagai salah satu medium hasil olahan kegiatan komunikasi.
6	Peraturan Pemerintah No. 31 Tahun 2012 tentang	'Data dan Informasi' adalah kumpulan angka, huruf, kata, dan/atau citra, yang bentuknya dapat	Instansi pemerintah, lembaga, asosiasi, dan pihak lain wajib memberikan Data	Jenis Data dan Informasi sebagaimana dimaksud, berupa: a. Data dan Informasi

[263] *Ibid*., Pasal 95A.
[264] Indonesia, *Undang-Undang tentang Kearsipan*, UU No. 43 Tahun 2009, LN No. 152 Tahun 2009, TLN No. 5071.
[265] *Ibid.,* Pasal 1 angka 2.
[266] *Ibid.,* Pasal 44 ayat 1 huruf h.
[267] Indonesia, *Undang-Undang tentang Telekomunikasi*, UU No. 36 Tahun 1999, LN No. 154 Tahun 1999, TLN No. 3881.
[268] *Ibid.,* Pasal 1 angka 1.
[269] *Ibid.,* Pasal 42 ayat (1).

	Pemberian dan Penghimpunan Data dan Informasi yang Berkaitan dengan Perpajakan[270]	berupa surat, dokumen, buku, atau catatan serta keterangan tertulis, yang dapat memberikan petunjuk mengenai penghasilan dan/atau kekayaan/harta orang pribadi atau badan, termasuk kegiatan usaha atau pekerjaan bebas orang pribadi atau badan.[271]	dan Informasi yang berkaitan dengan perpajakan.[272] Data dan informasi sebagaimana dimaksud [...] disampaikan kepada Direktorat Jenderal Pajak.	yang berkaitan dengan kekayaan atau harta yang dimiliki orang pribadi atau badan; b. Data dan Informasi yang berkaitan dengan utang yang dimiliki orang pribadi atau badan; c. Data dan Informasi yang berkaitan dengan penghasilan yang diperoleh atau diterima orang pribadi atau badan; d. Data dan Informasi yang berkaitan dengan biaya yang dikeluarkan dan/atau yang menjadi beban orang pribadi atau badan; e. Data dan Informasi yang berkaitan dengan transaksi keuangan; dan f. Data dan Informasi yang berkaitan dengan kegiatan ekonomi orang pribadi atau badan.
7	Peraturan Menteri Komunikasi dan Informatika No. 11 Tahun 2019 tentang Pengendalian Alat dan/atau Perangkat yang Tersambung	Setiap Penyelenggara wajib mengidentifikasi IMEI[273] Alat dan/atau Perangkat Telekomunikasi yang tersambung ke jaringannya.[274] Identifikasi sebagaimana dimaksud pada ayat (1) dilakukan dengan mengumpulkan paling sedikit data IMEI dan data	Direktur Jenderal dapat mengakses data dan informasi yang dikelola oleh Sistem Pengelolaan IMEI Nasional.[275]	IMEI merupakan bagian dari data pribadi karena memiliki sifat identifikasi.

[270] Indonesia, *Peraturan Pemerintah tentang Pemberian dan Penghimpunan Data dan Informasi yang Berkaitan dengan Perpajakan*, PP No. 31 Tahun 2012, LN No. 56 Tahun 2012, TLN No. 5289.

[271] *Ibid.,* Pasal 1 ayat (2).

[272] *Ibid.,* Pasal 2 ayat (1).

[273] *International Mobile Equipment Identity* (IMEI) adalah nomor identitas internasional yang terdiri dari 15 digit, dihasilkan dari 8 digit *Type Allocation Code* yang dialokasikan oleh *Global System for Mobile Association* untuk mengidentifikasi secara unik Alat dan/atau Perangkat Telekomunikasi yang tersambung ke jaringan bergerak seluler.

[274] *Ibid.*, Pasal 3 ayat (1).

[275] *Ibid.*, Pasal 15.

	ke Jaringan Bergerak Seluler Melalui Identifikasi IMEI[276]	*Subscriber Identity*.[277]		

4.3.4. Sektor Kesehatan

Beberapa regulasi perihal data pribadi di sektor kesehatan termuat dalam tabel 4.3.4.1 di bawah. Ada lima peraturan perundang-undangan yang diulas dengan substansi beririsan dengan konteks pelindungan informasi, antara lain:

Tabel 4.3.4.1 Regulasi Data Pribadi di Sektor Kesehatan

No	Regulasi	Konteks Pengaturan	Cakupan	Catatan
1	UU No. 36 Tahun 2009 tentang Kesehatan[278]	Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.[279] Kebocoran data kesehatan termasuk ke dalam kerugian yang disebabkan pelayanan kesehatan yang bisa dituntut ganti kerugian.[280]	Ketentuan mengenai hak atas rahasia kondisi kesehatan pribadi [...] tidak berlaku dalam hal:[281] a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut.	Rahasia kondisi kesehatan, atau biasa dikenal dengan istilah rekam medis, tercakup ke dalam data pribadi dalam UU Administrasi Kependudukan. Pembukaan data kependudukan diwajibkan melalui proses otorisasi berdasar persetujuan pasien yang bersangkutan.
2	UU No. 29 Tahun 2004 tentang Praktik Kedokteran[282]	Mengatur perihal 'Rekam Medis' dan 'Rahasia Kedokteran' namun tidak ada definisinya dalam ketentuan umum. Setiap dokter atau dokter gigi dalam menjalankan praktik kedokteran wajib membuat rekam medis [yang] harus segera	Rahasia kedokteran dapat dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan perundang-undangan.[283]	Mengatur status kepemilikan atas data pribadi berupa rekam medis. Dokumen rekam medis merupakan milik dokter, dokter gigi, atau sarana pelayanan kesehatan, sedangkan isi rekam medis

[276] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Pengendalian Alat dan/atau Perangkat yang Tersambung ke Jaringan Bergerak Seluler Melalui Identifikasi IMEI*, Permenkominfo No. 11 Tahun 2019, Berita Negara Nomor 1238 Nomor 2019.

[277] *Ibid.*, Pasal 3 ayat (2).

[278] Indonesia, *Undang-Undang tentang Kesehatan*, UU No. 36 Tahun 2009, LN Nomor 114 Tahun 2019, TLN Nomor 5063.

[279] *Ibid.*, Pasal 57 ayat (1).

[280] *Ibid.*, Pasal 57 ayat (2).

[281] *Ibid.,* Pasal 58 ayat (1) jo. Penjelasan Pasal 58 ayat (1).

[282] Indonesia, *Undang-Undang tentang Praktik Kedokteran*, UU No. 29 Tahun 2004, LN Nomor 116 Tahun 2004, TLN Nomor 4431.

[283] *Ibid.*, Pasal 48 ayat (2)

		dilengkapi setelah pasien selesai menerima pelayanan kesehatan.[284] Setiap dokter atau dokter gigi dalam melaksanakan praktik kedokteran wajib menyimpan rahasia kedokteran.[285]		merupakan milik pasien.[286]
3	UU No. 36 Tahun 2014 tentang Keperawatan[287]	Setiap Tenaga Kesehatan yang melaksanakan pelayanan kesehatan perseorangan wajib membuat rekam medis Penerima Pelayanan Kesehatan.[288] Rekam medis Penerima Pelayanan Kesehatan harus segera dilengkapi setelah Penerima Pelayanan Kesehatan selesai menerima pelayanan kesehatan.[289]	Setiap rekam medis Penerima Pelayanan Kesehatan harus dibubuhi nama, waktu, dan tanda tangan atau paraf Tenaga Kesehatan yang memberikan pelayanan atau tindakan. Rekam medis Penerima Pelayanan Kesehatan harus disimpan dan dijaga kerahasiaannya oleh Tenaga Kesehatan dan pimpinan Fasilitas Pelayanan Kesehatan.	Mengatur rekam medis yang dilakukan oleh tenaga perawat/tenaga kesehatan non-dokter.
4	UU Nomor 44 Tahun 2009 tentang Rumah Sakit[290]	Setiap pasien mempunyai hak: (i) mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya.[291] Setiap rumah sakit mempunyai kewajiban menyelenggarakan rekam medis.[292]	Pasien dapat "menggugat dan/atau menuntut Rumah Sakit apabila Rumah Sakit diduga memberikan pelayanan yang tidak sesuai dengan standar baik secara perdata ataupun pidana".	Konteks gugatan perihal pelayanan yang dimaksud melingkupi juga terkait kegagalan pelindungan atas kerahasiaan penyakit.
5	Peraturan Menteri Kesehatan Nomor 269 Tahun 2008 tentang Rekam Medis[293]	'Rekam medis' adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan	Rekam medis harus dibuat secara tertulis, lengkap dan jelas atau secara elektronik.[294] Isi rekam medis untuk pasien rawat jalan pada	Memberi definisi rekam medis yang tidak terakomodasi oleh UU Praktik Kedokteran Membagi macam-

[284] *Ibid.*, Pasal 46 ayat (1) dan (2).
[285] *Ibid.*, Pasal 48 ayat (1).
[286] *Ibid.*, Pasal 47.
[287] Indonesia, *Undang-Undang tentang Keperawatan*, UU No. 36 Tahun 2014, LN Nomor 298 Tahun 2014, TLN Nomor 5607.
[288] *Ibid.,* Pasal 70 ayat (1).
[289] *Ibid.,* Pasal 70 ayat (2).
[290] Indonesia, *Undang-Undang tentang Rumah Sakit,* UU No. 44 Tahun 2009, LN Nomor 153 Tahun 2009, TLN Nomor 5072.
[291] *Ibid.*, Pasal 32 huruf i.
[292] *Ibid.*, Pasal 29 huruf h.
[293] Indonesia, *Peraturan Menteri Kesehatan tentang Rekam Medis*, Permenkes No. 269/Menkes/Per/III/2008.
[294] *Ibid.*, Pasal 2 ayat (1).

		kepada pasien.[295]	sarana pelayanan kesehatan sekurang-kurangnya memuat: (a) identitas pasien; (b) tanggal dan waktu; (c) hasil anamnesis, mencakup keluhan dan riwayat penyakit; (d) hasil pemeriksaan fisik dan penunjang medik; (e) diagnosis; …(j) persetujuan tindakan bila diperlukan.[296]	macam rekam medis berdasarkan tipe pasien, yakni rawat jalan, rawat inap, dan pasien gawat darurat.

4.4. Regulasi dalam Proses

Setelah mengetahui regulasi inti dan regulasi penunjang perlindungan data pribadi di Indonesia, kita perlu meninjau arah kebijakan pemerintah dengan menelaah produk regulasi yang sedang dalam proses. Salah satu yang paling banyak diharapkan segera rampung adalah RUU Perlindungan Data Pribadi.

Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP)

Berbeda dengan regulasi yang telah diulas sebelumnya, pada draf RUU PDP (versi Januari 2020),[297] perancang undang-undang mulai mengadopsi istilah-istilah yang relevan dengan kegiatan pemrosesan data, seperti 'prosesor', 'pengendali data pribadi' atau umum dikenal dengan *data controller,* dan seterusnya. Substansi undang-undang ini dimaksudkan untuk berlaku kepada setiap orang, badan publik, dan organisasi/institusi yang melakukan perbuatan hukum pemrosesan data pribadi, baik di dalam wilayah maupun di luar wilayah Republik Indonesia, yang memiliki akibat hukum bagi pemilik data pribadi WNI.[298] Sementara, hak privasi individu mulai diangkat sebagai isu yang diseriusi, setidaknya terlihat dalam beberapa poin pada tinjauan teoritis yang diadopsi dalam naskah akademik RUU ini.[299]

Dalam draf terakhir, ada beberapa bagian pembahasan yang diatur, di antaranya: Jenis Data Pribadi (Bab II), Hak Pemilik Data Pribadi (Bab III), Pemrosesan Data Pribadi (Bab IV), Kewajiban Pengendali Data Pribadi (Bab V), Transfer Data Pribadi (Bab VI), Sanksi Administratif (Bab VII), Larangan Penggunaan Data Pribadi (Bab VIII), Pembentukan Pedoman Perilaku Pengendali Data Pribadi (Bab IX), Kerja Sama Internasional (Bab XI), Ketentuan Pidana (Bab XIII) dan seterusnya (lihat Gambar 4.4.1).

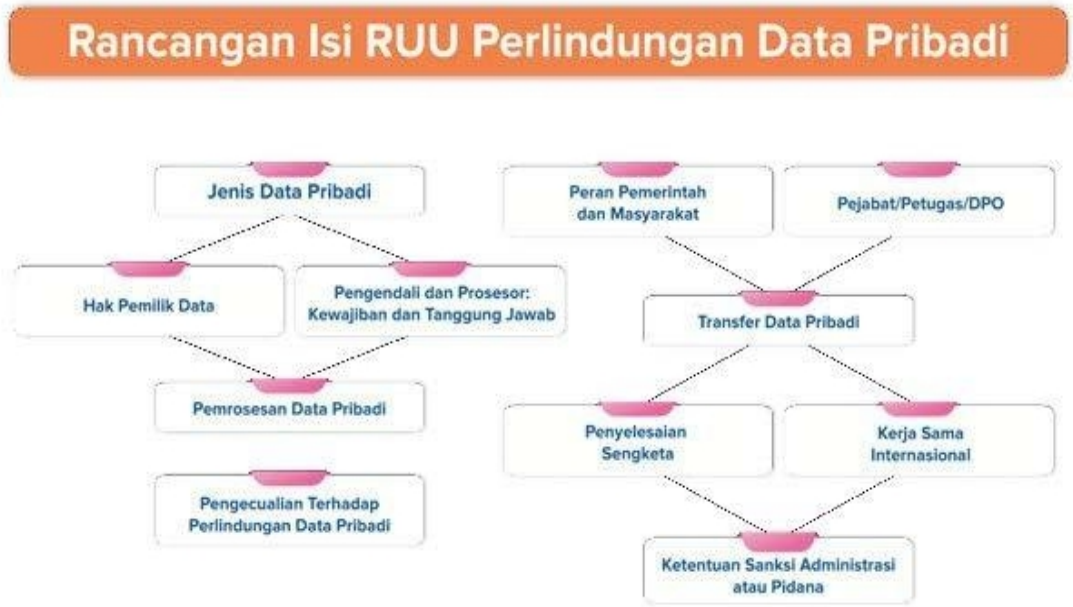
Selanjutnya, Pasal 3 draf RUU PDP mengkategorisasikan data pribadi menjadi dua jenis, yaitu (1) data yang bersifat umum dan (2) bersifat spesifik. Pengklasifikasian ini tergolong lebih komprehensif dibanding Permen Kominfo PDPSE, dan dapat dikatakan

---

[295] *Ibid.*, Pasal 1 angka 1.
[296] *Ibid.*, Pasal 3 ayat (1).
[297] Hukum Online, 'RUU Perlindungan Data Pribadi Tahun 2020', *hukumonline.com*, (n.d.). Tautan: https://bit.ly/3qtAViJ.
[298] Pasal 2 RUU PDP versi 2020 (untuk selanjutnya disebut 'RUU PDP').
[299] Lihat: Naskah Akademik (NA) RUU Perlindungan Data Pribadi, hlm. 16-17.

sudah sejalan dengan pendekatan dalam GDPR.[300] Data pribadi yang bersifat umum terdiri, diantaranya, dari nama lengkap, jenis kelamin, kewarganegaraan, agama dan data-data lainnya yang dikombinasikan untuk mengidentifikasi seseorang.[301] Sedang data pribadi yang bersifat spesifik mencakup data dan informasi kesehatan, pandangan politik, catatan kejahatan, data keuangan pribadi, data anak, data biometrik dan genetika, dan seterusnya.[302]

Gambar 4.4.1 Rancangan Muatan Substansi RUU PDP



(Sumber: Pratiwi Agustini, 'Rancangan Undang-Undang Perlindungan Data Pribadi, 17 September 2019, diakses dari https://aptika.kominfo.go.id/2019/09/rancangan-undang-undang-perlindungan-data-pribadi/)

Sama halnya seperti Permen Kominfo PDPSE, RUU PDP juga mengadopsi tahapan pemrosesan data sesuai siklus hidup informasi (C.U.D.S) yang terbagi menjadi:[303]

a. Tahap perolehan dan pengumpulan (*collection*)
b. Pengolahan dan penganalisisan (*usage*)
c. Penyimpanan (*storage*)
d. Penampilan, pengumpulan, transfer, penyebarluasan atau pengungkapan (*disclosure*)
e. Penghapusan atau pemusnahan (*disposal*).

Terhadap pemrosesan data pribadi tersebut, RUU PDP menawarkan prinsip perlindungan data pribadi umum, yakni:[304]

---

[300] Naskah akademik RUU PDP masih menggunakan istilah data sensitif. Hal ini karena NA tersebut mengadopsi skema dalam Derivatif Perlindungan Data Pribadi Uni Eropa yang merupakan instrumen sebelum GDPR. Lihat: NA RUU PDP, hlm. 22-23.
[301] Pasal 3 ayat 1 RUU PDP.
[302] Pasal 3 ayat 2 RUU PDP.
[303] Pasal 17 ayat (1) RUU PDP.
[304] Pasal 17 ayat (2) RUU PDP.

a. Pengumpulan data pribadi dilakukan secara terbatas dan spesifik (*data minimisation*); sah secara hukum, patut, dan transparan (*lawfulness, fair, and transparency*);
b. pemrosesan data pribadi dilakukan sesuai dengan tujuannya (*purpose limitation*);
c. pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi; (*confidentiality and security*);
d. pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, (*accuracy*) mutakhir, dan dapat dipertanggungjawabkan; (*accountability and liability*);
e. pemrosesan dilakukan dengan melindungi keamanan dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan data pribadi; (*confidentiality and security*);
f. pemrosesan dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan (*purpose limitation*), serta kegagalan pelindungan Data Pribadi (*accountability and liability*);
g. Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan pemilik data pribadi kecuali ditentukan lain oleh peraturan perundang-undangan; (*storage limitation*);
h. pemrosesan Data Pribadi dilakukan secara bertanggung jawab dengan memenuhi pelaksanaan prinsip pelindungan Data Pribadi dan dapat dibuktikan secara jelas; (*accountability and liability*).

Lebih jauh, beberapa pengaturan penting dalam RUU PDP yang bisa dielaborasikan antara lain:

4.4.1.1. Hak Pemilik Data Pribadi (Data Subjek)

Penggunaan istilah 'pemilik data' dalam RUU PDP menyiratkan bahwa terdapat relasi ekonomi yang inheren pada sebuah data dan subyek data. Terkait hal ini, beberapa pihak mengusulkan penggunaan istilah pemilik data diganti dengan 'subjek data' untuk menguatkan filosofi pelindungan. Terlepas dari perdebatan sebelumnya, RUU PDP mengatur beberapa hak pemilik data pribadi, antara lain:

a. Hak atas kejelasan identitas [pihak pengumpul data] dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data pribadi.[305] Redaksi norma ini sejalan dengan prinsip *lawfulness* and *fairness* yang diadopsi dari GDPR. Meski demikian, aspek transparansi belum terlihat pada rumusan ini padahal prinsip ini berada dalam satu tubuh prinsip yang sama.
b. Hak untuk melengkapi data pribadi miliknya sebelum diproses oleh kontroler atau pengendali data pribadi.[306] Aturan ini sejalan dengan prinsip *accuracy,* namun bedanya, dalam GDPR prinsip akurasi lebih dikhususkan pada ranah pemrosesan data (*usage*), sedang dalam RUU PDP prinsip akurasi diletakan pada siklus sebelum pemrosesan, yang artinya, pada ranah pengumpulan (*collection)*. Selain itu, frasa

[305] Pasal 4 RUU PDP
[306] Pasal 5 RUU PDP

'melengkapi' data pribadi yang dimaksud perlu diperjelas lagi karena pada dasarnya pengumpulan data sebisa mungkin minim (*data minimization*) sedang dalam penjelasan RUU PDP hanya dikatakan 'cukup jelas'.

c. Hak untuk mengakses data pribadi miliknya,[307] berdasarkan permintaan tertulis kepada *data controller*. Agar subjek data pribadi dapat memperbarui datanya secara akurat, harus ada jaminan bahwa pemilik data akan selalu dapat mengakses data pribadi miliknya. Pengaturan hak ini masih berada dalam satu tubuh prinsip *accuracy and up-to-date processing* dalam GDPR.
d. Hak pemilik data pribadi untuk mengakhiri pemrosesan, menghapus dan memusnahkan data pribadi miliknya,[308] berdasarkan permintaan tertulis; serta hak untuk menarik kembali persetujuan pemrosesan data yang telah diberikan kepada *data controller*.[309]
e. Hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang,[310] berdasarkan permintaan tertulis. Lalu, hak untuk memilih atau tidak memilih pemrosesan data pribadi melalui mekanisme pseudonym untuk tujuan tertentu.[311]
f. Hak untuk menunda atau membatasi pemrosesan data pribadi secara proporsional sesuai dengan tujuan pemrosesan data,[312] serta hak untuk menuntut dan menerima ganti rugi atas pelanggaran data pribadi.[313]
g. Hak untuk mendapatkan atau menggunakan data pribadi miliknya dari *data controller*, dengan struktur/format yang lazim terbaca oleh sistem elektronik atau perangkat keras,[314] serta hak untuk mengalihkan atau mengirimkan data pribadi miliknya ke pengendali data lainnya sepanjang sistem tersebut bisa saling berkomunikasi dengan aman.[315]

Tabel 4.4.1.1 Perbandingan Hak Subjek Pemilik Data Pribadi dalam RUU PDP dan GDPR

No	Redaksi Pasal dalam RUU PDP	Redaksi Artikel dalam GDPR
1	[Pasal 4] Pemilik Data Pribadi berhak meminta Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi. Catatan: Redaksi pasal ini belum mengatur keharusan pencantuman tujuan permintaan dan	*[Art. 13: Information to be provided when data are collected]* *Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:* *1. the identity and the contact details of the controller and, where applicable, of the controller's representative;*

[307] Pasal 6 RUU PDP
[308] Pasal 8 RUU PDP
[309] Pasal 9 RUU PDP
[310] Pasal 10 RUU PDP
[311] Pasal 11 RUU PDP
[312] Pasal 12 RUU PDP
[313] Pasal 13 RUU PDP
[314] Pasal 14 RUU PDP
[315] Pasal 15 RUU PDP

	penggunaan data pribadi oleh pihak ketiga yang terafiliasi oleh kontroler.	2. *the contact details of the data protection officer, where applicable;* 3. *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;* 4. *[…] the legitimate interests pursued by the controller or by a third party;* 5. *the recipients or categories of recipients of the personal data, if any;* 6. *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers […] reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*
2	[Pasal 5] Pemilik Data Pribadi berhak melengkapi Data Pribadi miliknya sebelum diproses oleh Pengendali Data Pribadi. [Pasal 7] Pemilik Data Pribadi berhak memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi miliknya sesuai dengan ketentuan perundang-undangan.	*[Art. 16: Right to rectification]* *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*
3	[Pasal 6] Pemilik Data Pribadi berhak mengakses Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan. [Pasal 10] Pemilik Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*). [Pasal 11] Pemilik Data Pribadi berhak untuk memilih atau tidak memilih pemrosesan Data Pribadi melalui mekanisme pseudonim untuk tujuan tertentu. [Pasal 12] Pemilik Data Pribadi berhak menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi.	*[Art. 15: Right of Access by the data subject]* *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:* *the purposes of the processing;* 1. *the categories of personal data concerned;* 2. *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;* 3. *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;* 4. *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*

	Catatan: Pengaturan untuk mengetahui masa retensi tidak masuk sebagai hak pemilik data pribadi dalam RUU PDP, namun dirumuskan sebagai kewajiban *data controller*.	5. *the right to lodge a complaint with a supervisory authority;* 6. *where the personal data are not collected from the data subject, any available information as to their source;* 7. *the existence of automated decision-making, including profiling […], meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.* *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards [….] relating to the transfer.* 1. *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.* 2. *Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.* 3. *The right to obtain a copy […] shall not adversely affect the rights and freedoms of others.*
4	[Pasal 10] Pemilik Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*). *Catatan: Dalam hal keberatan diajukan, mekanisme GDPR mengharuskan kontroler untuk tidak lagi memproses data tersebut, kecuali dengan dasar kepentingan yang sah.* [Pasal 14] (1) Pemilik Data Pribadi berhak mendapatkan dan/atau menggunakan Data Pribadi miliknya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik atau perangkat keras yang digunakan dalam interoperabilitas antar sistem elektronik.	*[Art. 20: Right to protability]* *[1] The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where […] (2) the processing is carried out by automated means.* *[2] In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.* *[Art. 21: Right to object]* *The data subject shall have the right to object, on grounds relating to his or her particular*

	(2) Pemilik Data Pribadi berhak menggunakan dan mengirimkan Data Pribadi miliknya ke Pengendali Data Pribadi lainnya, sepanjang sistem tersebut dapat saling berkomunikasi secara aman sesuai dengan prinsip pelindungan Data Pribadi berdasarkan Undang-Undang ini.	*situation, at any time to processing of personal data concerning him or her [...] including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*

4.4.1.2. Kewajiban Pengendali Data (Kontroler Data)

Beberapa kewajiban yang dibebankan kepada *data controller* dalam konteks pemrosesan data pribadi dalam RUU PDP antara lain:

a. Dalam hal pengumpulan data, *data controller* wajib berbasis persetujuan yang sah dari pemilik data pribadi, dengan menjelaskan satu atau beberapa tujuan dilakukannya pemrosesan data yang telah disampaikan kepada pemilik data pribadi sebelumnya.[316] Persetujuan sebagaimana dimaksud harus dibuat secara tertulis atau lisan terekam, baik secara elektronik maupun nonelektronik, menggunakan bahasa yang sederhana dan jelas.[317] Persetujuan ini paling sedikit mencantumkan informasi berupa:[318]
   - Legalitas pemrosesan data pribadi;
   - Tujuan pemrosesan data pribadi;
   - Jenis dan relevansi data pribadi yang akan diproses
   - Periode retensi;
   - Rincian mengenai informasi yang dikumpulkan
   - Jangka waktu pemrosesan;
   - Hak pemilik data pribadi

   Di samping itu, klausul perjanjian yang tidak memuat persetujuan eksplisit dari subjek data pribadi dinyatakan batal demi hukum.[319]
b. Kewajiban *data controller* untuk menjaga kerahasian data.[320] Dan kewajiban pengendali data pribadi untuk menghentikan pemrosesan data pribadi dalam hal pemilik data menarik persetujuannya.[321]
c. Kewajiban untuk melakukan penundaan dan pembatasan pemrosesan data pribadi sebagian atau seluruhnya paling lambat 2 x 24 jam sejak adanya permintaan penundaan atau pembatasan pemrosesan dari pemilik data.[322]
d. Kewajiban untuk melakukan pengamanan dan perlindungan atas data pribadi yang diprosesnya dengan melakukan penyusunan langkah teknis operasional untuk

[316] Pasal 18 RUU PDP
[317] Pasal 19 RUU PDP
[318] Pasal 24 RUU PDP
[319] Pasal 20 RUU PDP
[320] Pasal 21 ayat 1
[321] Pasal 25 RUU PDP
[322] Pasal 26

melindungi dari gangguan, serta penentuan tingkat keamanan berdasarkan sifat risiko.[323]

e. Kewajiban untuk melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data di bawah kendali pengendali data pribadi.[324] Termasuk kewajiban mencegah akses secara tidak sah dengan menciptakan sistem keamanan yang andal.[325]
f. Kewajiban melakukan perekaman terhadap seluruh kegiatan pemrosesan.[326]
g. Kewajiban memberikan akses terhadap pemilik data pribadi terhadap data yang diproses beserta rekam jejak pemrosesan, paling lambat 3 x 24 jam sejak permintaan.[327] Namun, pengendali data pribadi wajib menolak memberikan akses dalam hal diketahui dapat membahayakan keamanan atau kesehatan fisik/mental pemilik data pribadi, berdampak pada pengungkapan data pribadi milik orang lain, atau bertentangan dengan kepentingan nasional.[328]
h. Kewajiban memperbarui atau memperbaiki kesalahan data atau ketidakakuratan data pribadi paling lambat 1 x 24 jam terhitung sejak permintaan diterima.[329] Dalam hal itu, *data controller* wajib menjamin akurasi, kelengkapan dan konsistensi data, dengan melakukan serangkaian upaya verifikasi.[330]
i. Kewajiban untuk melakukan minimalisasi data, yakni, pemrosesan hanya dilakukan sesuai dengan tujuan yang disetujui pemilik data pribadi.[331]
j. Kewajiban mengakhiri pemrosesan apabila jangka waktu retensi telah berakhir; tujuan pemrosesan telah tercapai; atau terdapat permintaan dari pemilik data pribadi.[332] Termasuk kewajiban melakukan penghapusan data pribadi jika data pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan data; pemilik data telah melakukan penarikan persetujuan; terdapat permintaan dari subjek pemilik data; dan perolehan yang bersifat melawan hukum.[333]
k. Kewajiban melakukan pemusnahan data pribadi dalam hal tidak ada nilai guna lagi; telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip; atau terdapat permintaan dari subjek pemiliknya.[334]
l. Kewajiban melakukan pemberitahuan dalam hal terjadi kegagalan pelindungan data pribadi paling lambat 3 x 24 jam, kepada Menteri dan subjek pemilik data pribadi.[335]
m. Dalam hal data diproses oleh pihak ketiga (prosesor) yang ditunjuk oleh pengendali data, pemrosesan data wajib didasarkan pada instruksi atau perintah dari pengendali data pribadi dan berada di bawah tanggung jawab *data controller,* kecuali pemrosesan dilakukan di luar instruksi dari pengendali data.[336]

---

[323] Pasal 27
[324] Pasal 28
[325] Pasal 39 dan 30
[326] Pasal 31
[327] Pasal 32
[328] Pasal 33
[329] Pasal 34
[330] Pasal 35
[331] Pasal 36
[332] Pasal 37
[333] Pasal 38
[334] Pasal 39
[335] Pasal 40
[336] Pasal 43

n. Kewajiban untuk menunjuk petugas pelindungan data pribadi (*data protection officer*) yang professional, kompeten (mengenai hukum perlindungan data pribadi), dalam hal pemrosesan data yang dilakukan untuk kepentingan layanan publik; kegiatan inti yang melakukan pemanfaatan data berskala besar dan sistematis;[337]

Lebih lanjut, RUU PDP mengadopsi penggunaan *data protection officer* dalam GDPR yang bertanggung jawab untuk menginformasikan dan memberi saran kepada kontroler maupun prosesor agar mematuhi kewajiban pelindungan data pribadi; memantau dan memastikan kepatuhan atas undang-undang dan kebijakan PDP; memberi saran mengenai penilaian dampak perlindungan data pribadi dan memantau kinerja kontroler dan prosesor; serta berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan data pribadi, termasuk dalam hal mitigasi risiko.

4.4.1.3. Otoritas Pelindungan Data Pribadi dalam RUU PDP

Dari total 72 pasal yang diatur dalam naskah RUU PDP versi Januari 2020, belum ada satu pun butir pasal yang menyinggung soal otoritas yang akan menangani persoalan pelindungan data pribadi. Padahal, otoritas tersebut diperlukan, bukan sekedar sebagai pengawas, tapi juga memetakan perkembangan standar proteksi dalam kaitannya dengan kegiatan penempatan data pribadi di luar negeri.

Menurut Elsam, lembaga ini menjadi salah satu aktor kunci dalam upaya perlindungan data, yang berfungsi sebagai ujung tombak regulator di bidang privasi dan perlindungan data.[338] Peran kunci lembaga ini tidak hanya sebagai pelaksana kebijakan privasi dan perlindungan data, tetapi juga dalam hal peningkatan kesadaran, konsultasi, dan pengembangan jaringan.[339] Sehingga, tanpa adanya otoritas, maka proteksi data pribadi bisa dikatakan berada sepenuhnya pada inisiatif swa-regulasi pengelola data lewat DPO. Sebagai pembanding, Uni Eropa yang mengenal kebijakan restriksi berdasarkan standar minimal proteksi memberikan kewenangan kepada otoritas *Data Protection Authority* yang berfungsi melakukan penilaian sebelum data pribadi dapat ditempatkan atau ditransfer ke luar negeri.

Dalam perkembangan pembahasannya isu ini telah didiskusikan. Beberapa anggota DPR mengusulkan bahwa fungsi otoritas tersebut bisa diletakkan pada Komisi Informasi di tingkat pusat, agar tidak perlu lagi membentuk satu lembaga baru.[340] Lainnya memandang perlu dilekatkan ke Ombudsman. Perdebatan ini didasarkan pada dua model konsep DPA, yakni otoritas tunggal ataupun *dual*. Model otoritas dual yang memisahkan lembaga yang memiliki kewenangan hampir serupa, seperti Ombudsman dan Komisi Informasi, yang oleh Budiman sebut banyak diadopsi negara-negara Eropa.[341] Sementara, model otoritas tunggal, yaitu satu badan yang secara khusus menangani akses informasi

---

[337] Pasal 45 RUU PDP

[338] Elsam, "Perlindungan Data Pribadi: Perlunya Otoritas Pengawasan Independen", elsam.or.id, kertas kebijakan, 8 Juli 2020, diakses dari https://bit.ly/3xuYYjQ.

[339] *Ibid.*

[340] Komisi Informasi, "Anggota DPR RI Mendukung Lembaga Pelindungan Data Pribadi Digabung ke Komisi Informasi", komisiinformasi.go.id, 25 Januari 2021, diakses dari https://bit.ly/3wCbcqx.

[341] Ahmad Budiman, "Otoritas Pengawas Perlindungan Data Pribadi", *Info Singkat: Bidang Politik dalam Negeri,* Vol. XIII, No.5/I/Puslit/Februari/2021, (Jakarta: Badan Keahlian DPR RI), hlm. 27, diakses dari https://bit.ly/3wQNaIQ.

publik sekaligus pelindungan privasi sebagaimana diterapkan di Jerman, Swiss, Hungaria, dan Irlandia.[342]

Terkait hal itu terdapat beberapa catatan yang perlu diperhatikan terkait pemilihan otoritas ini: *Pertama*, secara tugas, pokok dan fungsi, Komisi Informasi (KI) Pusat dibentuk lewat UU Keterbukaan Informasi Publik sehingga hanya dimandatkan terbatas pada pengelolaan dan pemberian akses informasi publik. *Kedua*, peletakan otoritas PDP di bawah kekuasaan eksekutif seperti kementerian berbeda dengan desain konsep GDPR yang mendorong adanya otoritas independen. *Ketiga*, pemilihan otoritas PDP mesti juga disesuaikan dengan fungsi menangani sengketa perihal PDP. Jika ketiga aspek itu tidak bisa diakomodir, maka kebutuhan pembentukan lembaga baru yang sifatnya khusus jadi tidak bisa dihindari.

4.4.1.4. Pengaturan Transfer Data Pribadi dalam RUU PDP

RUU PDP menggolongkan aktivitas transfer data berdasarkan wilayahnya, yaitu, transfer dalam wilayah Indonesia dan ke luar wilayah Indonesia. Pada prinsipnya, kontroler dapat melakukan transfer kepada kontroler lainnya yang berada dalam yurisdiksi hukum Indonesia sepanjang pihak yang menerima melakukan pelindungan data pribadi. Khusus transfer data pribadi yang merupakan konsekuensi dari aksi korporasi, semisal *merger*, akuisisi, pemisahan atau peleburan; kontroler yang berbadan hukum diwajibkan untuk melakukan pemberitahuan pengalihan data pribadi pada saat sebelum dan sesudah terjadinya kegiatan tersebut.[343]

Sementara, untuk transfer data pribadi ke luar wilayah hukum, hanya dapat dilakukan dalam hal, *pertama*, wilayah tujuan transfer memiliki standar tingkat pelindungan data pribadi yang setara atau lebih tinggi dari Indonesia. Artinya, pertukaran data pribadi bisa leluasa dilakukan sesama negara yang memiliki aturan setara UU Pelindungan Data Pribadi. Meski demikian, hal ini perlu pengelaborasian lebih teknis mengingat harus ada otoritas yang dapat secara berkala melakukan pengumuman perihal negara-negara mana saja yang secara resmi diakui oleh Indonesia memiliki standar PDP yang setara. Selain itu, *kedua,* transfer data lintas batas juga dapat dilakukan berbasis perjanjian internasional antarnegara. Karena sifat muatan pasalnya adalah alternatif, maka kegiatan transfer data lintas batas negara sejatinya tetap bisa dilakukan ke negara yang tidak memiliki standar setara, namun dengan syarat diikat dengan perjanjian internasional. Misalnya, ASEAN Framework on Cross-Border Data Transfer, yang mendorong adanya kemudahan akses bagi negara-negara kawasan Asia Tenggara. Kemudian, *ketiga*, transfer data ke luar wilayah Indonesia juga bisa dilakukan dalam hal terdapat kontrak antar kontroler yang memiliki standar atau jaminan pelindungan yang sesuai undang-undang, atau berdasarkan persetujuan dari pemilik data. Sekilas perbedaan antara pendekatan RUU PDP dan GDPR dalam kegiatan *cross-border data transfer* diuraikan dalam tabulasi dibawah.

Tabel 4.4.1.1 Perbandingan Pengaturan *Cross-Border Data Flow*

[342] *Ibid.*
[343] Pasal 48 RUU PDP

RUU PDP	GDPR
[Pasal 49] Menggunakan 3 (tiga) aspek pertimbangan yang sama dengan GDPR, namun tidak mesti diikuti semuanya (opsional). Bersifat alternatif. Karena pendekatannya alternatif, ini membuka peluang untuk dilakukannya transfer ke negara yang standar perlindungannya berada di bawah Indonesia.	[Art. 44-50] Pendekatan bersifat kumulatif dan tiga aspek pertimbangan harus terpenuhi, yakni: a. Berdasarkan penilaian tingkat kelayakan negara penerima. Jika negara ketiga memiliki kebijakan perlindungan data pribadi yang adekuat berdasarkan penilaian Komisi, transfer data tidak memerlukan otorisasi. b. Adanya perjanjian internasional atau kontrak sesuai standar GDPR. c. Adanya persetujuan pemilik data pribadi

Dalam rilis yang dibuat Dirjen Aptika Kominfo pada 5 November 2020, RUU PDP disebut akan mempermudah pertukaran data dengan negara lain.[344] Hal ini karena standar yang diadopsi RUU PDP, meski mengacu pada GDPR, namun menggunakan pendekatan yang lebih lunak. Dalam beberapa komponen muatan substansi pasal yang dijabarkan, terdapat perbedaan antara kedua instrumen tersebut. Misalnya, dalam hal kewajiban *data controller*, RUU PDP mengatur kewajiban secara umum tanpa melihat tinggi rendahnya risiko pemrosesan data pribadi yang dilakukan, sementara dalam GDPR dilakukan berdasarkan penilaian dampak atau *Data Protection Impact Assessment* untuk pemrosesan yang sifatnya berisiko tinggi.

Dalam hal kewajiban prosesor, dalam RUU PDP beberapa kewajiban prosesor yang juga merupakan kewajiban kontroler data, sementara dalam GDPR dibedakan, dalam arti, kewajiban prosesor berbeda dengan kewajiban kontroler data. Begitu pun dalam hal pembatasan penyimpanan, dalam instrumen Indonesia tersebut dibuka peluang perpanjangan periode penyimpanan sepanjang mekanisme dan tujuannya diatur dalam undang-undang, sedang GDPR hanya memperbolehkan perpanjangan periode penyimpanan untuk tujuan spesifik. Dalam urusan mekanisme sanksi, RUU PDP menggunakan pendekatan sanksi administratif dan pidana, sementara instrumen Uni Eropa itu menggunakan mekanisme sanksi administratif yang detail, semisal, dengan penghukuman denda berbasis *global revenue*.

[344] Dirjen Aptika Kominfo, "UU PDP Akan Permudah Pertukaran Data dengan Negara Lain", aptika.kominfo.go.id, 5 November 2020, diakses dari https://aptika.kominfo.go.id/2020/11/uu-pdp-akan-permudah-pertukaran-data-dengan-negara-lain/

BAB 5

CATATAN TEMUAN BERDASARKAN PEMETAAN REGULASI

Menurut Friedman, dalam mengukur kualitas dan efektivitas hukum harus melihat tiga dimensi yang mempengaruhinya. Ketiganya antara lain (1) substansi hukum; yang berbicara tentang tersedia-tidaknya infrastruktur kebijakan berwujud norma peraturan yang memayungi, atau apakah norma-norma yang dimaksud memiliki nilai kualitas keberlakuan yang baik; (2) struktur hukum, yakni tentang bagaimana para aparatur hukum bisa menjalankan norma-norma yang ada sesuai filosofi dan tujuan pembuatannya; dan terakhir, (3) kultur hukum: bagaimana desain kebijakan hukum yang dimaksud bisa terefleksikan dalam kehidupan kebudayaan sehari-hari publik.[345] Selain itu, tidak terbatas pada frame hukum tersebut, terdapat juga temuan lain sebagai fakta penting yang perlu dimasukan sebagai temuan yang diperoleh dalam proses penelitian ini. Berangkat dari situ, berdasarkan hasil pemetaan regulasi sebelumnya, tercatat beberapa masalah yang ditemukan. Pemaparannya akan dibagi berdasarkan masing-masing dimensi sebagaimana disebut sebelumnya, yakni:

5.1. Dimensi Substansi Hukum

Pada wilayah ini, ditemukan beberapa masalah dalam materi muatan perundang-undangan yang berujung pada tidak optimalnya pelindungan data pribadi, di antaranya:

5.1.1. Obesitas Regulasi

Sebagaimana diuraikan sebelumnya, aturan perihal pelindungan data pribadi saat ini masih tersebar sporadis di berbagai sektor pengaturan, yang umumnya beririsan dalam tataran definisi kontekstual. Misalnya, definisi ‘barang’ dalam UU Perdagangan bisa dilekatkan kepada data pribadi yang dikumpulkan pengendali sehingga data, dengan kata lain, dapat diperlakukan sebagai komoditas perdagangan bebas, terutama dalam situasi ketiadaan undang-undang yang tegas melarang akan itu. Ketidakjelasan ini, di satu sisi, menyebabkan ‘data pribadi’ memiliki status kebendaan tidak ubahnya komoditas umum pada umumnya, padahal di dalamnya terikat dimensi privasi yang jadi kepentingan subjek pemilik data. Semestinya substansi RUU PDP menjelaskan perihal status kebendaan dari data berikut limitasi nilai ekonomisnya, agar data tidak otomatis dapat dikomodifikasi sekalipun dengan dalih persetujuan penggunanya.

Selain itu, masalah substansi juga terlihat pada tidak koherennya aturan spesifik di sektor jasa keuangan, yang relatif berbeda dengan aturan di sektor non-jasa keuangan. Yang awal diatur tersendiri lewat Peraturan OJK dan/atau Peraturan BI, sementara yang terakhir diatur lewat Permenkominfo PDPSE dan/atau PP TPSE. Padahal, keduanya mengadopsi prinsip yang sama, misalnya, dalam hal kewajiban kerahasiaan dan persetujuan atau otorisasi dari subjek data. Lalu, norma pada sektor perbankan memungkinkan ‘rahasia nasabah’ dipertukarkan dalam rangka pertukaran informasi antar

[345] Lawrence M. Friedman, *Hukum Amerika: Sebuah Pengantar, Terjemahan dari American Law: An Introduction*, 2nd Edition, Wisnu Basuki (trans), (Jakarta: Tatanusa, 2001), hlm. 6-8.

bank sementara tidak ada ukuran perihal pembatasan aktivitas pertukaran itu. Akhirnya, kepentingan pemasaran pun bisa leluasa diklaim jadi salah satu kegiatan pertukaran informasi tersebut. Tentu saja jika dikaitkan dengan asas *lex specialis,* diferensiasi tadi bisa diterima mengingat di antara keduanya terdapat rincian konteks kegiatan yang berbeda, namun, jangan dilupakan bahwa objek yang digunakan pada tataran implementasinya adalah sama-sama sistem elektronik. Karena itu, agar kerangka kebijakan yang dibuat konsisten, diperlukan konstruksi pengaturan yang seragam di tiap sektornya.

5.1.2. Tidak Konsistennya Peristilahan yang Digunakan

Permasalahan lainnya muncul seputar penggunaan istilah dalam hukum positif yang berbeda-beda antara satu peraturan perundang-undangan dengan lainnya. Contohnya, pada satu produk undang-undang digunakan istilah 'pemrosesan data', sementara pada regulasi lainnya digunakan istilah 'transmisi'; keduanya memiliki kemiripan karena dalam tiap tahap pemrosesan data (pengumpulan hingga pembukaan), secara teknis pasti terjadi transmisi.

Selain istilah, ada pula ketidakkonsistenan definisi. Data pribadi dalam UU Administrasi Kependudukan relatif berbeda dengan definisinya dalam RUU PDP atau Permen Kominfo PDPSE; lalu di sektor perbankan, misalnya, disebut data konsumen/nasabah. Juga istilah-istilah teknis dalam pelindungan data pribadi, seperti dalam PP TPMSE dan Permen Kominfo PDPSE menggunakan istilah yang relatif berbeda dengan GDPR. Meski hal itu bisa dipahami mengingat perancang peraturan barangkali berupaya agar peristilahan yang dipakai memudahkan dalam dipahami oleh awam. Namun, sebaiknya penggunaan istilah diseragamkan, selain untuk menciptakan kepastian dan keselarasan dengan instrumen di tingkat internasional, juga agar memudahkan pengarusutamaan dan sosialisasi peristilahannya nanti ke khalayak luas.

Perancang perlu memperhitungkan istilah kata serapan yang lebih dekat dengan terminologi asalnya, semisal, menggunakan 'kontroler' (serapan dari '*controller*' dalam bahasa Inggris) daripada menggunakan sebutan 'pengendali'. Ini jadi makin krusial mengingat regulasi atas data, pada praktiknya, bersifat ekstrateritorial imbas dari 'Efek Brussels' aturan perlindungan data pribadi di Uni Eropa. Karena aturan yang dipakai negara lain sangat mungkin punya efek regulatif di sini, penggunaan peristilahan yang seragam akan sangat membantu memudahkan dalam hal penyeragaman standar.

5.1.3. Belum Adanya Aturan Mengenai Anti-Monopoli Digital

Dalam konteks liberalisasi ekonomi digital, belum ada pengaturan spesifik perihal larangan praktik monopoli bisnis digital,[346] baik di level nasional maupun di tingkat internasional. Sementara komodifikasi data terus menjadi konsekuensi yang tak terhindarkan dari aktivitas ekonomi digital. Belajar dari kasus monopoli bisnis digital oleh Facebook dan Google di Amerika Serikat, pengumpulan atas data tak hanya terjadi lewat

[346] Di Amerika Serikat, Facebook dan Google sedang tersandung skandal monopoli bisnis digital yang kini disidangkan oleh Komisi Perdagangan Federal (FTC). Kasus itu mencuat pasca akuisisi besar-besar yang dilakukan kedua perusahaan sementara penyedia layanan tidak memberikan opsi pilihan bagi penggunanya yang enggan tunduk pada kebijakannya—persis praktik monopoli. Lihat lebih lanjut: Andrea Lidwina, "Mengukur Monopoli Bisnis Digital Facebook dan Google", *katadata.co.id*, 17 Desember 2020.

transmisi elektronik, tapi bisa juga lewat akuisisi perusahaan.[347] Kasus itu didapuk menjadi salah satu preseden monopoli data pertama yang tampaknya segera menjadi yurisprudensi untuk kasus-kasus serupa ke depannya. Di Indonesia pun hal ini terjadi: penggabungan unicorn Tokopedia dan Gojek membawa konsekuensi atas dataset konsumen. Di satu sisi ketentuan dalam RUU PDP sudah menyinggung perihal peralihan data pasca *merger* atau penggabungan badan hukum, yang menjalan kegiatan pengendalian data pribadi. Meski demikian, kewajiban yang diharuskan masih berupa pemberitahuan saja. Pendekatan ini dirasa tidak cukup untuk meminimalisir potensi monopoli data oleh satu kontroler, meski sebenarnya memberi pilihan bagi konsumen yang tidak berkenan untuk menuntut penghapusan. Ke depannya, perlu inisiatif-kolektif untuk membuat kebijakan pengaturan terkait hal ini. Undang-undang yang ada saat ini, yakni UU Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat, belum bisa menjangkau model-model monopoli digital terkini.[348]

Selain itu, persoalan turunan dari monopoli data muncul dalam fenomena yang oleh Sudibyo sebut 'monopoli rantai periklanan digital'.[349] Periklanan programatik, di antara semarak lahirnya fenomena promosi digital baru yang lainnya, dapat didefinisikan sebagai penggunaan sistem yang serba otomatis, daring, dan cepat dalam proses penjualan dan pembelian slot iklan.[350] Faktor penguasaan pada data-data terpersonalisasi membuat anak-anak perusahaan dari Google, Facebook, Instagram dibanjiri permintaan periklanan oleh pelaku pasar. Di samping itu, pengaturan di bidang perdagangan perihal nilai ekonomis minimal dan maksimal dari data agaknya diperlukan; semisal tarif ambang bawah dan ambang atas. Pasalnya selama ini penentuan harga atas data ditentukan secara kompromis berbasis permintaan atau penjualan, dan asumsi perihal mekanisme pasar nyatanya tidak benar-benar berjalan. Isu ini akhirnya memberi peluang bagi pemilik bank data untuk secara sepihak menetapkan harga.

5.1.4. Ketimpangan Sanksi dan Konsekuensi Penegakan

Terkait sanksi pidana pun mencuatkan masalah baru. Pelanggaran kerahasiaan data strategis yang dimuat UU Administrasi Kependudukan, misalnya. Sanksi yang diintroduksi untuk tindakan pelanggaran penggunaan data kependudukan relatif sangat kecil, yakni Rp25 Juta atau penjara paling lama dua tahun. Pendekatan sanksi ini jelas sangat timpang jika dibandingkan dengan UU Kearsipan yang mengatur denda sebesar Rp250 Juta dengan pidana penjara paling lama lima tahun. Padahal, jika dikritisi, risiko kebocoran lebih besar pada data-data kependudukan mengingat kelengkapan informasi identitasnya, sementara data dalam ranah kearsipan yang lebih banyak bersifat non-pribadi sehingga bisa dikatakan tak begitu punya daya tarik bagi pelaku bisnis.

Di sisi lain, keberadaan beragam sanksi ini juga menciptakan jenis pelanggaran yang berganda: tidak hanya UU Administrasi Kependudukan, UU ITE juga mengenal sanksi

---

[347] Fahmi Ahmad Burhan, "AS Resmi Sebut Goolge-Facebook Monopoli, Mulai Kaji Aturan Baru", *katadata.co.id*, 16 April 2021, diakses dari https://bit.ly/3pLx1BE.

[348] Lihat: Mohammad Januar Rizky, "Tantangan Penegakan Hukum Anti-Monopoli Era Ekonomi Digital", *hukumonline.com*, (17 Februari 2021), diakses dari https://bit.ly/35YhaGA.

[349] Agus Sudibyo, 'Monopoli Rantai Periklanan Digital', dalam *Jagad Digital: Pembebasan dan Penguasaan,* (Jakarta: Kepustakaan Populer Gramedia, 2019): 63-128, hlm. 67-68.

[350] *Ibid.*

pidana atas transmisi ke dalam sistem elektronik secara melawan hukum. Dalam kronologi banyak kasus kebocoran data kependudukan, pengelola data mengklaim terjadi peretasan ke dalam sistem sehingga data-data strategis itu bisa diakses lagi diambil secara illegal. Karenanya, ketimpangan beban sanksi ini juga menyisakan problem tersendiri lain, sebab jika menggunakan pendekatan asas *lex specialis*, ketentuan pada UU Administrasi Kependudukan haruslah diterapkan pada kasus pelanggaran data kependudukan (mengingat undang-undang itu lebih khusus mengatur tentang objek datanya, dan pengelolaan data pribadi yang dilakukan oleh badan publik). Namun, penggunaan instrumen sebelumnya dengan sendirinya 'meringankan' sanksi bagi pelakunya, mengingat lamanya masa hukuman yang dikenal pada UU Administrasi Kependudukan jauh lebih rendah dari delik transmisi illegal dalam UU ITE.

5.1.5. Terbukanya Potensi Manipulasi Asas Konsensualitas

Baik RUU PDP maupun serangkaian hukum positif tentang PDP yang saat ini berlaku mensyaratkan adanya persetujuan atau otorisasi dari pemilik data dalam pengumpulannya. Yang jadi catatan, dalam kaitannya dengan hak privasi, konsensualitas yang dimaksud semestinya tidak bisa dibatasi dengan pilihan biner (setuju atau tidak setuju) dengan dalih kebebasan berkontrak. Keberadaan klausula demikian dalam praktiknya kerap membuat posisi tawar data subjek tak berarti di hadapan penyelenggara sistem elektronik.

Dalam penyediaan layanan aplikasi saat ini, data kontroler seringkali memberlakuan klausula baku 'setuju sepenuhnya atau tidak sama sekali'. Artinya, jika pemilik data menemui satu saja ketentuan kebijakan privasi yang tidak disetujui, maka pemberi layanan tidak akan memberi akses guna kepadanya. Padahal, jika berpegang sepenuhnya pada konsep privasi, otonomi individu tidak terbatas pada dua pilihan: paling tidak harus ada opsi pilihan ketiga. Contoh baik ditunjukan pada praktik pengumpulan identitas diri pada formulir daring, misalnya, pengisi dapat memilih untuk mengisi atau tidak mengisi kolom gender (pilihannya ada tiga: 'laki-laki', 'perempuan', atau 'cenderung tidak ingin memberitahu'). Perlakuan serupa jarang muncul dalam konteks pengumpulan data untuk kepentingan personalisasi iklan karena penyedia layanan memberlakukan sistem 'wajib diisi'. Ringkasnya, semestinya tersedia pilihan-pilihan ketiga di mana pemilik data bisa menolak memberikan informasi pribadinya atas dasar privasi, tanpa menghilangkan kesempatan akses terhadapnya.

Lagipula, memperhatikan tingkat literasi (keamanan) digital masyarakat Indonesia yang relatif rendah, penggunaan konsensus-biner tadi justru membuka ruang untuk pengumpulan data secara eksesif, yang pada akhirnya bertentangan dengan prinsip minimalisasi data. Pada banyak survei ditemukan bahwa mayoritas masyarakat, dalam melakukan pendaftaran suatu akun, tidak berhitung matang-matang perihal apa tujuan penggunaan data miliknya yang dikumpulkan.[351] Artinya, sebagian besar persetujuan pemrosesan diberikan pemilik data tanpa pemahaman atau kesadaran atas risiko.

Dalam KUHPerdata sendiri, meski mengenal asas kebebasan berkontrak dan konsensualitas (kesepakatan) sebagai syarat sahnya perjanjian, namun kontrak akan selalu bisa dibatalkan jika pada saat pembuatannya mengandung unsur kekhilafan dari salah satu

[351] CNN Indonesia, "Riset Pengguna Internet Rela Bagi Data Pribadi Demi Gratisan", *cnnindonesia.com,* 9 Oktober 2019, diakses dari https://bit.ly/2RNbeNe.

pihak[352] atau terindikasi adanya penyalahgunaan kehendak. Kekhilafan bisa terjadi manakala ada klausula-klausula merugikan yang sedari awal tak dijabarkan untuk diketahui salah satu pihak dalam perjanjian. Dalam teori, masalah ini beririsan dengan perluasan konsep *unjust enrichment* yang dikenal dalam doktrin hukum perikatan.[353] Bahwa setiap keuntungan yang didapatkan seseorang yang didapat berdasarkan kesalahan/kelalaian pihak lain semestinya tak serta merta menggugurkan hak dari pihak lain itu untuk menuntut pengembalian/pemulihan walau pihak yang diuntungkan itu pada dasarnya tidak juga salah.
Sedang keterpaksaan mengikat perjanjian atau penyalahgunaan kehendak pada praktiknya dipicu dari adanya adanya ketimpangan relasi, semisal dalam konteks ekonomi.

Contohnya, pada situasi pandemi hari ini di mana semua aktivitas pertemuan beralih ke digital, seseorang bisa saja tidak menghendaki data-data pribadinya diambil oleh aplikasi video conference karena tidak setuju dengan kebijakan privasinya, tapi keadaan tidak memberinya pilihan dan mau tak mau memaksanya untuk tetap menggunakan, yang sama saja berarti harus menerima kebijakan privasi dari aplikasi. Pengguna yang memiliki kesadaran keamanan digital tinggi pun sering menghadapi kendala yang sama karena klausula baku kebijakan privasi yang ditetapkan. Dalam skenario itu, sekalipun berkeberatan atas penggunaan data pribadinya, pengguna sering kali terpaksa menyetujui karena membutuhkan aplikasi tersebut untuk menunjang kegiatannya. Oleh karena itu, selain perlu mengatur rincian larangan klausula baku terhadap konsumen digital, RUU PDP perlu menempatkan pula kewajiban bagi pengendali data untuk memasukan opsi ketiga sebagai manifestasi privasi.

5.1.6. Belum Adanya Penegasan tentang Aturan Pilihan Hukum

Pengaturan perihal pilihan hukum harus dipertegas dan dimasukan ke dalam bagian yang tak terpisahkan dari informasi pemrosesan data, yang diwajibkan untuk disediakan oleh data kontroler. Hal ini jadi krusial mengingat lokasi data bisa jadi dasar untuk memberlakukan yurisdiksi hukum. Sementara, ketika data-data sudah ditempatkan di luar wilayah Indonesia, bukan tidak mungkin data subjek bisa terjebak dalam standar

---

[352] Pasal 1321 KUHPerdata: "Tiada suatu persetujuan pun mempunyai kekuatan jika diberikan karena kekhilafan atau diperoleh dengan paksaan atau penipuan."

Pasal 1322 KUHPerdata: "Kekhilafan tidak mengakibatkan batalnya suatu persetujuan, kecuali jika kekhilafan itu terjadi mengenai hakikat barang yang menjadi pokok persetujuan. Kekhilafan tidak mengakibatkan kebatalan, jika kekhilafan itu hanya terjadi mengenai diri orang yang dengannya seseorang bermaksud untuk mengadakan persetujuan, kecuali jika persetujuan itu diberikan terutama karena diri orang yang bersangkutan."

[353] Fajar Kurniawan, Peter Mahmud Marzuki, dkk, 'Unsur Kerugian dalam *Unjustified Enrichment* untuk Mewujudkan Keadilan Korektif', *Yuridika,* Vol. 33 No. 1, (Januari 2018): 19-39, hlm. 20.

Kasus serupa digambarkan oleh Kurniawan dkk: "Contoh paling nyata dan kerap digunakan untuk menggambarkan keadaan tersebut adalah terjadinya kesalahan pembayaran. Seorang pelanggan yang salah membayar tagihannya sebanyak dua kali seharusnya berhak atas pengembalian pembayaran yang dilakukan untuk kedua kalinya. Akan tetapi dalam kondisi tersebut, pembayaran kedua yang dilakukan oleh pelanggan yang bersangkutan dilakukan tanpa adanya hubungan kontraktual dengan penjual, begitu pula penjual juga tidak melakukan kesalahan yang menyebabkan pelanggannya melakukan pembayaran untuk kedua kalinya. Dengan kata lain, pelanggan tersebut tidak dapat mengajukan gugatan atas dasar hubungan kontraktual maupun perbuatan melanggar hukum. Hal tersebut jelas bertentangan dengan prinsip-prinsip dasar dari keadilan sebagai salah satu tujuan hukum yang utama, di antara tujuan kepastian hukum dan tujuan kemanfaatan hukum."

pengungkapan yang digunakan negara asing. Semisal, adanya restriksi mengeluarkan data pribadi ke luar wilayahnya. Pada gilirannya, faktor ini pun akan menyulitkan penegakan hukum lintas-teritori manakala antara Indonesia dan negara pihak ketiga dimaksud belum terikat pada kerjasama internasional mengenai pelindungan privasi. Untuk itu, pilihan hukum yang berpihak pada subjek data mesti dirumuskan eksplisit sebagai bagian dalam kebijakan privasi. Kebutuhan ini semakin kentara sebab di saat bersamaan pemerintah diketahui sedang menyusun regulasi terkait Rancangan Undang-Undang Hukum Perdata Internasional (RUU HPI), yang salah satunya mengatur terkait pengaturan pilihan hukum. Penyesuaian diperlukan agar konstruksi ketentuan perihal pilihan hukum dalam regulasi yang disusun RUU HPI berkoresponden dengan kepentingan privasi data dalam RUU PDP.

5.1.7. Pengaturan Perihal Aliran Data Bebas Cenderung Berseberangan dengan Upaya Pemaksimalisasian Proteksi atas Privasi

Dalam muatan PP TPSE, Indonesia menunjukan gestur membuka diri pada kebijakan fleksibilitas penempatan data, bahkan untuk data-data strategis yang dikelola badan publik. Manuver kebijakan ini sama sekali berbeda dengan pendekatan restriksi yang digunakan sebelumnya, yakni kewajiban lokalisasi data. Sebelumnya, penyelenggara sistem elektronik lingkup publik (dan privat yang menjalankan kegiatan pelayanan publik) diharuskan punya pusat data di Indonesia. Dalam praktiknya terdapat dua jenis restriksi yang marak digunakan, pertama kewajiban penyeragaman standar pelindungan dan kedua lokalisasi data. Kebijakan pertama mensyaratkan sebelum transfer data dilakukan, negara tujuan penempatan harus memiliki standar pelindungan data pribadi yang minimal setara atau lebih tinggi dari negara asalnya; sedang yang kedua sama sekali melarang migrasi data-data tertentu keluar negeri karena alasan proteksionis.

Penundaan demi penundaan pengesahan RUU PDP akhirnya membuat Indonesia kehilangan momentum puncaknya sebab pasca pandemi, yang membawa migrasi besar pola konsumsi ke digital, inisiasi komunitas internasional mulai bergerak ke arah tuntutan pelonggaran hambatan. Dalam skenario itu, muatan substansi RUU PDP akan sangat mungkin terpengaruh dinamika perundingan yang berlangsung. Dikhawatirkan, pada pembahasannya nanti agenda-agenda baru untuk mendukung liberalisasi aliran data justru diakomodasi RUU PDP dan hal itu akan berkonsekuensi menurunkan standar proteksi privasi yang diharapkan. Sinyal ke situ sudah tertangkap sejak eks-Menkominfo Rudiantara menyebut pelonggaran itu akan membuka sumur devisa tambahan negara dari aktivitas ekonomi digital.

Persoalan mendasar dari hal itu muncul lantaran upaya pemaksimalisasian privasi dan pelonggaran arus data lintas negara adalah dua kebijakan yang secara naluri berseberangan. Yang satu menghendaki data seminim mungkin dikumpulkan sekalipun berbasis konsensus dari pemiliknya; sementara yang satu lagi menghendaki keleluasaan pengungkapan dan pemindahan lokasi penempatan. Oleh karena itu, pemerintah dan DPR harus berhati-hati dan berhitung matang-matang sebelum mengangkat agenda ekonomi di atas isu privasi. Jangan juga dilupakan bahwa jumlah pengguna internet yang banyak membuat Indonesia jadi sasaran empuk praktik *phishing*. Jangan sampai akibat ambisi ekonomi yang belakangan makin menguat pasca krisis pandemi, justru melegitimasi agenda baru di atas upaya maksimalisasi standar pelindungan data pribadi.

5.1.8. Masih Ada Kekosongan Pengaturan Fungsi Otoritas Pelindungan Data Pribadi

Draf RUU PDP versi Januari 2020 belum mengatur tentang otoritas pelindungan data pribadi. Padahal, otoritas yang dimaksud akan menjalankan fungsi strategis dalam melakukan pengawasan atas implementasi PDP. Dalam praktik di berbagai negara khususnya benua Eropa, masing-masing negara memiliki satu *Data Protection Authority* (DPA) yang berfungsi melakukan tata kelola standar pelindungan data. Misalnya, Belanda memiliki *Autoriteit Persoonsgegevens (AP)* yang merupakan lembaga independen berbadan hukum yang berfungsi sebagai pengawas atas kepatuhan terhadap standar pelindungan data pribadi sesuai GDPR.[354] Sebagai badan hukum tersendiri, AP tidak terikat pada *Ministry of Justice and Security* Belanda, namun dapat berkoordinasi dalam pelaksanaan tugas dan fungsinya. Sementara, Prancis memiliki DPA yang berbentuk komisi nasional dan bernama *Commission Nationale de l'Informatique et des Libertés* (CNIL), sebuah lembaga pemerintahan dengan fungsi mirip dengan AP, namun ditambah dengan kewenangan menjatuhkan denda. CNIL sendiri telah dibentuk sejak 1974.

Pada konteks Indonesia, pembahasan masih terjebak pada usulan penggabungan DPA ke Komisi Informasi (KI) pada level pusat. Namun, sejauh ini tidak bisa dibaca ke mana arah keputusan yang akan diambil karena di satu sisi KI selama ini hanya berwenang mengurusi informasi yang bersifat terbuka untuk publik. Bagaimanapun, ketiadaan otoritas khusus yang ditunjuk RUU PDP sangat disayangkan karena DPA sebenarnya adalah komponen penting dalam hukum pelindungan data pribadi mengingat ia punya peran strategis untuk bukan hanya melakukan pengawasan namun juga memastikan bahwa standar regulasi pelindungan data pribadi terimplementasikan oleh pemangku kepentingan.

5.1.9. Perumusan Sanksi Pidana pada RUU PDP Dinilai Tidak Tepat

Menurut Lintang dari Lembaga Studi dan Advokasi Masyarakat (ELSAM), naskah RUU PDP saat ini memiliki masalah terkait dengan pemberlakuan sanksi pidana yang sebenarnya tidak diperlukan oleh model regulasi administratif setipe RUU PDP.[355] Pada naskah terakhir terdapat sembilan pasal pidana, mulai dari Pasal 61 hingga Pasal 69, yang salah satunya merumuskan hukuman penjara hingga tujuh tahun. “Penggunaan pasal pidana tidak tepat karena sifat RUU PDP adalah tata kelola data dan privasi sehingga ketika terjadi pelanggaran, itu masuk ke ranah kejahatan siber yang sudah diatur dalam UU ITE”, jelas Lintang. Dalam konstruksi hukum pidana, kejahatan dengan ancaman pidana di atas lima tahun tergolong sebagai tindak pidana serius yang memberi peluang pada penegak hukum untuk melakukan penahanan.

Upaya mempertahankan sanksi pidana ini bisa jadi berbalik merugikan publik, selain juga membuka celah korupsi baru, karena sangat mungkin berpotensi menciptakan pendekatan punitif yang rawan kriminalisasi. Desakan penghapusan pasal pidana juga disampaikan oleh Asosiasi Penyelenggara Telekomunikasi Seluruh Indonesia (ATSI) bahwa perumusan sanksi pidana bisa menyebabkan tumpang tindih, selain dengan undang-undang yang sudah ada sebelumnya, juga pada gilirannya bertabrakan dengan model

---

[354] Autoriteit Persoonsgegevens, “Organization”, *autoriteitpersoonsgegevens.nl*, (n.d), diakses dari https://bit.ly/3qglM4n.

[355] Berdasarkan wawancara dalam *Focus Group Discussion* IGJ-PSHK dengan Blandina Lintang dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) tanggal 19 Juni 2021.

pendekatan sanksi pidana korporasi yang diatur dalam Peraturan Mahkamah Agung Nomor 1 Tahun 2016.[356] Jika pun memang dibutuhkan untuk merekayasa perilaku pengendali data, pendekatan yang lebih tepat adalah sanksi administratif semisal denda (dengan hitungan persentase pendapatan tahunan), sebagaimana juga diterapkan dalam GDPR.

5.1.10. Substansi Hukum Belum Mengantisipasi Terjadinya Diskriminasi Digital

Perlindungan data pribadi akan berkaitan erat dengan pemanfaatan teknologi *big data* dan salah satu tantangan besar dalam meregulasi tata kelola sistem elektronik adalah memastikan algoritme yang didesain penciptanya bebas dari diskriminasi. Fenomena ini belakangan disebut 'diskriminasi digital'. Menurut Criado dan Such, *"Digital discrimination entails treating individuals unfairly, unethically, or just differently based on their personal data that is automatically processed by an algorithm. Digital discrimination often reproduces the existing instances of discrimination in the offline world by either inheriting the biases of prior decision-makers, or simply reflecting widespread prejudices in society."*[357] Isu ini mulai diantisipasi oleh banyak negara maju. Teranyar, pada 2014 terjadi kasus yang disebut "Airbnb Case". Luca dan Edelman menemukan bahwa penggunaan algoritma pada *platform* airbnb.com, di mana penyewa diberikan fitur untuk bisa membuat preferensi tertentu untuk memasarkan produknya, nyatanya telah menciptakan bentuk diskriminasi digital terhadap calon penyewa berlatar belakang ras minoritas di New York.[358]

Pada konteks RUU PDP sendiri, dari naskah terakhir belum terlihat adanya pengakuan asas non-diskriminasi atau hak subjek data untuk bebas dari tindak diskriminasi dalam konteks pengambilan keputusan berbasis teknologi kecerdasan buatan. Padahal, isu yang terakhir disebut juga berada pada siklus penganalisisan data dan informasi sehingga beralasan untuk diatur dalam kerangka regulasi PDP. Meski memang akan sangat menantang bagi perancang untuk bisa mengatur hingga ke wilayah pemrograman, tapi perlindungannya bisa dimulai dengan upaya perumusan asas non-diskriminasi agar setidaknya meletakan acuan filosofis pada kerangka regulasi perihal data dan pemrosesan data—bahwa diskriminasi digital merupakan sebuah keniscayaan. Aturan yang ada saat ini sebenarnya telah mengatur kewajiban penyerahan kode sumber (s*ource code)* perangkat lunak ke otoritas yang ditunjuk pemerintah.[359] Menurut Hartadi, pemrogram dari Pusat Ilmu Komputer Fakultas Ilmu Komputer Universitas Indonesia, algoritma yang dipakai

---

[356] "Sanksi Pidana dalam RUU PDP Diminta Dihapus", *kompas.com*, 9 Juni 2020, diakses dari https://bit.ly/2SfTbzv.

[357] Lihat: Natalia Criado dan Jose M Such, "Digital Discrimination", dalam Karen Yeung (Ed) dan Martin Lodge (Ed), *Algorithmic Regulation,* (Oxford: Oxford University Press, 2019).

[358] Benjamin G. Edelman dan Michael Luca, "Digital Discrimination: The Case of Airbnb.com", *Harvard Business School NOM Unit Working Paper No. 14-054*, (January 10, 2014). DOI: http://dx.doi.org/10.2139/ssrn.2377353.

[359] Indonesia, P*eraturan Pemerintah tentang Penyelenggara Sistem dan Transaksi Elektronik...*, Pasal 9 ayat (1): "Pengembang yang menyediakan Perangkat Lunak yang khusus dikembangkan untuk Penyelenggara Sistem Elektronik Lingkup Publik *wajib menyerahkan kode sumber* dan dokumentasi atas Perangkat Lunak kepada Instansi atau institusi yang bersangkutan."

sebuah perangkat bisa dilihat dari kode sumber.[360] Sehingga, mekanisme penyerahan kode sumber itu bisa ditindaklanjuti untuk menilai apakah suatu perangkat mengandung bias diskriminasi atau tidak dalam pemrogramannya. Dengan memasukan asas non-diskriminasi, perancang secara simbolis mengakui bahwa bias digital adalah problem yang niscaya terjadi. Beberapa negara pun dilaporkan mulai menyusun kerangka regulasi non-diskriminasi digital, termasuk salah satunya Belanda.[361]

5.2. Dimensi Struktur

Beberapa refleksi permasalahan pada dimensi struktur yang ditemukan berdasarkan temuan peta regulasi yang dikaitkan dengan fenomena yang muncul di lapangan adalah antara lain:

5.2.1. Penambahan Regulasi Tidak Menjamin Optimalnya Perlindungan

Berkaca pada preseden beberapa tahun terakhir, sekalipun sudah ada UU ITE, PP PSTE, Permen Kominfo PDPSE serta beberapa regulasi inti lainnya, pelanggaran data pribadi masih marak terjadi. Bahkan, sebagian besar bersumber dari kebocoran sistem milik penyelenggara sistem elektronik yang merupakan badan publik. Anomali ini membawa pada keyakinan bahwa sesempurna apapun materi muatannya dibuat, implementasinya akan sangat bergantung pada kemampuan otoritas untuk tidak hanya melakukan pengawasan tetapi juga melakukan penegakan hukum.

Sejauh ini otoritas bisa dikatakan belum berhasil menunjukan bahwa keberadaan hukum positif perihal perlindungan data pribadi telah benar-benar efektif dijalankan. Isu pada dimensi struktur ini jadi persoalan utama yang perlu dibenahi agar problem serupa tidak berulang pasca keberlakuan RUU PDP nantinya. Dengan kata lain, selain perlu memastikan secara substansi telah memiliki standar pelindungan yang baik sesuai *best practice* internasional, problem utamanya adalah bagaimana negara mampu memastikan substansi itu terimplementasikan.

5.2.2. Terlalu Banyak Otoritas Menimbulkan Kecenderungan Saling Lempar Tanggung Jawab

Pada bagian sebelumnya telah diulas perihal potensi tumpang tindih kewenangan otoritas. Selama ini ada beberapa otoritas berbeda yang saling beririsan dalam konteks PDP, semisal Kemkominfo untuk urusan tata kelola informasi dan sistem elektronik, Badan Sandi dan Siber Negara (BSSN) untuk urusan keamanan jaringan, dan Otoritas Jasa Keuangan (OJK) untuk pengaturan PDP konsumen jasa keuangan dan bidang perbankan. Di satu sisi, banyaknya otoritas bisa jadi sebuah hal positif manakala fungsinya teroptimalisasi sesuai porsi yang didesain. Namun, realitasnya di sisi lain menunjukan bahwa terlalu banyak otoritas cenderung membuat pembagian kewenangan tidak jelas dan pada gilirannya memunculkan anomali seperti kecenderungan saling lempar tanggung jawab, terutama manakala terjadi kegagalan pelindungan data pribadi.

---

[360] Berdasarkan wawancara dengan Budi Hartadi dari Pusat Ilmu Komputer Fakultas Ilmu Komputer Universitas Indonesia tanggal 21 Juni 2021.

[361] Fredrick Borgesius, "Strenghtening legal protection against discrimination by algorithms and artificial intelegence", *The International Journal of Human Rights,* Vol. 24 No. 10, (2020): 1572-1593. Doi:10.1080/13642987.2020.1743976

Oleh karena itu, perlu dibuat penegasan yang konkret mengenai tugas, pokok, dan fungsi lewat pembentukan satu otoritas independen (DPA) yang dimandatkan lewat undang-undang PDP, yang nantinya diharapkan mampu mengintegrasikan seluruh fungsi berkaitan dengan pelindungan data pribadi dalam satu badan khusus. Tantangan selanjutnya adalah untuk memastikan transisi itu berjalan dengan lancar serta meleburkan/membubarkan fungsi lembaga yang dinilai tidak berhasil bekerja optimal.

5.2.3. Inferioritasi Isu PDP di Hadapan Upaya Pemaksimalisasian Ekonomi

Salah satu faktor penghambat pelindungan privasi data datang dari problem komodifikasi. Diketahui, meskipun secara sektoral perlindungan data pribadi dalam penyelenggaraan administrasi kependudukan sudah diatur, beberapa preseden terkini memperlihatkan bahwa kinerja pemerintah tidak cukup serius dalam memperlakukan ketiga kriteria perlindungan tadi, terutama poin yang terakhir. Pada 2019, misalnya, Menteri Dalam Negeri Tjahjo Kumolo justru menekan kerja sama dengan pihak swasta untuk memberi akses pihak swasta pada data pribadi penduduk, termasuk nomor induk kependudukan (NIK), dan Kartu Tanda Penduduk elektronik (e-KTP).[362] Dilaporkan, ada lebih dari 1300 instansi dan lembaga yang bisa akses data kependudukan.[363] Lembaga Studi Advokasi dan Masyarakat (ELSAM) juga menyayangkan pihak Mendagri tidak menjelaskan hak akses seperti apa yang diberikan dalam Perjanjian Kerja Sama tersebut.[364] Jika perlakuan atas data kependudukan yang bersifat administrasi publik saja sedemikian leluasa ditransaksikan oleh otoritas, bagaimana praktiknya dengan data pribadi yang dikelola pihak swasta. Meskipun UU Administrasi Kependudukan (UU No. 23/2006 jo UU No. 24/2013) membuka peluang kerjasama penggunaan data kependudukan, khususnya untuk alasan pengembangan layanan publik (Pasal 58 ayat (4) UU Adminduk), namun ancaman eksploitasi data pribadi mengintai dalam pelaksanaan kerjasama ini.[365]

Inferiorisasi isu publik seperti pelindungan privasi kerap terjadi ketika disandingkan dengan isu-isu lain seperti pertumbuhan ekonomi. Pasalnya, dalam rencana pembangunan jangka menengah, pertumbuhan ekonomi yang salah satunya ditumpu dari sektor digital masih jadi prioritas nasional yang mendominasi, dan hal ini bukan tidak mungkin akan membawa dampak tukar terhadap pelindungan privasi secara umum. Sinyal ini sudah terlihat pada revisi PP PSTE tahun 2019 silam. Contohnya, penempatan data strategis bagi PSE lingkup publik yang awalnya diwajibkan memiliki pusat data di dalam negeri, kini dimungkinkan ditempatkan di luar wilayah Indonesia.

5.2.4. Setengah Hati Mengakui Kebebasan Digital

Masalah juga datang karena komitmen pemerintah mendorong pertumbuhan ekonomi dari sektor ekonomi digital tidak lantas diiringi dengan pemberian jaminan akan otonomi

---

[362] Dias Prasongko, "Kemendagri dan Jasa Keuangan Teken Kerja Sama Manfaatkan NIK", *tempo.co*, (15 Januari 2019), diakses dari https://bit.ly/3jet5Ip.

[363] Kontan, "Ada Lebih dari 1300 Instansi dan Lembaga yang Bisa Akses Data Kependudukan", *kontan.co.id*, (14 Juni 2020), diakses dari https://bit.ly/3xYwKxW.

[364] ELSAM, 'Kemendagri harus tinjau ulang Kerja Sama Pemberian Akses Data Kependudukan', *elsam.or.id*, (2 Agustus 2019), diakses dari https://bit.ly/35WQrKx.

[365] ELSAM, "Kerentanan Perlindungan Data Pribadi dalam Pengelolaan Data Kependudukan", *elsam.or.id*, (22 Juli 2019), diakses dari https://bit.ly/3gXb1AU.

digital yang memadai—baik terhadap pelaku usaha maupun masyarakat pengguna. Terlihat adanya upaya untuk memanfaatkan momentum perlindungan data pribadi guna mendorong model kebijakan proteksionis atau bahkan surveilans, yang sebenarnya tak begitu relevan dibutuhkan. Memang peran negara dibutuhkan untuk meminimalisasi risiko, tapi bukan berarti negara bisa terlalu tampil intervensif dengan alasan perlindungan.

Corak proteksionis terlihat dari Permen Kominfo Nomor 5 Tahun 2020 yang mewajibkan Penyelenggara Sistem Elektronik untuk memberi akses kepada otoritas, bukan hanya berdasarkan kebutuhan penegakan hukum, tapi juga berdasarkan penilaian ketertiban umum—yang tidak memiliki ukuran yang baku, dan pada gilirannya dapat memberi kewenangan bagi otoritas untuk melakukan *take down* konten berdasarkan perintah. Intervensi ini terbilang sudah masuk terlalu dalam pada ranah privasi pengguna *platform,* serta rentan melanggar hak sipil warga karena berpotensi mengatur kebebasan berekspresi digital warganet, mengingat negara bisa senantiasa menyeleksi peredaran konten yang dinilai berbahaya berdasarkan subjektivitas otoritas. Bukan hanya mengganggu kebebasan digital, kebijakan semacam ini juga dirasa memberatkan penyedia aplikasi lantaran memberi beban kewajiban baru berbentuk pemberian akses setiap kali dibutuhkan.

5.2.5. Keterbatasan Pemahaman Sumber Daya Manusia

Pelindungan data pribadi merupakan isu multidimensi yang membutuhkan atensi setiap pemangku kepentingan. Masalah pada dimensi sumber daya manusia (SDM) muncul karena adanya gap pengetahuan teknis antara pelaksana di bidang IT, regulator dan pelaksana. Mulai dari persoalan peristilahan hingga perbedaan logika berpikir disipliner. Misalnya, pelaksana pada bagian IT pada suatu departemen bisa saja memahami teknis tata kelola sistem dan pemrosesan data, tapi di sisi lain tidak begitu paham tentang aspek hukum atau filosofi privasi. Ada perbedaan naluri pada logika berpikir eksakta dan sosial: mayoritas pelaku IT beranggapan pengumpulan data sebanyak mungkin dibutuhkan karena informasi yang padat akan jadi bekal sempurna bagi pemrosesan. Prinsipnya, *the more (data) the merrier*. Tapi, di sisi lain logika eksakta itu berseberangan dengan konstruksi berpikir konsep privasi yang secara naluri menghendaki pengumpulan data seminimal dan serelevan mungkin karena ada risiko-risiko sosial di dalamnya.

Problem ini bisa selesai jika SDM pelaku IT yang dimaksud juga punya perspektif hukum yang mumpuni, tapi kombinasi yang diharapkan itu agaknya jarang ditemui. Selain itu, sekalipun sebuah norma hukum telah coba dibahasakan dengan bahasa awam, perbedaan penggunaan terminologi kerap membuat orang berlatar belakang non-hukum kesulitan memahaminya karena telah terbiasa menggunakan terminologi teknis. Perbedaan itu misalnya, istilah *data analysis* yang dalam rumusan hukum disebut ‘pengolahan’; atau istilah kode sumber yang oleh pelaku IT lebih dikenal sebagai ‘*source code*’. Begitupun sebaliknya, pelaksana pada bidang hukum yang notabene mengerti asas-asas pelindungan kerap terkendala pada konteks pemahaman teknis komputasi.

5.2.6. Banyak Laporan Pelanggaran Data Pribadi Tidak Diterima/Ditindaklanjuti Kepolisian

Salah satu problem struktural yang terlihat adalah ketidakmampuan kepolisian untuk menindaklanjuti laporan perihal pelanggaran data pribadi. Ini berkaitan erat dengan masalah yang disebut sebelumnya. Dilansir oleh Kompas, sepanjang 2020 ada tujuh kasus kebocoran data pribadi yang terlaporkan, yaitu kasus Tokopedia (sejumlah 91 juta data pribadi pengguna), bhineka.com (sejumlah 1,2 juta data pengguna), kebocoran data KPU tentang data pemilih tetap (sejumlah 190 juta data pemilih), Kredit Plus (sejumlah 890 ribu data nasabah), ShopBack (data kartu kredit pengguna), Red Doorz (5,8 juta data pengguna), dan Cermati (sejumlah 2,9 juta data pengguna).[366] Jumlah yang fantastis sebelumnya belum menghitung laporan yang datang dari orang-perorang yang diduga berjumlah jutaan.

Persoalannya, meski merupakan sebuah tindak pidana dalam banyak undang-undang, banyak laporan dari masyarakat yang kemudian dimentahkan oleh unit *cyber crime* di kantor-kantor kepolisian. Menurut informasi yang didapat dari wawancara dengan sejumlah informan (identitas sengaja dirahasiakan), beberapa alasan yang kerap diangkat petugas administrasi kepolisian antara lain: (1) jumlah kerugian tidak bisa dipastikan (atau terlalu kecil); (2) Polsek atau Polres tidak memiliki unit sendiri sehingga pelapor diminta untuk mengadu ke Polda; (3) Pengadu diminta menghubungi perusahaan penyedia platform terlebih dahulu; (4) Belum timbul kerugian dari kejahatan (walaupun data sudah berpindah tangan secara ilegal); (5) tidak ada bukti telah terjadi kejahatan.[367]

Logika kepolisian, khususnya pada poin nomor satu dan empat, tentu keliru karena pelanggaran data pribadi bersifat delik formil—yang merujuk pada perbuatannya, sehingga alasan 'tidak adanya akibat' tidak bisa dipakai untuk menolak laporan dari korban. Terlebih, sifat kerugian dari kasus pelanggaran data pribadi tentu tidak langsung, namun lebih bersifat tidak langsung dan mengganggu kenyamanan privasi dari subjek data. Kemudian, kecenderungan menolak laporan karena tidak ada bukti konkret pun patut dikritisi mengingat pembebanan kewajiban pembuktian pada korban tentu adalah perspektif yang salah karena akan membuat korban semakin terperangkap pada masalah yang dihadapi, dan pada gilirannya akan membuat korban kapok untuk melapor kembali karena terbebani keharusan membuktikan yang semestinya berada pada domain tugas dari penyidik.

5.3. Dimensi Kultur

Beranjak dari struktur, problem lebih pelik muncul dalam konteks masyarakat, terutama berkaitan dengan aspek literasi digital. Beberapa permasalahan pada dimensi kultur yang teridentifikasi adalah sebagai berikut:

5.3.1. Rendahnya Tingkat Literasi Digital Masyarakat

Menurut Tulus Abadi dari Yayasan Lembaga Konsumen Indonesia (YLKI), karakter konsumen di Indonesia memiliki beberapa problem, yakni: (1) tidak cermat membaca syarat dan ketentuan yang berlaku; (2) tidak cermat membaca kontrak perjanjian

[366] Conney Stephanie, "7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020", kompas.com, (1 Januari 2021), diakses dari https://bit.ly/3x0jby5.

[367] Wawancara dilakukan selama periode 4 hingga 23 Juni 2021 dengan delapan korban PDP (informan) yang mengaku pernah melakukan pelaporan ke polisi namun mengalami penolakan.

elektronik; (3) tidak paham konten/substansi perjanjian elektronik; (4) cenderung gampang menyerahkan data pribadi; (5) kurang memahami proses bisnis dan *product knowledge* aspek digital ekonomi.[368] Pendapat Tulus patut jadi catatan penting mengingat demografi pengguna internet Indonesia sangat besar. Idealnya, ketika suatu angka demografi tinggi, harus diikuti dengan meningkatnya pemahaman akan keamanan data pribadi. Artinya sekalipun sebuah kebijakan privasi telah dibuat, namun ketika pengguna tidak membaca dengan sungguh-sungguh, akan rentan menimbulkan problem di lain waktu, terutama ketika data yang disetujui dipindahtangankan ke pihak ketiga. Di lain pihak, temuan lainnya menunjukan bahwa konsumen digital Indonesia cenderung memanfaatkan tren fitur-fitur gratis namun tidak menyadari, jika tidak ingin disebut mengabaikan, bahwa di balik itu ada konsekuensi pengumpulan data pribadi yang harus diterima.

5.3.2. Isu Privasi dan Pelindungan Data Pribadi Masih Eksklusif Pada Kelas Sosial Menengah

Jumlah pengguna internet Indonesia menyentuh 197 juta orang atau berkisar 73,7 persen dari total seluruh populasi, menurut temuan Asosiasi Penyedia Jasa Internet Indonesia (APJII).[369] Meski angka penggunanya terbilang tinggi, literasi perihal isu tentang privasi data pribadi relatif terbatas dipahami oleh masyarakat kelas menengah ke atas. Survei Literasi Digital yang dibuat Katadata menemukan fakta bahwa indeks literasi digital berkorelasi positif pada latar belakang pendidikan, pekerjaan, serta usia penggunanya.[370] Survei itu dilakukan terhadap 56 persen responden yang berasal dari wilayah rural Indonesia dan sisanya berlatar belakang kaum urban, dengan tingkat penghasilan mayoritas Rp 2-4 Juta per bulan.[371]

Dari temuan ini, jika dikaitkan dengan fenomena literasi keamanan data pribadi, dapat diambil beberapa hal yang patut direfleksikan bahwa: (1) efek digitalisasi terjadi secara berantai di mana pengguna dari kelas sosial menengah ke bawah cenderung mengikuti tren yang sebelumnya telah berkembang di kelas sosial di atasnya; (2) motivasi penggunaan platform mayoritas dominan didasari karena tren yang sedang berkembang; (3) pengguna platform relatif tidak menempatkan risiko pemanfaatan data sebagai pertimbangan awal ketika mendaftar atau mengunduh suatu aplikasi. Oleh karena itu, pengarusutamaan budaya sadar risiko digital ke seluruh lapisan masyarakat menjadi penting agar proteksi privasi bisa ditingkatkan dan membangun kesadaran inklusif.

5.4. Kerentanan Masyarakat Atas Bias Algoritma

Melalui FGD yang dilakukan bersama kelompok masyarakat pengguna aplikasi digital seperti buruh (manual), pengemudi online, pemerhati persoalan data pribadi dan mahasiswa, selain mendapatkan masukan terkait persoalan data pribadi, melalui diskusi juga memberikan temuan adanya bias algoritma yang mengganggu dan meresahkan para

---

[368] Tulus Abadi, dalam pemaparannya pada seminar daring 'Peluang dan Tantangan Hukum Bisnis terhadap Perubahan Era Digital: *Quo Vadis* Perlindungan Konsumen di Indonesia tanggal 26 Juni 2021.

[369] Leo Dwi Jatmiko, "APJII: 196,7 Juta Warga Indonesia Sudah Melek Internet", *bisnis.com*, (10 November 2020), diakses dari https://bit.ly/3dlAZvA.

[370] Katadata & Ditjen APTIKA, "Survei Literasi Digital…, hlm. 20.

[371] *Ibid.*, hlm. 21.

pengguna aplikasi atau platform. Berdasarkan pengalaman mereka pada bidang dan aktivitas mereka masing-masing diketahui adanya bias algoritma yang merugikan mereka.

Oleh para pengemudi online ditemukan beberapa persoalan seperti: sistem memberikan keuntungan terhadap pengemudi tertentu, adanya sistem yang mendiskriminasi pengemudi tertentu apabila melakukan tindakan yang tidak sesuai prosedur tanpa melakukan verifikasi, adanya sistem yang mengutamakan pengemudi tertentu apabila membayar sejumlah uang dan lainnya. Terdapat juga fakta bahwa sistem aplikasi dapat diretas (hacking) dan digunakan oleh sekelompok orang yang di dalamnya melibatkan para programer. Persoalan serupa terkait bias algoritma yang digunakan pada aplikasi juga terjadi pada pekerjaan yang menggunakan aplikasi maupun sistem keputusan yang dilakukan secara otomatis pada program secara digital.

Persoalan bias algoritma ini memiliki spektrum yang luas tidak saja terhadap pekerja pengguna aplikasi tetapi kepada pihak mana saja yang menggunakan atau mendapatkan keputusan-keputusan yang dilakukan berdasarkan algoritma dalam sebuah pemrograman. Persoalan ini disadari kemudian menjadi persoalan yang luas dan sangat berdampak kepada masyarakat umum dan bila tidak mendapatkan respons yang kuat berpotensi menjadi persoalan dalam waktu yang panjang. Keterbatasan waktu penelitian dan ruang lingkup yang telah disepakati pada akhirnya memberikan keterbatasan melakukan tinjauan terhadap persoalan ini lebih mendalam. Tetapi mengingat pentingnya persoalan ini, terlebih terkait dengan salah satu tujuan penelitian ini yaitu mengetahui sejauh mana perundangan telah melindungi hak-hak masyarakat dari dampak akibat aturan liberalisasi perdagangan digital maka perlu disebutkan setidaknya dalam laporan ini sebagai sebuah perhatian yang penting.

Data atau identitas seseorang merupakan persoalan sentral dalam dunia digital. Hal itu menyebabkan persoalan bias algoritma terlihat seperti sebuah persoalan terpisah, tetapi bila dilihat dari sebuah pemrosesan data, maka sesungguhnya keputusan-keputusan yang dilakukan pada sebuah algoritma tentunya berkaitan dengan karakter atau keunikan sebuah data, dimana hal tersebut terkait dengan adanya data pengguna atau pribadi didalamnya. Persoalannya adalah keputusan yang dilakukan secara otomatis melalui algoritma tertentu tidak memiliki jaminan fairnes dan kelayakan atau konfirmasi kepada pengguna aplikasi atau mereka yang terdampak dari keputusan atau penilaian yang diambil. Hal ini menunjukan bahwa terkait bias algoritma ini masyarakat secara luas berada pada posisi yang rentan mendapatkan perlakuan tidak adil.

Beberapa poin penting yang dicatat dalam FGD dapat disebutkan sebagai berikut:

1) Algoritma bersifat sangat penting strategis karena berdampak kepada kelompok buruh, UMKM dan masyarakat secara umum.
2) Fakta menunjukan terdapat bias algoritma pada program atau aplikasi yang dipakai selama ini.
3) Dibutuhkan keterbukaan terkait algoritma yang digunakan pada sebuah program atau aplikasi.
4) Perlu adanya kepastian bahwa algoritma yang digunakan harus sesuai (*comply*) dengan peraturan yang melindungi melindungi masyarakat dan nilai-nilai yang berkembang.
5) Dibutuhkan adanya lembaga atau institusi yang bersifat independen dan dipercaya untuk mengawasi atau menilai terkait hal ini.

6) Algoritma dan persoalan terkait pemrograman lainnya terlindungi oleh aturan WTO terkait IPR dan rahasia dagang sehingga tidak dapat atau sulit dilakukan intervensi atau perubahan.

Pengamatan ringkas yang dilakukan sejauh ini belum ditemukan adanya aturan secara langsung dan tegas mengatur persoalan terkait bias algoritma di Indonesia. Perlindungan yang bisa dilakukan masih sejauh terlihat yaitu apabila hal-hal tersebut melanggar aturan-aturan yang berlaku seperti UU ITE dan UU HAM serta peraturan lain terkait aturan perdagangan seperti persaingan dagang yang sehat serta perundangan lainnya yang dimungkinkan. Pengamatan ringkas juga memperlihatkan belum adanya tuntutan atau gugatan ke ranah hukum terkait persoalan bias algoritma di Indonesia. Peraturan Pemerintah PP PTE pasal 13 (lihat halaman 60 laporan ini) mengatur terkait pemrosesan data tetapi lebih fokus pada pemrosesan data pribadi. Pasal 9 PP PTE menyebutkan pada penggunaan untuk publik, penyelenggarann sistem elektronik wajib menyerahkan source code kepada instansi terkait.

Persoalan lain yang juga penting adalah terkait adanya sebuah lembaga, khususnya untuk tingkat nasional, yang melakukan pemantauan atau pengawasan terkait bias algoritma ini. Dapat dipastikan belum adanya lembaga atau institusi di Indonesia yang secara resmi atau legal maupun berdasarkan kapasitasnya melakukan pengujian terhadap kemungkinan adanya bias dalam aplikasi atau platform yang ada selama ini. Karena persoalan ini terkait dengan pengetahuan dan kemampuan yang sangat spesifik sehingga di kebutuhan akan adanya lembaga tersebut dirasakan menjadi kebutuhan penting bagi kepentingan masyarakat.

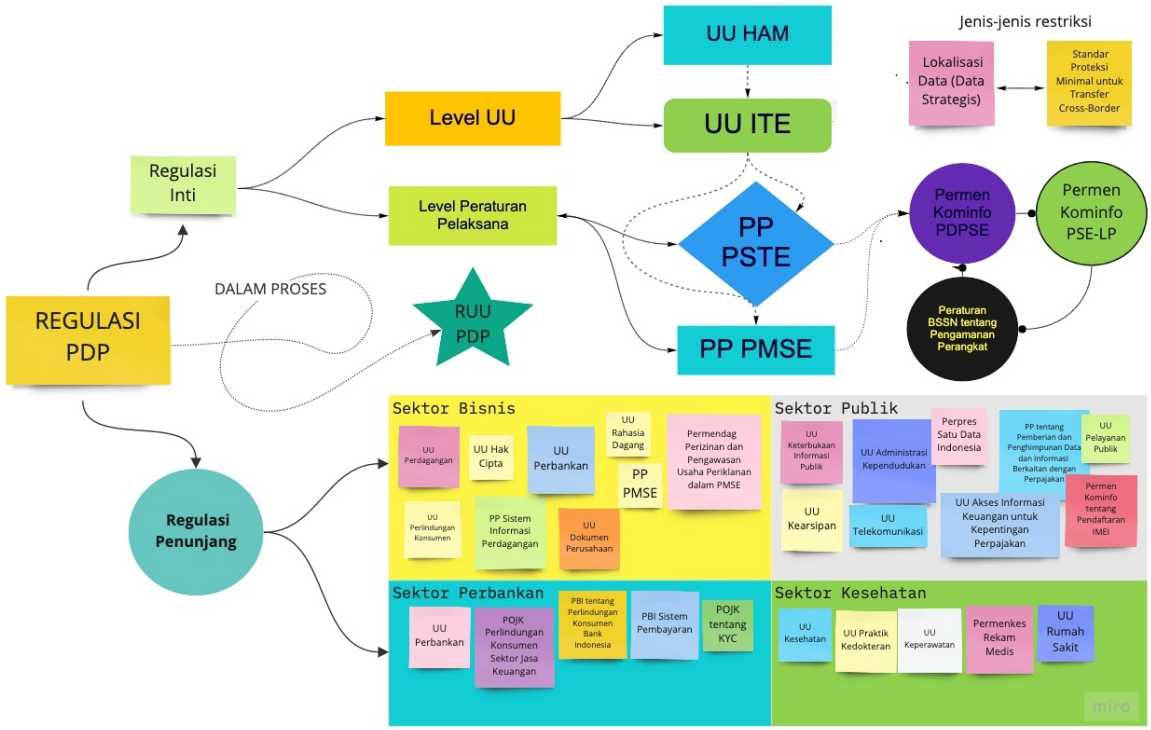
Pada kondisi yang seperti ini, aturan terkait source code atau algoritma ini dilindungi oleh aturan WTO terkait aturan perlindungan terhadap IPR (*Intellectual Property Right*) dan aturan perlindungan atas kerahasiaan barang perdagangan. Pada RCEP persoalan terkait *source code* belum memiliki aturan secara khusus dan persoalan ini hanya dimasukan sebagai salah satu topik yang dirasakan penting dalam dialog yang harus dilakukan antara negara seperti yang disebutkan pada *Article 12.16: Dialogue on Electronic Commerce*. Hal ini menunjukkan bahwa FTA dan aturan WTO yang sangat terbuka pada liberalisasi perdagangan yang meluas pada persoalan lain pada soal-soal non perdagangan memiliki celah yang berdampak sangat luas dan buruk terhadap aktivitas ekonomi dan persoalan kehidupan masyarakat global. Terhadap aturan yang berlaku nasional terdapat kontradiksi dimana desakan WTO dan FTA terhadap liberalisasi untuk memberikan ruang seluas mungkin kepada pemilik aplikasi tetapi perundangan Indonesia seperti ditunjukan pada PP PSE berupaya melakukan perlindungan terhadap masyarakat. Kontradiksi ini akan terjadi pada perundingan-perundingan FTA yang terus berlangsung.

BAB 6
PENUTUP

6.1. Kesimpulan

Hasil temuan dan pemetaan regulasi yang dilakukan menunjukan bahwa sebenarnya Indonesia tidak kekurangan regulasi tentang pelindungan data pribadi. Bahkan, beberapa di antara ketentuan yang tersebar acak itu telah mengatur dengan standar yang kurang lebih mirip dengan praktik bisnis yang berkembang. Dalam kategori regulasi inti, setidaknya ada dua rujukan peraturan perundang-undangan utama, yakni Undang-Undang Hak Asasi Manusia (UU HAM) dan UU Informasi dan Transaksi Elektronik (UU ITE) yang memberi landasan perlindungan privasi data. Sementara pada tingkat peraturan pelaksana terdapat beberapa peraturan perundang-undangan yang menunjang kerangka regulasinya, diantaranya Peraturan Pemerintah tentang Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE), PP Perdagangan Melalui Sistem Elektronik (PP PMSE), Peraturan Menteri Kominfo tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permen Kominfo PDP SE), Permen Kominfo tentang Penyelenggara Sistem Elektronik Lingkup Privat, hingga Peraturan BSSN tentang Pengamanan Perangkat. Begitu pula dalam kategori regulasi penunjang, baik dari sektor bisnis, perbankan, publik, kesehatan, dan seterusnya, terdapat setidaknya lebih dari lima peraturan perundang-undangan di masing-masing sektor.

Gambar 6.1. Peta Regulasi PDP



Akan tetapi, banyaknya aturan yang tersedia tidak lantas memberi jaminan akan pelindungan yang optimal mengingat problemnya lebih banyak terletak pada dimensi

struktur, di samping substansi dan kultur. Banyaknya aturan ini menimbulkan suatu kebutuhan untuk mensimplifikasikannya ke dalam satu produk undang-undang serupa RUU Pelindungan Data Pribadi (RUU PDP). Tapi, sebelum lantas beranjak ke RUU PDP sebagai solusi, regulator harus juga menjelaskan kepada publik mengapa keberadaan setumpuk regulasi yang telah ada justru gagal mencegah terulangnya kasus kebocoran data pribadi, termasuk yang terjadi di instansi pemerintah. Tanpa penanganan yang sungguh-sungguh, kasus-kasus tersebut akan bermuara pada lebih banyak lagi kasus pelanggaran privasi data digital yang menyimpan potensi kerugian sangat besar bagi publik.

Secara umum, tingkat proteksi RUU PDP bisa dibilang lebih baik dari produk perundang-undangan yang ada saat ini karena mengatur secara spesifik perlakuan dan perlindungan apa saja yang harus dipatuhi dalam konteks pemrosesan data. Catatan penting yang harus diperhatikan adalah terkait penunjukan fungsi otoritas pelindungan data pribadi yang pada draf terakhir belum tercakup. Juga, perihal penggunaan sanksi pidana yang sebenarnya tidak ideal diadopsi dalam regulasi bersifat administrasi seperti RUU PDP. Alih-alih hukuman pidana penjara, semestinya luaran akhirnya berupa denda (dengan proporsi persentase pendapatan tahunan) agar memiliki efek kendali pada mayoritas penyedia platform yang merupakan perusahaan.

Persoalan lain yang juga mengemuka dalam FGD adalah persoalan terkait bias algoritma yang telah meresahkan para penggguna baik pekerja maupun para pelaku UMKM serta masyarakat secara umum yang terkena dari dampak keputusan-keputusan yang diambil secara otomatis melalui aplikasi atau pemgrograman. Dampak yang telah terasa dan semakin meluas pada masyarakat ini sangat berpeluang akan terus berkembang dan meluas serta menjadi persoalan yang panjang di masa depan. Kebutuhan akan pengaturan yang pasti dan ketat perlu dilakukan terkait hal ini. Mengingat persoalan ini bersifat sangat teknis dan spesifik maka kebutuhan akan adanya lembaga atau institusi dengan kemampuan yang baik menjadi kebutuhan di masa depan sehingga perlu mendapatkan pengaturan soal hal tersebut.

6.2. Saran

Mengawal dan memantau perkembangan RUU PDP penting dilakukan, namun yang lebih krusial adalah memastikan bagaimana pasca pembahasan dan pengesahannya nanti, substansinya bisa dipahami, dipatuhi dan diimplementasikan. Selain itu, tanpa diiringi literasi dan kesadaran akan keamanan digital yang mumpuni, RUU PDP sangat mungkin akan berakhir tak ubahnya UU ITE. Karena itu, sosialisasi dan pengarusutamaan literasi digital perlu dilakukan dari bawah ke atas, bukan sebaliknya. Terakhir, pemangku kebijakan diharapkan dapat menampung banyak catatan penting, terutama pada Bab 4 dan 5 untuk jadi pertimbangan dalam kebijakan pelindungan data pribadi.

Terkait dengan persoalan bias algoritma yang akan menjadi persoalan berdampak luas pada masa depan dimana akan menjadi pertarungan antara masyarakat dan pengusaha dan investor perangkat lunak, mkaa kajian atau penelitian lebih mendalam terhadap hal ini perlu dilakukan khususnya dalam mencari solusi-solusi alternatif bagi kepentingan masyarakat secara global.

BIBLIOGRAFI

'What is Data Minimisation?'. *Experian.co.uk*. Diakses dari https://www.experian.co.uk /business/glossary/data-minimisation/.

Anur, C. M. (2 Agustus 2019). "Pelanggaran Data Pribadi di Indonesia Diperdagangkan Hingga Ancaman". *Katadata.co.id*. Diakses dari https://bit.ly/34XOc9w.

APEC. (n.d.). "Cross-Border Privacy Rules System: Policies, Rules, and Guidelines". Diunduh dari https://bit.ly/3x3OFmz.

Arditya, A. Nugraha, I. R. (29 Januari 2021). "RUU PDP RUU PDP masih memiliki banyak kekurangan dibandingkan standar internasional dalam melindungi data pribadi". *Theconversation.com*. Diakses dari https://bit.ly/3v83EdL.

ASEAN. (2020). 'Summary of the Regional Comprehensive Economic Partnership Agreement'. *Asean.org*. Diakses dari https://asean.org/storage/2020/11/Summary-of-the-RCEP-Agreement.pdf

Autoriteit Persoonsgegevens. (n.d.). "Organization". *Autoriteitpersoonsgegevens.nl*. Diakses dari https://bit.ly/3qglM4n.

Aziz, M. F. (9 Mei 2020). "Pelindungan Data/Informasi Pribadi di Masa Pandemi Covid-19". Presentasi untuk webinar #ngoPI Vol. 2 PPI Scania Swedia dan PSHK.

Badan Pusat Statistik RI. (n.d.). "Tentang BPS: Tugas, Fungsi dan Kewenangan". *Bps.go.id*. Tautan: https://bit.ly/3w5j0B7.

Bernal, P. 2014. *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge: Cambridge University Press.

Besari, N. P. (24 Mei 2021). "Sistem Tak Siap, Pendaftaran Aplikasi ke Kominfo Diundur". *Cnbcindonesia.com*. Diakses dari https://bit.ly/3qEmo49.

Blandina Lintang, dalam paparannya pada *Focus Group Discussion* IGJ-PSHK tanggal 19 Juni 2021.

Borgesius, F. (2020). "Strenghtening legal protection against discrimination by algorithms and artificial intelegence". *The International Journal of Human Rights.* 24(10): 1572-1593. DOI:10.1080/13642987.2020.1743976

Boyne, S. M. (2020). "Data Protection in the United States: U.S. National Report". Vincente, D. M. Casimiro, S. de V (Eds). *Data Protection in the Internet.* Ius Comparatum Global Studies in Comparative Law Volume 38. Cham Switzerland: Springer Nature.

Briantika, A. (15 Agustus 2019). "Polisi Tangkap Penjual Data Nasabah dan Kependudukan". *Tirto.id*. Diakses dari https://bit.ly/34XCvQ4.

Brown, R. (2006). "Rethinking Privacy: Exclusivity, Private Relation and Tort Law". *Alberta Law Review.* 43(3): 589-614.

BSSN. (3 Februari 2021). 'Raker dengan Komisi I DPR RI, BSSN: SNKS RI sebagai Langkah Nyata Kehadiran Negara di Ruang Siber'. *Bssn.go.id*. Diakses dari https://bit.ly/2SKppTi.

Budi Hartadi dari Pusilkom Fakultas Ilmu Komputer Universitas Indonesia, dalam wawancara tanggal 21 Juni 2021.

Budiman, A. (Februari 2021). "Otoritas Pengawas Perlindungan Data Pribadi". *Info Singkat: Bidang Politik dalam Negeri.* Vol. XIII, No.5/I/Puslit/Februari/2021. Jakarta: Badan Keahlian DPR RI. Diakses dari https://bit.ly/3wQNaIQ.

Burhan, F. A. (16 April 2021). "AS Resmi Sebut Goolge-Facebook Monopoli, Mulai Kaji Aturan Baru". *Katadata.co.id*. Diakses dari https://bit.ly/3pLx1BE.

Burkhardt, B. (14 April 2021). 'China: Protection of Personal Information – Moving Closer to a Chinese GDPR?'. *Lexology.com.* Diakses dari https://bit.ly/3yPugDg.

Chabinsky, S. Wittman, F. P. (2020). “USA: Data Protection Laws and Regulation 2020”. Iclg.com. London: International Comparative Law Guides. Diakses dari https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
CNN Indonesia. (1 Oktober 2019). “Indonesia Jadi Salah Satu Negara Target Phishing’. *Cnnindonesia.com*. Diakses dari https://bit.ly/350GfAf.
CNN Indonesia. (3 Mei 2020). “Penelusuran 91 Juta Data Bocor Tokopedia, Dijual Rp74 Juta”. *Cnnindonesia.com*. Diakses dari https://bit.ly/3w72Wi2.
CNN Indonesia. (7 November 2019). “Poin-poin yang dianggap ancam kedaulatan RI di PP PSTE”. *Cnnindonesia.com*. Diakses dari https://bit.ly/35I7T5H.
CNN Indonesia. (9 Oktober 2019). “Riset Pengguna Internet Rela Bagi Data Pribadi Demi Gratisan”. *Cnnindonesia.com.* Diakses dari https://bit.ly/2RNbeNe.
Commissioner of Canada. (May 2019). ‘PIPEDA Fair Information Principles’. Priv.gc.ca. Diakses dari https://bit.ly/3q3KJ2E.
Council of Europe. (June 2018). *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. Diunduh dari https://bit.ly/3g52sU7.
Criado, N. Such, J. M. 2019. “Digital Discrimination”. Karen Yeung (Ed) & Martin Lodge (Ed). *Algorithmic Regulation.* Oxford: Oxford University Press.
D’Souza, Craig. (15 Januari 2019). ‘Big Data and Trade Secrets (A General Analysis)’. Diakses dari https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316328
Data Guidance. (November 2019). ‘International: US-EU cross-border data transfers’. *Dataguidance.com*. Diakses dari https://bit.ly/2U7sZYi.
DBS Website. (n.d.).‘How Website Cookies Affect Your Data Privacy’. *Dbswebsite.com*. Diakses dari https://www.dbswebsite.com/blog/website-cookies-and-data-privacy/
Dina, S. (9 Januari 2018). “Tumpang Tindih Tugas Badan Siber dengan Lembaga Lain”. *Kominfo.go.id.* Diakses dari https://bit.ly/2RCjPCs.
Dirjen Aptika Kominfo. (5 November 2020). “UU PDP Akan Permudah Pertukaran Data dengan Negara Lain”. *Aptika.kominfo.go.id*. Diakses dari https://aptika.kominfo.go.id/2020/11/uu-pdp-akan-permudah-pertukaran-data-dengan-negara-lain/
Djafar, W. “Hukum Perlindungan Data Pribadi di Indonesia”. Makalah untuk materi kuliah umum Tantangan Hukum dalam Era Analisis Big Data. 26 Agustus 2019. Yogyakarta: Universitas Gadjah Mada Yogyakarta.
Djafar, W. Dkk. 2016. *Pelindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia.* Seri Internat dan HAM. Jakarta: ELSAM.
Edelman, B G. & Luca, M. (January 2014). “Digital Discrimination: The Case of Airbnb.com”. *Harvard Business School NOM Unit Working Paper No. 14-054*. DOI: http://dx.doi.org/10.2139/ssrn.2377353.
ELSAM. (2 Agustus 2019). ‘Kemendagri harus tinjau ulang Kerjasama Pemberian Akses Data Kependudukan’. *Elsam.or.id*. Diakses dari https://bit.ly/35WQrKx.
ELSAM. (22 juli 2019). “Kerentanan Perlindungan Data Pribadi dalam Pengelolaan Data Kependudukan”. *Elsam.or.id*. Diakses dari https://bit.ly/3gXb1AU.
ELSAM. (8 Juli 2020). “Perlindungan Data Pribadi: Perlunya Otoritas Pengawasan Independen”. *Elsam.or.id*. Diakses dari https://bit.ly/3xuYYjQ.
Federal Trade Commission. (2021). “CAN-SPAM ACT: A Compliance Guide for Business”. *Ftc.gov*. Diakses dari https://www.ftc.gov/tips-advice/business-center/guidance/ can-spam-act-compliance-guide-business
Fefer, R. F. (26 Maret 2020). ‘Data Flows, Online Privacy, and Trade Policy’. Laporan untuk Congressional Research Service. Diakses dari https://fas.org/sgp/crs/misc/R45584.pdf.

Fertian, W. (14 Juli 2016). “Perbedaan Data dan Informasi”. *Binus.ac.id*. Diakses dari https://bit.ly/342zKfQ
Fioramonti, L. Soerjadinata, L (trans). 2017. *Problem Domestik Bruto: Sejarah dan Realitas Politik di Balik Angka Pertumbuhan Ekonomi.* Jakarta: Marjin Kiri Publisher.
Forgo, Nikolaus. Hanold, S & Schutze, B. 2017. “The Principle of Purpose Limitation". In Coralles, M. (Ed). Et. al. *New Technology, Big Data and the Law.* Springer Verlag.
Friedman, L. M. 2001. *Hukum Amerika: Sebuah Pengantar, Terjemahan dari American Law: An Introduction*. 2nd Edition. Wisnu Basuki (trans). Jakarta: Tatanusa.
Greze, B. (May 2019). ‘The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives’. *International Data Privacy Law.* 9(2): 109–128.
Harari, Y. N. (Mei 2017). ‘Dataism is Our New God’. *New Perspective Quarterly.* 34(2): 34-43. DOI: 10.1111/npqu.12080.
Harari, Y. N. 2016. ‘Data Religion’. *Homo Deus: A Brief History of Tomorrow*. London: Vintage.
Hasbullah, F. H. 2005. *Hukum Kebendaan Perdata: Hak-Hak yang Memberi Kenikmatan, Jilid 1.* Jakarta: Ind-Hill Co.
Hukum Online. (n.d.). ‘RUU Perlindungan Data Pribadi Tahun 2020’. *Hukumonline.com*. Diakses dari https://bit.ly/3qtAViJ.
Human Rights Watch. (21 Mei 2016). “Indonesia: Tangguhkan dan Revisi Permenkominfo No. 5 Tahun 2020”. *Hrw.org*. Diakses dari https://www.hrw.org/id/news/2021/05/21/378764
Human Rights Watch. (6 Juni 2018). ‘Peraturan Pelindungan Data Umum Uni Eropa’. *Hrw.org*. Diakses dari https://www.hrw.org/id/news/2018/06/06/318734
Ikram, Nemo. (9 Juni 2019). “Indonesia Dukung Data Free-Flow, Bagaimana Keamanannya”. *Cyberthreat.id*. Diakses dari https://bit.ly/3xy7kY1.
Iksan, M. F. Dkk, (June 2020). ‘Impact of digital economic liberalization and capitalization in the era of industrial revolution 4.0: case study in Indonesia’. *Problems and Perspectives in Management*. 18(2): 290-301. Doi:10.21511/ppm.18(2).2020.24
Indonesia for Global Justice. (6 Maret 2021). “Perlu Kebijakan Konsisten dalam Menghadapi Era Keterbukaan Platform Digital. *Igj.or.id.* Diakses dari https://bit.ly/3iw9yCK.
Indonesia, *Peraturan Menteri Kesehatan tentang Rekam Medis*, Permenkes No. 269/Menkes/Per/III/2008.
Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik*, Permen Kominfo Nomor 20 Tahun 2016, Berita Negara Nomor 1829.
Indonesia, *Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik*, PP Nomor 80 Tahun 2019, LN Nomor 222 Tahun 2019, TLN Nomor 6420.
Indonesia, *Undang-Undang tentang Keperawatan*, UU No. 36 Tahun 2014, LN Nomor 298 Tahun 2014, TLN Nomor 5607.
Indonesia, *Undang-Undang tentang Kesehatan*, UU No. 36 Tahun 2009, LN Nomor 114 Tahun 2019, TLN Nomor 5063.
Indonesia, *Undang-Undang tentang Pelayanan Publik*, UU No. 25 Tahun 2009. LN No. 112 Tahun 2009. TLN Nomor 5038.
Indonesia, *Undang-Undang tentang Praktik Kedokteran*, UU No. 29 Tahun 2004, LN Nomor 116 Tahun 2004, TLN Nomor 4431.
Indonesia, *Undang-Undang tentang Rumah Sakit,* UU No. 44 Tahun 2009, LN Nomor 153 Tahun 2009, TLN Nomor 5072.

Indonesia. *Peraturan Bank Indonesia tentang Pelindungan Konsumen Bank Indonesia*. PBI Nomor 22/20/PBI/2020, LN No. 299 Tahun 2020, TLN No. 6605, Pasal 30 (1).
Indonesia. *Peraturan Bank Indonesia tentang Sistem Pembayaran.* PBI No. 22/23/2020, LN No. 311 Tahun 2020. TLN No. 6610.
Indonesia. *Peraturan Menteri Komunikasi dan Informatika tentang Pengendalian Alat dan/atau Perangkat yang Tersambung ke Jaringan Bergerak Seluler Melalui Identifikasi IMEI*. Permenkominfo No. 11 Tahun 2019, Berita Negara Nomor 1238 Nomor 2019.
Indonesia. *Peraturan Menteri Perdagangan tentang Perizinan Usaha Periklanan, Pembinaan dan Pengawasan Pelaku Usaha dalam PMSE*. Permendag No. 50 Tahun 2020. LN No. 498 Tahun 2020.
Indonesia. *Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen Sektor Jasa Keuangan*. POJK No. 1/POJK.7/2013. LN No. 118 Tahun 2013, TLN No. 5431.
Indonesia. *Peraturan Pemerintah Pengganti Undang-Undang tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan*, Perppu Nomor 1 Tahun 2017. LN No. 95 Tahun 2017. TLN No. 6051.
Indonesia. *Peraturan Pemerintah tentang Pemberian dan Penghimpunan Data dan Informasi yang Berkaitan dengan Perpajakan*. PP No. 31 Tahun 2012. LN No. 56 Tahun 2012. TLN No. 5289.
Indonesia. *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP Nomor 71 Tahun 2019, LN Nomor 185 Tahun 2019, TLN Nomor 6400.
Indonesia. *Peraturan Pemerintah tentang Sistem Informasi Perdagangan, PP No. 5 Tahun 2020*. LN No. 9 Tahun 2020. TLN No. 6458.
Indonesia. *Peraturan Pemerintah tentang Transaksi Perdagangan Melalui Sistem Elektronik*. PP No. 80 Tahun 2019. LN No. 222 Tahun 2019, TLN No. 6420.
Indonesia. *Peraturan Presiden tentang Satu Data Indonesia,* Perpres Nomor 39 Tahun 2019. LN No. 112 Tahun 2019.
Indonesia. Subekti, R. Tjitrosudibio, R (trans). 2009. *Kitab Undang-Undang Hukum Perdata (KUHPerdata).* Jakarta: Pradnya Paramita.
Indonesia. *Undang-Undang Dasar 1945*. Amandemen Ke-II.
Indonesia. *Undang-Undang tentang Dokumen Perusahaan*. UU No. 8 Tahun 1997. LN No. 18 Tahun 1997. TLN No. 3674.
Indonesia. *Undang-Undang tentang Hak Asasi Manusia*, UU Nomor 39 Tahun 1999, LN Nomor 165 Tahun 1999, TLN Nomor 3886.
Indonesia. *Undang-Undang tentang Hak Cipta*. UU No. 19 Tahun 2002. LN No. 85 Tahun 2002.
Indonesia. *Undang-Undang tentang Kearsipan*. UU No. 43 Tahun 2009, LN No. 152 Tahun 2009, TLN No. 5071.
Indonesia. *Undang-Undang tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008. LN No. 61 Tahun 2008. TLN No. 4846.
Indonesia. *Undang-Undang tentang Keterbukaan Informasi Publik*. UU No. 14 Tahun 2008. LN No. 61 Tahun 2008. TLN No. 4846.
Indonesia. *Undang-Undang tentang Penetapan Peraturan Pemerintah Nomor 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan*. UU No. 9 Tahun 2017. LN No. 190 Tahun 2017. TLN No. 6112.
Indonesia. *Undang-Undang tentang Perdagangan*. UU No. 7 Tahun 2014. LN No. 45 Tahun 2014. TLN No. 5512.
Indonesia. *Undang-Undang tentang Perlindungan Konsumen*. UU No. 8 Tahun 1999. LN No. 22 Tahun 1999. TLN No. 3821.

Indonesia. *Undang-Undang tentang Perubahan atas Undang-Undang Perbankan*, UU No. 10 Tahun 1998. LN No. 182 Tahun 1998. TLN No. 3790.
Indonesia. *Undang-Undang tentang Perubahan atas UU Administrasi Kependudukan*. UU No. 24 Tahun 2013. LN No. 232 Tahun 2013. TLN No. 5475.
Indonesia. *Undang-Undang tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, UU No. 19 Tahun 2016, LN Nomor 251 Tahun 2016, TLN Nomor
Indonesia. *Undang-Undang tentang Telekomunikasi.* UU No. 36 Tahun 1999. LN No. 154 Tahun 1999. TLN No. 3881.
Jatmiko, L. D. (10 November 2020). "APJII: 196,7 Juta Warga Indonesia Sudah Melek Internet". *Bisnis.com*. Diakses dari https://bit.ly/3dlAZvA.
Katadata. (13 Juni 2017). "Berapa Nilai Pasar Big Data di Indonesia?". *Katadata.co.id*. Diakses dari https://bit.ly/3g3WNxH.
Kementerian Komunikasi dan Informasi. (17 Mei 2019). "Pernyataan BRTI Mengenai Praktik Jual Beli Data Pribadi". Siaran Pers untuk *kominfo.go.id*. Diakses dari https://bit.ly/3xZOeKz.
Kementerian Komunikasi dan Informatika. (n.d.). "Tugas dan fungsi". *Kominfo.go.id*. Diakses dari https://www.kominfo.go.id/tugas-dan-fungsi.
Kementerian Komunikasi dan Informatika. (November 2020). "Status Literasi Digital Indonesia: Survei di 34 Provinsi". Jakarta: Kominfo & Katadata.
Kemp, S. (18 February 2020). 'Digital 2020: Indonesia'. *Datareportal.com*. Diakses dari https://datareportal.com/reports/digital-2020-indonesia.
Kominfo. (30 Juli 2020). "5 Proposisi Indonesia soal Keamanan Data di Pertemuan G20". *kominfo.go.id*. Diakses dari https://bit.ly/35xl9Kd.
Komisi Informasi. (25 Januari 2021). "Anggota DPR RI Mendukung Lembaga Pelindungan Data Pribadi Digabung ke Komisi Informasi". *Komisiinformasi.go.id*. Diakses dari https://bit.ly/3wCbcqx.
Kompas. (13 Mei 2019). "Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial". *Harian Kompas*. Dimuat juga secara daring di https://bit.ly/3v4lAWP.
Kompas. (9 Juni 2020). "Sanksi Pidana dalam RUU PDP Diminta Dihapus". *Kompas.com*, Diakses dari https://bit.ly/2SfTbzv.
Kontan. (14 Juni 2020). "Ada Lebih dari 1300 Instansi dan Lembaga yang Bisa Akses Data Kependudukan". *Kontan.co.id*. Diakses dari https://bit.ly/3xYwKxW.
Kontan. (26 November 2018). "Asosiasi Game: Kewajiban Data Center di Indonesia Sulit Diterapkan". *Kontan.co.id*. Diakses dari https://bit.ly/3gIpxei.
Kumparan. (28 Juni 2018). "Waspada Aplikasi Pinjam Uang Ambil Data Kontak dan Baca SMS di Ponsel". *Kumparan.com*. Diakses dari https://bit.ly/2RGB4mc.
Kurniawan, F. Marzuki, P. M. dkk. (Januari 2018). 'Unsur Kerugian dalam *Unjustified Enrichment* untuk Mewujudkan Keadilan Korektif'. *Yuridika.* 33(1): 19-39.
Lidwina, A. (17 Desember 2020). "Mengukur Monopoli Bisnis Digital Facebook dan Google". *Katadata.co.id*.
Lidwina, A. (29 Januari 2021). "Facebook, Medsos yang Kehilangan Kepercayaan Publik Tertinggi Persentase Hilangnya Kepercayaan Publik pada Perusahaan (2018)". *Katadata.co.id*. Diakses dari https://bit.ly/3ipwaF5.
Lynskey, O. 2016. *The foundations of EU data protection law.* Oxford: Oxford University Press.
Makarim, E. 2005. 'Kajian Aspek Hukum Perlindungan Data dan Hak Pribadi'. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian.* Depok: Badan Penerbit FHUI & Rajawali Pers.

Malgieri, G. (April 2019). 'Pricing Privacy – the right to know the value of your personal data'. *Computer Law & Security Review: The International Journal of Technology and Law Practice.* 34(2): 289-303.
McLean, G. (18 Maret 2019). "Algoritma bantu pelaku bisnis online untuk tetapkan harga yang tinggi". *Theconversation.com*. Diakses dari https://bit.ly/3g4PyWe.
Miller, H. (25 Mei 2021). "UK's Data Spying After Snowden Violated Privacy Rights". *Bloomberg.com*. Diakses dari https://bloom.bg/3ghnHkw.
Naskah Akademik (NA) RUU Perlindungan Data Pribadi.
Novika, S. (20 November 2020). "Marak Kasus Jual Beli Data Pribadi, Dijual Ke Mana?". *Detik.com*. Diakses dari https://bit.ly/3ze6Zvd.
O'Neil, C. 2016. *Weapon of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York: Crown Publisher.
Patrick, J. (5 November 2019). "PP PSTE Atur Data Digital Publik Wajib Disimpan di Indonesia". *Cnnindonesia.com*. Diakses dari https://bit.ly/3zxSdzC.
Prasongko, D. (15 Januari 2019). "Kemendagri dan Jasa Keuangan Teken Kerja Sama Manfaatkan NIK". *Tempo.co*. Diakses dari https://bit.ly/3jet5Ip.
Pratama, A. M. (9 Oktober 2020). 'Pengguna Internet Indonesia hingga Kuartal II 2020 Capai 196,7 Juta Orang'. *Kompas.com*.
Privacy International. (26 Mei 2021). "UK Mass Interception Laws Violate Human Rights and Fight Continues…". *Privacyinternational.org*. Diakses dari https://bit.ly/3w6kIS4.
Rahayu, Y. A. (13 Februari 2019). "OJK Telusuri Kejadian Sopir Taksi Bunuh Diri Akibat Pinjaman Online'. *Merdeka.com*. Diakses dari https://bit.ly/3cpjKcf.
Rizky, M. J. (17 Februari 2021). "Tantangan Penegakan Hukum Anti-Monopoli Era Ekonomi Digital". *Hukumonline.com*. Diakses dari https://bit.ly/35YhaGA.
Sandhy, O. P. (1 November 2019). "PP 71 Dinilai Tak Pro Industri Data Center Lokal". *Cyberthreat.id*. Diakses dari https://bit.ly/3h7SkJH.
Scassa, T. 2020. 'Data Protection and the Internet: Canada'. Vincente, D. M. Casimiro, S. de V (eds). *Data Protection in the Internet.* Ius Comparatum Global Studies in Comparative Law Volume 38. Cham Switzerland: Springer Nature.
Schenable, C. O. Elger, B. S. Shaw, D. (July 2018). 'The Cambridge Analytica affair and internet-mediated research". *Embo Reports.* 19(1). DOI:10.15252/embr.201846579
Stephanie, C. (1 Januari 2021). "7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020". *Kompas.com*. Diakses dari https://bit.ly/3x0jby5.
Subekti. 2005. *Hukum Perjanjian*. Cetakan ke-21. Jakarta: Penerbit Intermasa.
Sudibyo, A. 2019. *Jagat Digital: Pembebasan dan Penguasaan.* Jakarta: Kepustakaan Populer Gramedia, 2019.
Thomas, V. F. (12 Februari 2019). "Pinjaman Online Kembali "Makan Korban", OJK Diminta Tak Bungkam". *Tirto.id.* Diakses dari https://bit.ly/3x6ifYz.
Toh, A. (22 Juli 2020). 'Cross Border Trade and Regional Data Protection – An Operational Perspective'. Presentasi untuk Webinar Global Connect @SBF, "Cross-Border Trade & Data Flows". Singapura.
Tsanacas, D. (1985). 'The Transborder Data Flow in the New World Information Order: Privacy or Control', *Review of Social Economy.* 43(3): 357-370. Taylor and Francis Group. DOI: 10.1080/00346768500000037.
Tulus Abadi, dalam pemaparannya pada seminar daring 'Peluang dan Tantangan Hukum Bisnis terhadap Perubahan Era Digital: *Quo Vadis* Perlindungan Konsumen di Indonesia tanggal 26 Juni 2021.
UNCTAD. (n.d.). 'Data Protection and Privacy Legislation Worldwide'. *Unctad.org*. diakses dari https://bit.ly/3djvxt7.

UNCTAD. 2019. *Digital Economy Report 2019*. New York: United Nations. Diunduh dari https://bit.ly/3vXuWDV.
Voigt, P. Bussche, A. von dem. 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer International.
Warren, S. Brandeis, L. (Desember 1980). "The Right to Privacy". *Harvard Law Review*. 4(5): 193-220.
West, S. M. (2019). 'Data Capitalism: Redefining the Logics of Surveillance and Privacy'. *Business & Society*. 58(1): 20–41. DOI: 10.1177/0007650317718185
White, A. (21 Maret 2020). "How the Brussels Effect Helps the EU Rule the World". *Bloomberg.com*. Diakses dari https://bloom.bg/3zgoyun.

LAMPIRAN

1. Daftar Pertanyaan Pada FGD

Narasumber	Ekspektasi Pemaparan
Ahli IT	● Apakah data komoditas bisa diperdagangkan secara legal ? ● Apakah lokalisasi adalah kebijakan yang ideal dari perspektif pelaku IT, dalam kaitannya dengan perlindungan data pribadi? ● Apakah standar GDPR bisa diterapkan di sini melihat praktik ● pengelolaan data yang ada selama ini? ● Bagaimana Source Code itu di atur untuk mengantisipasi tindakan monopoli data terhadap perusahan digital ? ● Apakah aturan-aturan yang ada saat ini telah mendukung pelindungan privasi data sesuai siklus hidup informasi (Collection, Usage, Disclosure, Storage)?
Pegiat HAM	● Argumentasi ketiadaan RUU PDP seringkali diangkat ketika terjadi pelanggaran, tapi sebenarnya Indonesia telah memiliki aturan tersendiri. Apa yang menyebabkan regulasi saat ini (Permen Kominfo PDPSE, UU ITE, dst) tidak efektif melindungi data pribadi? ● RUU PDP: Apakah sudah sesuai dengan desain kebijakan pelindungan privasinya mengingat pada aturan *cross-border data flow* ada perbedaan komponen dengan GDPR? ● Apakah sebaiknya Indonesia terbuka pada *cross border data flow* atau tidak? Jika ya, bagaimana cara memastikan tidak ada pelanggaran privasi? ● Adakah catatan penting yang belum terakomodir di RUU PDP? ● Monopoli data untuk kepentingan periklanan: apakah perlu dibuat suatu aturan yang mengakomodir anti-monopoli? ● Apakah Data sudah menjadi komoditi yang bisa diperdagangkan secara legal? Sehubungan dengan aturan jual beli, perpajakan dll. Bagaimana pengaturan anti monopoli data? ● Problem di pelaksanaannya.
Pekerja Gojek/Grab	● Apakah ada gangguan yang terjadi dalam adaptasi teknologi di perusahaan anda ? ● Apakah ada transfer teknologi yang didapatkan ketika anda menjadi pekerja di perusahaan digital ? ● Bagaimana Teknologi digital mempengaruhi anda dalam mengambil keputusan di tempat kerja ? ● Bagaimana hubungan kerja dalam perusahaan yang menggunakan teknologi digital ?
Masyarakat/Mahasiswa	● Apakah anda mengetahui bagaimana melindungi data pribadi ? ● Apa yang kan dilakukan ketika data pribadi anda dipakai oleh orang/badan usaha tanpa diketahui oleh anda ?
Penanggap	Olisias Gultom - Peneliti IGJ Auditya Saputra – Peneliti PSHK