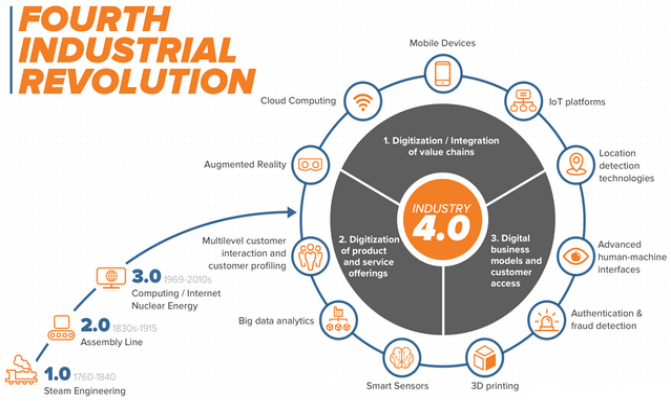
Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan[1]

Oleh: Wahyudi Djafar[2]

A. Pengantar: Revolusi Data dan Kebutuhan Perlindungan Data

Revolusi digital telah menciptakan sebuah inovasi baru dalam kapasitas untuk memperoleh, menyimpan, memanipulasi dan mentransmisikan volume data secara nyata (*real time*), luas dan kompleks. Oleh karenanya revolusi digital seringkali dianggap identik dengan revolusi data. Perkembangan tersebut telah mendorong pengumpulan berbagai data, tidak lagi tergantung pada pertimbangan data apa yang mungkin berguna di masa depan. Akan tetapi, hampir semua data dikumpulkan, pemerintah dan swasta bersaing untuk memperbesar kapasitas penyimpanan data mereka, dan semakin jarang melakukan penghapusan data. Mereka menemukan nilai baru dalam data, sehingga data diperlakukan seperti halnya aset yang berwujud. Era baru pengelolaan data inilah yang biasa disebut sebagai Big Data.[3]



Sumber: ICTWorks, 2019.

Prubahan dalam corak pengolahan data ini pula yang kerap disebut sebagai inti dari Revolusi Industri Keempat. Sebuah revolusi digital yang dicirikan dengan perpaduan teknologi yang mengaburkan garis antara bidang fisik, digital, dan biologis. Revolusi Industri Keempat sering digambarkan sebagai munculnya "*cyber-physical systems*", yang melibatkan kemampuan yang sepenuhnya baru bagi manusia dan mesin, terutama dalam hal kecepatan, cakupan, dan dampak sistem. Perkembangan ini telah memungkinkan lahirnya berbagai terobosan teknologi yang muncul di bidang-bidang seperti kecerdasan buatan (*artificial intelligence*), robotika, *Internet of Things*, kendaraan otomatis, pencetakan 3-D, nanoteknologi, bioteknologi, penyimpanan energi, dan komputasi kuantum.[4]

Big Data atau revoluasi data pada umumnya, sering dianggap sebagai substansi dari inovasi teknologi. Artinya konsep ini sebatas ditentukan oleh atribut atau unsurnya, yang terdiri dari data yang baru ditemukan dan daya komputasi yang super canggih. Memang, konsep Big Data sendiri datang tidak dengan definisi yang baku, yang disepakati semua ahli. Namun demikian secara umum disepakati bahwa Big Data berbeda dari analisis bisnis tradisional dan data skala kecil, yang jumlahnya banyak sekalipun. Akibatnya memang seringkali muncul kebimbangan dan kesalahpahaman dalam memahami Big Data ini, sebagai akibat keluasan definisinya. Bahkan pada titik tertentu definisi tersebut saling bertentangan satu sama lain.[5] Dari perspektif ilmu komputer, Big Data atau revoluasi data pada umumnya, sering dianggap semata-mata hanya sebagai substansi dari inovasi teknologi. Artinya konsep ini sebatas ditentukan oleh atribut atau unsurnya, yang terdiri dari data yang baru ditemukan dan daya komputasi yang super canggih. Hal ini seperti dikemukakan Manovich (2011) yang menyatakan, Big Data umumnya merujuk pada set data

---

[1] Makalah disampaikan sebagai materi dalam kuliah umum "Tantangan Hukum dalam Era Analisis Big Data", Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, Yogyakarta, 26 Agustus 2019.
[2] Deputi Direktur Riset Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta.
[3] Malik, P., 2013. Governing Big Data: Principles and practices. IBM Journal of Research and Develpoment 57, 1:1–1:13.
[4] Klaus Schwab, The Fourth Industrial Revolution, (Redfem: Currency Press, 2017). Lihat juga: Alec Ross, The Industries of the Futures, (New York: Simon & Schuster, 2017).
[5] Ward, J., & Barker, A. (2013). Undefined by Data: A Survey of Big Data Definitions.

(glanuralitas data) yang cukup besar, yang membutuhkan super komputer. Meski pada saat ini, proses tersebut cukup dianalisis melalui komputer desktop dengan menggunakan perangkat lunak standar.[6] Secara lugas dikatakan oleh Rob Kitchin (2014), bahwa Big Data adalah hasil dari pengembangan dan konvergensi berbagai kemajuan teknologi.[7]

Memang, dalam sebagian besar kasus, istilah 'Big Data' umumnya merujuk pada gabungan: volume, velocity, variety, veracity (4Vs)—sebuah konsep yang dikembangkan oleh Gartner (2012), dan kemudian sebagian besar konsep tersebut diambil oleh IBM.[8] Pendekatan data-sentris ini terutama menekankan pada besaran lonjakan data, peningkatan kecepatan, produksi data pada saat itu juga, serta keragaman format data yang diproses.[9] Faktanya, setiap detik, dunia menghasilkan lebih banyak data daripada yang disimpan 20 tahun yang lalu, semuanya dari kumpulan data yang berbeda, berbagai sumber dan beragam format, mulai dari audio, sinyal GPS, interaksi media sosial, dan berbagai macam jenis konten.[10]

Lebih jauh, Big Data biasa digunakan untuk menjelaskan penerapan teknik-teknik analisis untuk mencari, mengumpulkan dan merujukkan secara silang kumpulan-kumpulan data dalam jumlah besar untuk mengembangkan sistem kecerdasan dan wawasan. Kumpulan data yang berjumlah besar ini bisa didapatkan dari sumber-sumber umum, maupun kumpulan data pelanggan perusahaan tertentu. Big Data berangsur-angsur mencakup tidak hanya data yang bersifat umum, namun juga mencakup informasi yang dikumpulkan oleh sektor privat. Faktor itulah yang kemudian mendasari lahirnya definisi Big Data sebagai munculnya kumpulan data baru dengan volume besar yang berubah dengan cepat, sangat kompleks, dan melampaui jangkauan kemampuan analisis lingkungan perangkat keras dan perangkat lunak yang umum digunakan untuk pemrosesan data. Singkatnya, volume data menjadi terlalu besar untuk ditangani dengan alat dan metode konvensional.[11]

Namun demikian dalam penggunaan Big Data, ada sejumlah elemen fundamental yang harus diperhatikan, khususnya yang terkait dengan privasi dan perlindungan data pribadi. Hal ini khususnya mengacu pada banyaknya penggabungan dataset yang akan memudahkan identifikasi individu atau kelompok individu, yang berpotensi membahayakan pribadi orang tersebut. Oleh karena itu, langkah-langkah perlindungan data yang tepat harus dilakukan untuk mencegah penyalahgunaan atau kesalahan penanganan data. Tegasnya, bila peningkatan massif dalam pengumpulan data ini tidak dilakukan dalam kerangka penghormatan hak, maka mau tidak mau proses dan tujuannya akan digunakan dengan cara yang mengesampingkan hak-hak—privasi masyarakat.

B. Privasi dan Perlindungan Data Pribadi

Sebagai sebuah hak yang melekat pada diri pribadi, perdebatan mengenai pentingnya perlindungan terhadap hak atas privasi seseorang mula-mula mengemuka di dalam putusan-putusan pengadilan di Inggris dan kemudian di Amerika Serikat. Hingga kemudian Samuel Warren dan Louis Brandeis menuliskan konsepsi hukum hak atas privasi dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890. Tulisan dengan judul "*The Right to Privacy*" inilah yang pertama kali mengonseptualisasi hak atas privasi sebagai sebuah hak hukum.[12] Tulisan ini sendiri muncul ketika koran-koran mulai mencetak gambar orang untuk

---

[6] Manovich, L. (2011) 'Trending: the promises and the challenges of big social data', in Debates in the Digital Humanities, ed. M. K. Gold, The University of Minnesota Press, Minneapolis.

[7] Rob Kitchin, Big Data, New epistemologies and paradigm shifts, Big Data & Society April–June 2014: 1–12.

[8] Ward, J., & Barker, A., Op.Cit. Lihat juga: James R. KalyvasMichael R. Overly, Big Data A Businessand Legal Guide, (New York: CRC Press, 2015).

[9] Goes, Paulo, B,. (2014). "Big Data and IS Research", MIS Quarterly Vol. 38 No. 3 pp. iii-viii.

[10] Mcafee, A., & Brynjolfsson, E. (2012). Big Data: The management revolution. Harvard Business Review, 90(10), 60-6, 68, 128.

[11] Babak Akhgar, et.al. (eds.), Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies, (Oxford: Butterworth-Heinemann, 2015).

[12] Lihat: Samuel Warren dan Louis Brandeis, The Right to Privacy, dalam *Harvard Law Review* Vol. IV No. 5, 15 Desember 1890, tersedia di http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Gagasan dua orang pengacara Boston ini sebenarnya berangkat dari ide yang dicetuskan oleh hakim Thomas Cooley, yang menulis *Treatise on the Law of Torts* (1880), yang memperkenalkan pertama kali mengenai istilah 'hak untuk dibiarkan sendiri'.

pertama kalinya. Dalam tulisan tersebut Warren dan Brandeis secara sederhana mendefinisikan hak atas privasi sebagai 'hak untuk dibiarkan sendiri' (*the right to be let alone*). Definisi mereka didasarkan pada dua aras: (i) kehormatan pribadi; dan (ii) nilai-nilai seperti martabat individu, otonomi dan kemandirian pribadi.[13] Gagasan ini kemudian mendapatkan justifikasi dan pengakuan dengan adanya beberapa gugatan hukum yang kemudian memberikan pembenaran tentang perlunya perlindungan hak atas privasi, terutama dengan sandaran alasan moralitas.

Melanjutkan konsep yang dibangun oleh Warren dan Brandeis, William L. Prosser (1960) mencoba mendetailkan cakupan ruang lingkup dari hak privasi seseorang, dengan merujuk setidaknya pada empat bentuk gangguan terhadap diri pribadi seseorang, yakni:[14]

(a) Gangguan terhadap tindakan seseorang mengasingkan diri atau menyendiri, atau gangguan terhadap relasi pribadinya
(b) Pengungkapan fakta-fakta pribadi yang memalukan secara publik
(c) Publisitas yang menempatkan seseorang secara keliru di hadapan publik
(d) Penguasaan tanpa ijin atas kemiripan seseorang untuk keuntungan orang lain.

Sementara Alan Westin (1967) mendefinisikan hak atas privasi sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri mengenai kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. Keluasan cakupan privasi bisanya menjadikan banyaknya pengaturan mengenai privasi di suatu negara, baik dalam jenis maupun tingkatnya.[15] Hal ini serupa dengan konsep yang disodorkan oleh Arthur Miller (1971) yang menitikberatkan konsep privasi pada kemampuan individu untuk melakukan kontrol terhadap penyebaran informasi terkait dirinya sendiri.[16]

Selanjutnya Julie Innes (1992) mendefinisikan privasi sebagai suatu kondisi ketika seseorang memiliki kontrol atas ranah keputusan privat mereka, yang mencakup keputusan atas akses privat, informasi privat dan tindakan privat. Sementara privat sendiri dijelaskannya sebagai produk dari kecintaan, kesukaan dan kepedulian terhadap sesama.[17] Hal ini sejalan dengan penjelasan Solove (2008) yang mengatakan bahwa konteks privasi meliputi: keluarga, tubuh, jenis kelamin, rumah, dan komunikasi dan informasi pribadi seseorang.[18] Sementara Gavison (1980) melihat privasi sebagai suatu konsep yang 'kompleks', yang di dalamnya terdiri dari 'tiga unsur independen dan tereduksi, yakni: kerahasiaan, anonimitas, dan kesendirian'. Setiap elemen tersebut sifatnya independen, oleh karena 'kehilangan atau pelanggaran dapat terjadi akibat instrusi terhadap salah satu dari tiga unsur tersebut.[19]

Dari berbagai definisi yang diajukan mengenai "privasi", nampak sejumlah polarisasi yang mengemuka, yang pada intinya menempatkan privasi sebagai klaim, hak, atau hak individu untuk menentukan informasi apa saja tentang dirinya (sendiri), yang dapat disampaikan kepada orang lain. Privasi juga telah diidentifikasi sebagai ukuran kontrol individu terhadap sejumlah elemen kehidupan pribadinya, yang meliputi: (i) informasi tentang diri pribadinya; (ii) kerahasiaan identitas pribadinya; atau (iii) pihak-pihak yang memiliki akses indrawi terhadap seseorang/pribadi tersebut.[20]

---

[13] Lihat E. Bloustein, Privacy as An Aspect of Human Dignity: an Answer to Dean Prosser, dalam *New York University Law Review* Vol. 39 (1964).
[14] William L. Prosser, "Privacy: A Legal Analysis", *California Law Review* 48: 338-423, 1960.
[15] A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), hal. 7-8.
[16] Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, (Ann Arbor: University of Michigan Press, 1971) hal.25.
[17] Julie C. Inness, *Privacy, Intimacy, and Isolation*, (New York: Oxford University Press, 1992), hal. 140.
[18] Selengkapnya lihat Daniel J. Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008).
[19] Ruth Gavison, Privacy and the Limits of Law, dalam *Yale Law Journal* 89: 421-71 (1980).
[20] Ferdinand Schoeman, "Privacy: Philosophical Dimensions", dalam Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984), hal. 2.

Berbeda dengan Amerika Serikat, yang menekankan pada informasi dan komunikasi pribadi untuk menjelaskan terma dan ruang lingkup privasi, rezim Eropa menekankan pada aspek perlindungan data pribadi atau sering hanya disebut "data", sebagai bagian dari perlindungan kehidupan pribadi. Definisi ini mengacu pada ketentuan Pasal 8 Konvensi Eropa, yang telah mendorong lahirnya sejumlah penafsiran mengenai cakupan dari kehidupan pribadi, khususnya melalui sejumlah kasus, baik di Pengadilan HAM Eropa (ECtHR), maupun di dalam Pengadilan Eropa (CJEU). Cakupan ruang lingkup kehidupan pribadi menurut Pasal 8 Konvensi Eropa antara lain meliputi: akses ke data pribadi, intersepsi komunikasi, pilihan atau perubahan nama, kehidupan seksual, profesi atau domisili, perlindungan terhadap gangguan lingkungan, serta hak untuk membangun dan mengembangkan hubungan dengan orang lain.[21]

C. Perkembangan Hukum Perlindungan Data

Hukum perlindungan data pribadi berkembang sejatinya bersamaan dengan perkembangan teknologi itu sendiri, khususnya teknologi informasi dan komunikasi. Sebagaimana disinggung sebelumnya, rezim perlindungan data lahir di Eropa sebagai akibat dari ketiadaan definisi yang jelas mengenai privasi dan kehidupan pribadi, yang diatur oleh ketentuan Pasal 8 Konvensi Eropa. Hak atas perlindungan data ini sendiri bertujuan untuk melindungi individu di era masyarakat informasi. Negara yang pertama kali mengesahkan UU Perlindungan Data adalah Jerman pada tahun 1970, yang kemudian diikuti oleh Inggris pada tahun yang sama, dan kemudian sejumlah negara-negara Eropa lainnya, seperti Swedia, Prancis, Swiss, dan Austria. Perkembangan serupa juga mengemuka di Amerika Serikat, dengan adanya UU Pelaporan Kredit yang Adil pada tahun 1970, yang juga memuat unsur-unsur perlindungan data.

Pada dekade berikutnya, sejumlah organisasi regional juga mulai memberikan respon terkait dengan perlindungan data pribadi, seperti lahirnya The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), pada 1981 (diamandemen pada 2018). Sebelumnya juga lahir The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, pada 1980 (diamandemen 2013), dan The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72). Sedangkan APEC (Asia Pacifif Economic Cooperation) baru mengeluarkan APEC Privacy Framework pada 2004, yang kemudian diamandemen pada 2015.

Perkembangan signifikan hukum perlindungan data terjadi ketika Uni Eropa melakukan unifikasi hukum perlindungan datanya melalui Peraturan Perlindungan Data Umum Uni Eropa (EU GDPR—*General Data Protection Regulation*), pada 2016, dan mulai berlaku pada 25 Mei 2018. GDPR bersifat komprehensif, mencakup hampir semua pemrosesan data pribadi. Selain itu, implementasinya juga tidak hanya akan mempengaruhi pengendali dan prosesor data yang berbasis di Uni Eropa, tetapi juga mereka yang menawarkan barang atau jasa kepada, atau memantau perilaku, individu warga negara Uni Eropa. Sebagai hukum nasional, sampai dengan Januari 2018, setidaknya lebih dari 100 negara telah mengadopsi undang-undang perlindungan data. Hukum perlindungan data umumnya strukturnya memuat mengenai:

- Cakupan dan jangkauan dari perlindungan data, termasuk cakupan pengendali dan prosesor data, dan jangkauan territorial/yurisdiksi;
- Definisi dan jenis data pribadi;
- Prinsip-prinsip perlindungan data, mencakup di dalamnya alasan pemrosesan data;
- Kewajiban pengendali dan prosesor data;
- Hak-hak dari pemilik data (*data subject*); dan
- Pengawasan dan penegakan undang-undang, yang umumnya dilengkapi dengan *independent supervisory authority* (*data protection authority*).

(***Penjelasan terkait dengan beberapa struktur hukum perlindungan data di atas, pada uraian berikut ini, umumnya mengacu pada ketentuan EU GDPR***)

[21] Adrienn Lukács, What Is Privacy? The history and Definition of Privacy, dalam Keresztes, Gábor (ed.): Tavaszi Szél 2016 Tanulmánykötet I., Budapest, Doktoranduszok Országos Szövetsége, 2016.

Perlindungan data sendiri secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Singkatnya, pemilik data harus dapat memutuskan apakah ingin membagikan beberapa informasi atau tidak, siapa yang memiliki akses, untuk berapa lama, untuk alasan apa, dan dapat memodifikasi beberapa informasi ini, dll. Sedangkan data pribadi jika mengacu pada EU GDPR adalah: "*Setiap informasi terkait seseorang ('subjek data') yang dapat mengenali atau dapat dikenali; mengenali secara langsung atau tidak lansung seseorang tersebut, terutama dengan merujuk pada sebuah tanda pengenal seperti nama, nomor identitas, data lokasi, data pengenal daring atau pada satu faktor atau lebih tentang identitas fisik, psikologis, genetik, mental, ekonomi, atau sosial orang tersebut*".[22] Data pribadi umumnya dibedakan menjadi dua kategori: Data Pribadi Bersifat Umum, seperti: Nama, Alamat, Alamat e-mail, Data lokasi, IP address, web cookie; dan Data Pribadi Spesifik (Sensitif), seperti: ras, etnis, agama, pandangan politik, orientasi seksual, genetik, biometrik, kondisi mental dan kejiwaan, catatan kriminal.

Hukum perlindungan data harus berlaku untuk data otomatis dan pemrosesan data otomatis, serta format terstruktur untuk menyimpan data manual (*filing system*). Artinya UU harus mencakup segala pemrosesan data pada komputer, telepon, perangkat IoT, juga catatan kertas. Dia juga menjangkau lembaga publik (pemerintah) dan swasta. Sementara terhadap perseorangan, diterima secara luas bahwa pemrosesan untuk keperluan perseorangan atau rumah tangga dikecualikan dari berlakunya UU. Pada umumnya, hukum perlindungan data juga mempertimbangkan bahwa data bergerak lintas batas (*cross border*), yang seringkali menimbulkan masalah yurisdiksi, termasuk kemungkinan bentrok UU nasional yang berlaku. Oleh karenanya hukum harus menempatkan individu sebagai pusatnya, yang berarti memastikan bahwa data pribadi dilindungi, terlepas dari apakah data mereka diproses di dalam atau di luar wilayah di mana mereka berada (*extra territorial scope*). Dengan jangkauan ini, tranfers data pribadi kepada entitas di luar negeri, hanya dapat dilakukan jika penerima data memiliki tingkat perlindungan data yang paling tidak setara dengan ketentuan yang ada di hukum nasional pengirim.

Sedangkan prinsip-prinsip perlindungan data pada umumnya menekankan pada sejumlah hal berikut ini (perbandingan OECD, APEC, dan GDPR):

OECD (2013)	APEC (2015)	GDPR (2016)
1. Collection limitation 2. Data quality 3. Purpose specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	1. Preventing harm 2. Notice 3. Collection limitation 4. Uses of personal information 5. Choice 6. Integrity of personal information 7. Security safeguards 8. Access and correction 9. Accountability	1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimization 4. Accuracy 5. Storage limitation 6. Integrity and confidentiality 7. Accountability

Dengan mengacu pada prinsip-prinsip tersebut, pemrosesan data pribadi baru dapat dilakukan apabila ada sejumlah alasan hukum berikut ini: ada persetujuan atau konsen dari subjek data; memastikan perlunya pemrosesan untuk berlakunya kontrak dengan subjek data; kepatuhan terhadap kewajiban hukum; melindungi kepentingan vital subjek data atau orang lain; pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali (data); atau tujuan kepentingan sah (*legitimate interest*), yang dilakukan oleh pengendali atau pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan, hak atau kebebasan dari subjek data.

[22] Pasal 4 (1) EU GDPR.

Sementara kewajiban bagi pengendali dan prosesor data secara umum harus mengambil langkah-langkah teknis dan organisasional untuk memastikan dan menunjukkan bahwa pengolahan data yang mereka lakukan telah sesuai hukum. Secara detail kewajiban mereka umumnya meliputi: menyediakan audit data terkini; kebijakan & prosedur perlindungan data yang komprehensif; privasi *by design* dan *by default*; petugas perlindungan data (DPO); prosedur yang jelas bagi pemilik data; penilaian dampak perlindungan data (*data protection assessment*); peningkatan kapasitas staf-stafnya; langkah keamanan data yang kuat; prosedur terkait palanggaran, merekam dan melaporkan pelanggaran; prosedur penilaian untuk meninjau dan memperbaharui langkah-langkah yang telah diambil. Sedangkan hak-hak dari pemilik data (*rights of data subject*) terdiri dari: hak atas informasi, hak akses; hak untuk memperbaiki, memblokir, dan menghapus; hak untuk menyangkal (*right to object*); hak atas portabilitas data; hak yang terkait dengan pemrofilan dan pengambilan keputusan secara otomatis; hak atas pemulihan yang efektif; serta hak atas kompensasi dan pertanggungjawaban.

D. Lanskap Hukum Perlindungan Data Pribadi di Indonesia

Dalam diskursus publik di Indonesia, konsep privasi seringkali diidentifikasi sebagai konsep barat (Eropa), seperti halnya hak asasi manusia. Alasan ini menjadi pembenar atas rendahnya kesadaran publik mengenai privasi, apalagi yang terkait dengan perlindungan data pribadi seseorang. Publik di Indonesia dengan mudah menceritakan pada orang lain, tempat tinggalnya, tanggal lahirnya, serta seluruh hubungan kekerabatannya. Selain itu juga menjadi praktik umum di Indonesia, untuk menyerahkan KTP (kartu tanda penduduk) maupun identitas diri lainnya, yang di dalamnya terdapat data pribadi seseorang, kepada pihak ketiga, misalnya ketika akan memasuki suatu tempat atau gedung. Dalam konteks kekinian, para pengguna media sosial di Indonesia, umumnya secara terbuka menyantumkan tempat tinggal asli (alamat rumah); tanggal, bulan dan tahun lahir; nomor telepon; juga hubungan kekerabatan dengan orang tua atau saudara kandung. Hal ini memperlihatkan masih besarnya problem kesadaran untuk melindungi privasi atau data pribadi, sebagai bagian dari properti pribadi. Klaim yang menyatakan privasi sebagai konsep barat sesungguhnya tidak sepenuhnya benar di Indonesia, studi yang dilakukan Alan Westin (1967), terutama ketika dia memberikan gambaran mengenai konsep privasi dalam era pra-modern atau dalam struktur masyarakat tradisional, justru menggunakan contoh privasi rumah tangga dalam tatanan masyarakat Jawa dan Bali di Indonesia, dengan merujuk pada studi yang dilakukan oleh Clifford Geertz. Memang sebagai sebuah konsep hukum perlindungan terhadap privasi seseorang memang baru hadir bersamaan dengan hadirnya peraturan perundang-undangan kolonial, terutama setelah disahkannya KUHPerdata pada 1848, dan KUHP pada 1915, oleh pemerintah colonial Hindia Belanda. Hal ini salah satunya dapat diidentifikasi dengan hadirnya konsep larangan untuk memasuki rumah atau pekarangan orang lain tanpa ijin, atau adanya larangan untuk melakukan pembukaan surat tanpa ijin dari Ketua Pengadilan, yang diatur dalam Postordonnantie 1935 (Staatsblad 1934 No. 720).

Dalam perkembangannya, khususnya pasca-amandemen konstitusi—UUD 1945, hak atas privasi termasuk di dalamnya perlindungan data pribadi diakui sebagai salah hak konstitusional warga negara. Hal ini sejalan dengan dimasukannya bab khusus tentang hak asasi manusia (bill of rights) dalam konstitusi hasil amandemen (Bab XA—Pasal 28 A-J). Ketentuan memgenai jaminan perlindungan data pribadi dapat ditemukan di dalam Pasal 28G ayat (1) UUD 1945 yang menyatakan, "*Setiap orang berhak atas perlindungan atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*" . Selain perlindungan konstitusional, keterlibatan Indonesia sebagai negara pihak dari International Covenant on Civil and Political Rights (ICCPR), yang telah disahkan melalui UU No. 12/2005, juga menegaskan kewajiban pemerintah Indonesia untuk melindungi privasi dan data pribadi warga negaranya.

Hal itu juga sejalan dengan UU No. 39/1999 tentang Hak Asasi Manusia, yang dalam beberapa pasalnya menjamin perlindungan hak atas privasi warga negara, misalnya Pasal 14 (2), Pasal 29 (1) dan Pasal 31. Secara umum Pasal 29 ayat (1) menyatakan pengakuan akan hak setiap orang atas perlindungan diri

pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Perlindungan tersebut tidak hanya dalam konteks hubungan langsung, melainkan atas informasi atau data pribadi. Sedangkan dalam Pasal 14 ayat (2) disebutkan bahwa salah satu hak mengembangkan diri adalah hak untuk mencari, memperoleh, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia. Hal ini berkaitan dengan Pasal 31 UU HAM yang juga mengatur bahwa kemerdakaan rahasia dalam hubungan komunikasi melalui sarana elektronik dijamin, kecuali atas perintah hakim atau kekuasaan yang lain yang sah sesuai dengan ketentuan perundangan.

Pada level yang lebih khusus, juga terdapat sejumlah peraturan perundang-undangan yang berlaku saat ini, yang memiliki keterkaitan atau di dalamnya terdapat materi yang berhubungan dengan data pribadi—perlindungan, pengumpulan, pemrosesan, penggunaan, pembukaan data pribadi. Sejumlah peraturan perundang-undangan tersebut dapat dikelompokan menjadi sektor: (i) telokumunikasi dan informatika; (ii) Kependudukan dan kearsipan; (iii) keuangan, perbankan, dan perpajakan; (iv) perdagangan dan perindustrian; (v) layanan kesehatan; dan (vi) keamanan dan penegakan hukum.

- **Telekomunikasi dan Informatika**

Pada sektor telekomunikasi dan informatika, mulanya pengaturan mengenai perlindungan hak atas privasi hanya terkait dengan kerahasiaan informasi dan komunikasi pribadi seseorang, yang diwujudkan melalui ketentuan larangan penyadapan, dalam UU No. 36/1999 tentang Telekomunikasi. Namun dalam aturan ini pula, operator telekomunikasi diberikan wewenang untuk melakukan perekaman telekomunikasi, dengan alasan pembuktian kebenaran pemakaian fasilitas telekomunikasi atas permintaanpengguna jasa telekomunikasi. Ketentuan mengenai perlindungan data pribadi dalam sektor telekomunikasi dan informatika atau lebih luasnya dalam penyelenggaraan sistem elektronik baru mengemuka seiring dengan adanya UU No. 11/2008 tentang Informasi dan Transaksi Elektronik. Mengacu pada ketentuan Pasal 26 ayat (1) UU ITE, setiap pemindahtanganan data pribadi seseorang harus terlebih dahulu mendapatkan ijin dari pemilik data (larangan pemindahtanganan data pribadi secara sewenang-wenang). Apabila data pribadi seseorang dipindahtangankan secara sewenang-wenang, pemilik data pribadi tersebut dapat mengajukan gugatan ganti kerugian ke pengadilan (Pasal 26 ayat (2)). Akan tetapi sulitnya proses pembuktian dalam peradilan perdata di Indonesia, menyulitkan publik (pemilik data) untuk mempersoalkan secara hukum dugaan kebocoran data pribadinya. Sampai dengan tahun 2018 baru ada satu gugatan citizen lawsuit (CLS) yang diajukan ke pengadilan. Sekelompok masyarakat menggugat Facebook atas dugaan kebocoran data pribadi pengguna Facebook di Indonesia, dalam kasus Cambridge Analytica. Dalam perkembangannya, pasca-putusan Mario Costeja di Court Justice of Europe (CJEU) pada 2014, yang melahirkan klausul right to be forgotten, juga telah mempengaruhi perubahan UU ITE pada 2016. Dalam proses amandemen UU ini, anggota DPR mengusulkan agar Indonesia juga mengadopsi konsep right to be forgotten. Usulan ini kemudian diakomodasi dalam Pasal 26 ayat (3) UU No. 19/2016 tentang Perubahan UU No. 11/2008 tentang ITE, yang menyatakan: "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". Ketentuan lebih lanjut mengenai penghapusan informasi yang tidak relevan selanjutnya akan diatur dalam Peraturan Pemerintah (Pasal 26 ayat (4)). Rumusan di atas terlalu umum, dengan semata-mata menyebutkan penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan. Tidak ada penjelasan detail tersendiri mengenai apa yang dimaksud dengan informasi yang tidak relevan. Akibatnya justru berpotensi bertabrakan dengan sejumlah peraturan perundang-undangan lain dalam implementasinya, terutama dengan sejumlah aturan yang menjamin hak publik atas informasi dan kebebasan berekspresi. Sebagai contoh, potensi ketegangan dengan UU No. 40 Tahun 1999 tentang Pers, serta UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik.[23]

[23] Lihat: "Belum Menjawab Tantangan Aktual, Revisi UU ITE (Masih) Berpotensi Melanggar Kebebasan Berekspresi", dalam http://elsam.or.id/2016/10/belum-menjawab-tantangan-aktual-revisi-uu-ite-masih-berpotensi-melanggar-kebebasan-berekspresi/.

Sementara dalam UU No. 14/2008 tentang Keterbukaan Informasi Publik, perlindungan terhadap data dan informasi publik yang dihimpun oleh badan publik yang termaktub dalam Pasal 6 ayat (3) huruf (c) UU KIP yang menegaskan kepada badan publik untuk tidak memberikan informasi publik yang berkaitan dengan hak-hak pribadi. Hal tersebut juga tertulis dalam butir Pasal 17 huruf (g) dan (h) yang menyebutkan bahwa akta otentik yang bersifat pribadi dan kemauan terakhir atau wasiat seseorang serta informasi yang berkaitan dengan rahasia pribadi dinyatakan sebagai informasi yang dikecualikan. Adapun informasi yang dapat mengungkap rahasia pribadi adalah berkaitan dengan riwayat dan kondisi anggota keluarga, pengobatan kesehatan fisik dan psikis seseorang, kondisi keuangan, pendapatan dan rekening bank seseorang, serta riwayat pendidikan formal dan satuan pendidikan non-formal.[24]

Dalam implementasinya, aturan-aturan perlindungan data pribadi yang terkait dengan penyelenggaraan system elektronik, termasuk di dalamnya komunikasi dan informatika, kemudian dirumuskan dalam PP No. 82/2012, serta sejumlah Permenkominfo, sebagaimana telah diuraikan pada bagian awal tulisan ini. Beberapa Permenkominfo yang terkait misalnya Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, juga Permenkominfo No. 21/2017 tentang Perubahan Kedua Atas Permenkominfo No. 12/2016 Tentang Registrasi Pelanggan Jasa Telekomunikasi. Perlindungan data pribadi menurut Permenkominfo PDPSE meliputi perlindungan pada proses: perolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; penampilan, pengumuman, pengiriman, penyebarluasan, dan/atau pembukaan akses; dan pemusnahan data pribadi.[25] Selain cakupan perlindungan data pribadi, yang meliputi semua aspek dan tahapan pemrosesan data pribadi, dalam Permenkominfo juga diatur hak-hak dari pemilik data pribadi (rights of subject data), kewajiban pengguna data pribadi, serta kewajiban dari penyelenggara sistem elektronik dalam semua tahapan pemrosesan tersebut. Menegaskan kembali mandat PP PSTE, dalam Permenkominfo ini juga diatur mengenai kewajiban untuk menempatkan pusat data di dalam wilayah Indonesia (data localizatioan), bagi penyelenggara sistem elektronik untuk pelayanan publik. Data center di wilayah Indonesia ini dimaksudkan sebagai fasilitas yang untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.[26] Jika terjadi sengketa dalam pengelolaan data pribadi atau terjadi kegagalan dalam perlindungan kerahasiaan data pribadi, Permenkominfo ini membuka ruang pengaduan kepada menteri (Kominfo), untuk dilakukan proses penyelesaian secara musyawarah atau alternatif penyelesaian sengketa lainnya, atau jika kedua mekanisme tersebut tidak berhasil dapat menggunakan mekanisme gugatan perdata di pengadilan.[27] Permenkominfo ini memberikan tenggat waktu (transisi) dua tahun bagi penyelenggara sistem elektronik, untuk melakukan penyesuaian berbagai kewajiban dalam perlindungan data pribadi. Akan tetapi dalam praktiknya, setelah dua tahun berlakunya Permenkominfo, mayoritas penyelenggara sistem elektronik di Indonesia belum sepenuhnya melakukan penyesuaikan dengan seperangkat kewajiban perlindungan data pribadi yang diatur dalam Permenkominfo tersebut. Lagi-lagi peraturan yang hanya setingkat peraturan menteri, dengan ancaman sanksi yang hanya berupa sanksi administrative, dinilai kurang memiliki daya ikat dan memaksa bagi penyelenggara sistem elektronik.

- **Kependudukan dan Kearsipan**

Berdasarkan UU Adminduk (UU No. 23/2006), negara memiliki kewajiban untuk menyimpan dan memberikan perlindungan atas data pribadi penduduk. Oleh karenanya, hak akses petugas Penyelenggara dan Instansi Pelaksana pengumpul data pribadi penduduk berkewajiban untuk menjaga informasi dan kerahasiaan data tersebut, yang pengaturannya secara lebih rinci dimuat dalam Peraturan Presiden No. 67 Tahun 2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional. Akan tetapi, peraturan ini masih belum mengakomodasi perlindungan data pribadi penduduk (penyimpanan dan penggunaannya), kaitannya dengan pasca-pemindaian dan perekaman data yang menyangkut sidik jari dan retina mata penduduk.

[24] Lihat pula Bab IV Peraturan Komisi Informasi Nomor 1 Tahun 2010 tentang Standar Layanan Informasi Publik (PerKIP No. 1 Tahun 2010).
[25] Pasal 3 Permenkominfo PDPSE.
[26] Pasal 17 ayat (1) dan (2) Permenkominfo PDPSE.
[27] Pasal 29-33 Permenkominfo PDPSE.

Sementara Pasal 1 poin 22 UU No. 23/2014 (perubahan UU No. 23/2006), mengakui data pribadi sebagai data perseorangan yang harus disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya. Kemudian dalam Pasal 85 UU Adminduk, disebutkan bahwa negara memiliki kewajiban untuk menyimpan dan memberikan perlindungan atas data pribadi penduduk tersebut. Hal tersebut juga tercantum dalam Pasal 79 yang mewajibkan negara untuk memberikan perlindungan dan menunjuk menteri sebagai penanggung jawab hak akses data pribadi warga. Masalahnya muncul ketika ada perbedaan klasifikasi data penduduk yang "harus dilindungi / dirahasiakan". Ada perbedaan yang signifikan antara UU No 23/2006 dan amandemennya, yaitu UU No 24/2013. Situasi demikian terjadi sebagai akibat dari tidak adanya kejelasan kategorisasi data pribadi di Indonesia.

Data Pribadi Penduduk yang Harus Dilindungi (Sensitive Data)	
Pasal 84 UU No. 23/2006	Pasal 84 UU No. 24/2013
(a) Nomor Kartu Keluarga (KK), (b) Nomor Induk Kependudukan (NIK), (c) Tanggal, bulan atau tahun lahir, (d) Keterangan tentang kecacatan fisik dan/atau mental, (e) NIK ibu kandung, (e) NIK ayah, dan (f) Beberapa isi catatan peristiwa penting.	(a) Keterangan tentang cacat fisik dan/atau mental; (b) Sidik jari; (c) Iris mata; (d) Tanda tangan; dan (e) Elemen data lainnya yang merupakan aib seseorang.

Sedangkan dalam konteks kearsipan, terkait erat dengan proses kegiatan administrasi negara yang salah satunya berhubungan dengan penyelenggaraan sistem kearsipan oleh pemerintah, dan tidak jarang mencakup data/informasi pribadi seseorang, misalnya data kependudukan, serta data tenaga pengajar dan pelajar dalam perguruan tinggi.[28] Dalam Pasal 3 huruf (f) No. 43/2009 tentang Kearsipan dinyatakan bahwa salah satu tujuan kearsipan ialah untuk menjamin keselamatan dan keamanan arsip sebagai bukti pertanggung-jawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Selain itu, dalam undang-undang ini juga diatur mengenai masa retensi dari suatu data/informasi, yang rentang waktunya mulai dari 10 hingga 25 tahun. Setelah masa retensi 25 tahun, suatu arsip (data/informasi), dapat diperpanjang masa retensinya, dapat juga dimusnahkan, atau dapat juga dibuka ke publik, dengan catatan salah satunya tidak mengungkapkan rahasia atau data pribadi.[29]

- **Keuangan, Perbankan, dan Perpajakan**

UU Perbankan (UU No. 10/1998), mengatur antara lain permasalahan terkait kerahasiaan bank (*bank secrecy*),[30] dengan berlandaskan prinsip kerahasiaan (*confidential principle*), yang mewajibkan bank untuk merahasiakan segala sesuatu yang berhubungan dengan data dan informasi mengenai nasabah, baik keadaan keuangannya maupun informasi yang bersifat pribadi.[31] Dalam Pasal 1 ayat (28) UU Perbankan, rahasia bank ditafsirkan sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.[32] Dengan demikian, asas kepercayaan dan kerahasiaan sebagai landasan kinerja lembaga keuangan, turut diterapkan dalam hubungan antara pihak nasabah dan bank. Nasabah dalam melakukan penyimpanan atau menggunakan produk bank lainnya harus memberikan data pribadi yang dianggap perlu kepada bank.

Hubungan tersebut harus didukung dengan kemampuan pihak bank dalam menjaga kepercayaan nasabah serta melindungi privasi dari nasabah yang telah memberikan dan memercayakan data pribadinya. Hal tersebut tertuang dalam Pasal 40 UU Perbankan dan Pasal 41 UU No. 21/2008 tentang Perbankan Syariah,

[28] Pasal 5 ayat (1) UU Kearsipan
[29] Pasal 66 ayat (3) huruf h.
[30] Yunus Husein, *Rahasia Bank dan Penegakan Hukum*, (Jakarta: Pustaka Juanda Tigalima, 2010) hal.11-13 (Yunus Husein menguraikan empat alasan pokok perlunya ketentuan rahasia bank dalam praktik perbankan).
[31] Djoni S. Gazali dan Rachmadi Usman, *Hukum Perbankan*, (Jakarta: Sinar Grafika, 2010) hal.30.
[32] Pengertian yang sama ditunjukan pula dalam Pasal 1 ayat (14) UU Perbankan Syariah.

yang menyebutkan bahwa bank berkewajiban untuk merahasiakan keterangan mengenai nasabah penyimpanan dan simpanannya, kecuali dalam hal-hal tertentu yang dibolehkan. Pengaturan tersebut mengisyaratkan perlindungan privasi nasabah tidak hanya berkenaan dengan data keuangan (simpanan atau produk bank lain) miliknya tetapi juga mengenai data pribadi nasabah yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data pribadi lain di luar data keuangan.

Perubahan cukup radikal terjadi seiring dengan keluarnya UU No. 21/2011 tentang Otoritas Jasa Keuangan, yang memiliki wewenang pengawasan terhadap seluruh penyelenggara jasa keuangan, termasuk perbankan yang semula diawasi bank sentral. Pengawasan ini juga mencakup kerahasiaan data pribadi nasabah. Ketentuan ini kemudian diperkukuh kembali melalui Peraturan OJK (POJK) No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang pada butir Pasal 2 huruf (d) menegaskan prinsip dasar perlindungan konsumen yang harus OJK emban adalah berdasarkan pada prinsip kerahasiaan dan keamanan data/informasi konsumen. Bahkan, POJK ini memuat pula Bab khusus yang mengatur mengenai pengawasan perlindungan konsumen sektor jasa keuangan sepenuhnya berada pada kewenangan OJK.[33]

OJK bahkan secara lebih terperinci memuat daftar data dan/atau informasi pribadi konsumen yang harus dirahasiakan melalui Surat Edaran OJK Nomor 14/SEOJK.07/ 2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen, berupa nama, alamat, nomor telepon, tanggal lahir dan/atau umur, dan/atau nama ibu kandung (khusus nasabah perorangan), serta susunan direksi dan komisaris termasuk dokumen identitas berupa Kartu Tanda Penduduk/paspor/izin tinggal, dan/atau susunan pemegang saham (khusus untuk nasabah korporasi). Selain itu, merespon berkembangnya layanan teknologi finansial, yang juga disertai dengan praktik pengumpulan data pribadi konsumennya, OJK juga telah mengeluarkan dua peraturan: (i) POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (LPMUBTI); dan (ii) POJK No. 13/POJK.01/2018 tentang Inovasi Keuangan Digital Di Sektor Jasa Keuangan.

Sementara dalam konteks perpajakan, perdebatan mengemuka seiring dengan keluarnya UU No. 11/2016 tentang Pengampunan Pajak, dan keluarnya Perpu No. 1/2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan (UU No. 9/2017). Perdebatan ini muncul terutama terkait dengan kualifikasi informasi perpajakan, serta wewenang otoritas pajak untuk mengakses informasi rekening wajib pajak.

- **Perdagangan dan Perindustrian**

Dalam konteks perdagangan, selain pembicaraan mengenai transaki elektronik, yang telah diatur oleh UU ITE dan PP PSTE, perlindungan data pribadi juga erat kaitannya dengan UU No. 8/1997 tentang Dokumen Perusahaan, UU No. 8/1999 tentang Perlindungan Konsumen, dan UU No. 7/2014 tentang Perdagangan. Sayangnya UU Perlindungan Konsumen belum secara spesifik menyebutkan perlindungan data pribadi (konsumen), sebagai bagian dari hak konsumen, yang harus dilindungi oleh pelaku usaha. UU Perlindungan Konsumen justru lebih menekankan pada ketersediaan informasi yang akurat bagi konsumen (terkait barang dan jasa), yang disediakan oleh pelaku usaha. Pun demikian UU Perdagangan tidak secara detail mengatur perihal kewajiban perlindungan data pribadi (konsumen). Namun demikian di dalam ketentuan Pasal 65 ayat (3) undang-undang ditegaskan bahwa dalam perdagangan yang menggunakan sistem elektronik (e-commerce), setiap pelaku perdagangan harus sepenuhnya mengacu pada ketentuan yang berlaku dalam UU ITE. Artinya ketentuan mengenai perlindungan data pribadi juga mengikat seutuhnya setiap perdagangan yang memanfaatkan sistem elektronik. Oleh karenanya, pembentukan peraturan pemerintah mengenai perdagangan melalui sistem elektronik yang dimandatkan oleh Pasal 66 UU Perdagangan, semestinya juga mengatur mengenai perlindungan data pribadi konsumen, dengan merujuk pada peraturan perundang-undangan yang ada, terutama UU ITE dan UU Perlindungan Konsumen.

- **Layanan Kesehatan**

[33] Lihat Pasal 51-52 POJK No. 1/POJK.07/2013.

Perlindungan data pribadi dalam penyelenggaran layanan kesehatan, pada level aturannya dapat dikatakan sudah sangat komperhensif. Perlindungan ini utamanya terkait dengan data rekam medis pasien, yang sedari awal menurut UU No. 29/2004 tentang Praktik Kedokteran, telah dikualifikasikan sebagai data yang harus dirahasiakan. Pun demikian dalam UU No. 36/2009 tentang Kesehatan, juga telah diatur perihal kewajiban untuk melindungi data pribadi seseorang. Penegasan itu pula—perlindungan data rekam medis—yang dirujuk dan diatur dalam UU Rumah Sakit (UU No. 44/2009), UU Kesehatan Jiwa (UU No. 18/2014), UU Tenaga Kesehatan (UU No. 36/2014), UU Keperawatan (UU No. 38/2014). Pun demikian UU No. 35/2009 tentang Narkotika juga telah menjamin perlindungan data pribadi, khususnya pengguna yang mengikuti proses rehabilitasi. Secara teknis untuk mengaplikasikan sejumlah UU di atas, Kementerian Kesehatan juga telah mengelurkan sejumlah peraturan, khususnya terkait rekam medis, sistem informasi rumah sakit, kewajiban rumah sakit dan pasien, dll.

Berdasarkan ketentuan Pasal 52 ayat (2) UU Kesehatan, tenaga kesehatan dalam melakukan tugasnya berkewajiban untuk mematuhi standar profesi dan menghormati hak pasien. Salah satu bentuk penghormatan tersebut adalah terkait dengan hak atas informasi kesehatan pribadinya.[34] Hal ini tertulis dalam Pasal 57 ayat (1) UU tersebut yang berbunyi hak setiap orang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.

Meskipun terdapat pengakuan hak pasien sebagai jaminan perlindungan atas data pribadinya yang berupa riwayat kesehatan, namun UU Kesehatan ini tidak mengatur penuh mengenai mekanisme pemulihan bagi pemegang hak (dalam hal ini pasien) atas pelanggaran terhadap perlindungan data pribadi pasien tersebut. Dalam Undang-Undang ini tidak ditemukan pengaturan sanksi atau hukuman, baik secara administratif ataupun pidana, bagi pelanggaran privasi atas riwayat kesehatan pasien tersebut. Ketentuan yang ada dalam UU Kesehatan ini hanyalah sebatas kepada pendelegasian kewenangan Menteri Kesehatan (Menkes) untuk mengawasi penyelenggaraan kegiatan di bidang kesehatan, termasuk penggunaan riwayat kesehatan pasien.[35]

Sebagai kelanjutan dari delegasi pengaturan tersebut, Menteri Kesehatan setidaknya telah mengeluarkan tiga peraturan: (i) Peraturan Menteri Kesehatan No. 269/Menkes/Per/III/2008 tentang Rekam Medis; (ii) Peraturan Menteri Kesehatan No. 36 Tahun 2012 tentang Rahasia Kedokteran; dan (iii) Peraturan Menteri Kesehatan No. 55 Tahun 2013 tentang Penyelenggaraan Pekerjaan Rekam Medis. Ketiga peraturan tersebut mengatur mengenai cakupan rekam medis (data kesehatan pasien), penyimpanan, pembukaan, pengawasan, kualifikasi, serta hak dan kewajiban petugas kesehatan yang melakukan perekaman medis.

- **Keamanan dan Penegakan Hukum**

Dalam konteks pertahanan dan keamanan, pembicaraan mengenai perlindungan data pribadi lebih terkait dengan pengecualian dari aparat penegak hukum/intelijen, untuk merekam komunikasi pribadi seseorang, membuka data-data pribadi seseorang, termasuk melakukan profiling, dan mengakses rekening seseorang.

Pengecualian dan wewenang dari penegak hukum/intelijen untuk melakukan sejumlah tindakan di atas dapat ditemukan antara lain dalam: UU No. 8/1981 tentang KUHAP, UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi, UU No. 30/2002 tentang KPK, UU No. 21/2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, UU No. 8/2010 tentang Pemberantasan Tindak Pidana Pencucian Uang, UU No. 17/2011 tentang Intelijen Negara, UU No. 18/2011 tentang Komisi Yudisial, UU No. 9/2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, UU No. 5/2018 tentang Pemberantasan Tindak Pidana Terorisme

[34] Pasal 8 UU Kesehatan.
[35] Pasal 182-188 UU Kesehatan.

Selain lanskap hukum di atas, saat ini pemerintah Indonesia juga tengah menyiapkan RUU Perlindungan Data Pribadi, yang materinya kurang lebih mengadopsi materi-materi yang ada pada EU GDPR, terdiri dari 15 Bab dan 74 Pasal. RUU ini mengatur mulai dari Ketentuan Umum, Jenis Data Pribadi, Hak Pemilik Data Pribadi, Pemrosesan Data Pribadi, Kewajiban Pengendali dan Prosesor Data Pribadi dalam Pemrosesan Data Pribadi, Transfer Data Pribadi, Larangan dalam Penggunaan Data Pribadi, Pembentukan Pedoman Perilaku Pengendali Data Pribadi, Penecualian Terhadap Perlindungan Data Pribadi, Penyelesaian Sengketa, Kerja Sama Internasional, Peran Masyarakat, Ketentuan Pidana, Ketentuan Peralihan, dan Ketentuan Penutup.

Dalam RUU ini, data pribadi ditafsirkan 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 non elektronik*". Data pribadi dibedakan menjadi dua kategori: data pribadi yang bersifat umum, dan data pribadi yang bersifat spesifik (sensitive). Sayangnya dalam rancangan ini, tidak disebutkan dengan detail mengenai jenis-jenis data pribadi yang masuk dalam kualifikasi spesifik/sensitive, hanya dikatakan ditetapkan sesuai dengan peraturan perundang-undangan. Penerapan UU ini akan mengikuti asas extra-teritorial jurisdiction. Dikatakan di dalamya, "Undang-Undang ini berlaku untuk setiap Orang, Badan Publik, Pelaku Usaha, dan organisasi/institusi yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Transfer data dimungkinkan dilakukan baik di dalam negeri, maupun keluar negeri, dengan sejumlah persyaratan. Jika di dalam negeri, data controller dan data processor harus memastikan perlindungan terhadap data-data pribadi tersebut, sesuai dengan ketentuan peraturan perundang-undangan. Sementara jika data transfer dilakukan keluar Indonesua, pengendali data harus terlebih dahulu meminta dan memperoleh persetujuan tertulis dari Pemilik Data Pribadi untuk mentransfer Data Pribadi yang diprosesnya kepada pihak ketiga di luar wilayah hukum Indonesia. Selain itu, transfer data pribadi keluar negeri, juga hanya dimungkinkan jika: (a) negara atau organisasi internasional tersebut memiliki tingkat pelindungan Data Pribadi yang setara atau lebih tinggi dari UU ini; (b) terdapat kontrak antara Pengendali Data Pribadi dengan pihak ketiga di luar wilayah Indonesia dengan memperhatikan aspek pelindungan Data Pribadi; dan/atau (c) terdapat perjanjian internasional antarnegara.

Dalam RUU juga diatur ketentuan mengenai pengecualian dalam berlakunya perlindungan data pribadi. Pengecualian ini berlaku: (a) untuk kepentingan pertahanan dan keamanan nasional; (b) diperlukan untuk kepentingan proses peradilan sesuai dengan ketentuan Peraturan Perundang-undangan; (c) untuk kepentingan tujuan penyelenggaraan negara dan kepentingan umum, khususnya kepentingan ekonomi atau keuangan; (d) untuk penegakan kode etik profesi; (e) untuk agregat data yang pemrosesannya ditujukan untuk kepentingan statistik dan penelitian ilmiah. Namun demikian tidak dijelaskan lebih lanjut mengenai batasan dan mekanisme dalam pengecualian tersebut, termasuk tidak adanya mandat pembentukan peraturan teknis untuk mengatur pengecualian. Hanya dikatakan, "pengecualian dilaksanakan hanya dalam rangka pelaksanaan ketentuan undang-undang dan/atau perjanjian internasional yang telah diratifikasi".

Hal yang belum sama sekali diatur dalam RUU ini adalah terkait dengan pembentukan lembaga yang berfungsi sebagai regulator, pengawas, dan pengendali (independent regulatory body), atau sebuah komisi perlindungan data pribadi. Tugas pengawasan ini justru diserahkan kepada pemerintah, sesuai dengan sektornya masing-masing, dengan berkoordinasi kepada Menteri Komunikasi dan Informatika. Ini berarti Kementerian Dalam Negeri akan mengawasi data pribadi yang terkait dengan kependudukan, OJK akan mengawasi data pribadi yang terkait dengan keuangan dan perbankan, Kementerian Kesehatan akan mengawasi data pribadi yang terkait dengan rekam medis pasien, Kementerian Hukum dan HAM akan mengawasi data pribadi yang terkait dengan passport dan data-data hukum lainnya, dan seterusnya.

E. Penutup: Tantangan Aktual dan Urgensi Pembaruan Hukum Perlindungan Data

Dalam pertemuan G20 di Hamburg pada 2017, menteri-menteri anggota G20 menyepakati salah satunya perihal pentingnya perlindungan data pribadi dalam konteks pengembangan ekonomi digital.[36] Kesepakatan ini pula yang kemudian diturunkan ke dalam Peta Jalan E-Commerce, yang disahkan melalui Peraturan Presiden No. 74/2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik Tahun 2017-2019.[37] Terdapat delapan prioritas dalam pengembangan e-commerce di Indonesia menurut Perpres ini, yang meliputi: pendanaan, perpajakan, perlindungan konsumen, pendidikan dan sumberdaya manusia, infrastruktur komunikasi, logistic, keamanan siber, dan pembentukan manajemen pelaksanaan SPNBE 2017-2019. Pembicaraan mengenai perlindungan data pribadi menjadi salah satu bagian dari prioritas mengenai perlindungan konsumen.

Perkembangannya, merespon kebutuhan di atas, beberapa negara ASEAN yang lain, justru telah lebih awal melakukan menyusun aturan khusus yang terkait dengan perlindungan data pribadi. Misalnya Singapura pada 2012, Malaysia pada 2010, Filipina pada 2012, Laos pada 2017, dan Thailand pada 2019. Keterlibatan Indonesia dalam sejumlah negosiasi perjanjian dagang, baik PTA, RCEP, maupun CEPA belakangan ini, yang mulai membicarakan sektor e-commerce, dengan isu cross border data flows, juga mengharuskan kita untuk segera memperbaiki aturan perlindungan data di dalam negeri. Belum lagi, mulai berlaku mengikatnya EU GDPR pada 25 Mei 2018 yang telah berdampak besar bagi perusahaan-perusahaan Indonesia di berbagai sektor, termasuk transportasi, e-commerce, perhotelan, maupun sektor lainnya yang melakukan praktik pengumpulan data pribadi.

Sayangnya, kebutuhan aturan perlindungan data pribadi yang komprehensif tersebut belum dibarengi dengan tumbuhnya kesadaran publik dalam melindungi data pribadi. Meski survey Mastel dan APJII pada 2017 menyebutkan, 79% dari responden survey tersebut keberatan data pribadinya dipindahtangankan tanpa ijin, dan 98% diantaranya bahkan menginginkan agar segera dibentuk UU Perlindungan Data Pribadi, namun praktik di lapangan kurang menunjukan perhatian tersebut. Publik umumnya belum menempatkan data pribadi sebagai bagian dari properti yang harus dilindungi. Hal ini salah satunya dapat dilacak dari banyaknya postingan yang mengandung konten data pribadi, baik di sejumlah platform media sosial, maupun diberbagai group jejaring sosial. Selain itu, ketika akan menggunakan sejumlah platform sistem elektronik (e-commerce, transportasi online, fintech, dll) umumnya pengguna juga belum secara utuh memahami kebijakan privasi serat syarat dan ketentuan layanan dari setiap aplikasi tersebut, khususnya yang terkait dengan penggunaan data pribadi.

Oleh karenanya, dibutuhkan pendekatan yang sifatnya lebih instrumental dan struktural untuk merespon situasi tersebut, diantaranya dengan pembentukan hukum perlindungan data pribdi yang komprehensif. Pendekatan ini juga sejalan dengan sejumlah perkembangan aktual, yang terkait erat dengan praktik pengumpulan data pribadi, baik oleh institusi pemerintah maupun swasta. Dalam lingkup pemerintah misalnya, sebagai implementasi dari program Nomor Identitas Tunggal Nasional, yang dimandatkan oleh UU Administrasi Kependudukan (tahun 2006, diubah tahun 2013), sejak tahun 2011 pemerintah telah memulai perekaman data pribadi kependudukan, melalui program KTP elektronik. Secara teknis program ini diatur melalui Perpres No. 67/2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, termasuk di dalamnya juga diatur mengenai jenis-jenis data pribadi kependudukan yang direkam dalam e-KTP. Sayangnya, ketentuan mengenai pemrosesan, pengelolaan, dan perlindungan data pribadi kependudukan, termasuk pihak ketiga yang melakukan pemrosesan, belum diatur dalam peraturan tersebut. Saat ini NIK yang tertera di dalam e-KTP merupakan pra-syarat mutlak dan utama, untuk mendapatkan berbagai layanan publik, baik dari pemerintah maupun swasta. Misalnya untuk mendapatkan layanan sosial baik kesehatan, pekerjaan, pensiun, dan jaminan sosial lainnya, syarat utamanya adalah e-KTP. Selain itu untuk membuka rekening bank, maupun mendapatkan kredit dari bank,

[36] Lihat: G20 Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World, dalam http://www.g20.utoronto.ca/2017/170407-digitalization.html.

[37] Peta jalan e-commerce merupakan salah satu Paket Kebijakan Ekonomi (paket ke 14) dari total 16 Paket Kebijakan Ekonomi yang diluncurkan oleh Presiden Joko Widodo.

syarat utamanya juga e-KTP. Bahkan untuk dapat menggunakan hak pilih dalam Pemilu, menurut UU Pemilu (UU No. 7/2017) seorang warga negara terlebih dahulu harus memiliki e-KTP. Artinya, seluruh komponen data pribadi seseorang, hampir semuanya terkoneksi dengan e-KTP, yang sekaligus juga memperlihatkan kerentanan data-data pribadi di dalamnya, dari ancaman peretasan dan kebocoran.

Selain problem dalam konteks data-data pribadi yang dikumpulkan oleh pemerintah, belakangan juga menyeruak masalah yang terkait dengan data-data pribadi yang dikumpulkan oleh swasta, khususnya perusahaan yang berbasis teknologi informasi dan komunikasi. Baru-baru ini di Indonesia menyeruak sejumlah kasus pengungkapan data pribadi pengguna platform financial technology (fintech) yang berbasis peer to peer landing. Mulanya perusahaan penyedia platform mengakses data-data pribadi yang ada di ponsel pengguna, seperti foto dan nomor kontak yang tersimpan, dengan alasan untuk melakukan *credit scoring* atau penilaian yang menentukan kelayakan pinjaman yang dapat diberikan. Namun praktiknya, data yang diakses tersebut justru digunakan untuk proses penagihan, yang dilakukan oleh pihak ketiga, yang tidak terkait dalam perjanjian pengumpulan data. Selain itu, *debt collector* (pihak ketiga) dalam penagihannya, juga kerap melakukan penyebaran data pribadi pengguna, yang berupa transaksi keuangan dan foto dari pengguna kepada kontak-kontak atau kerabat yang ditemukan dari ponsel kreditur tanpa seizin dari pemilik data. Tidak sedikit pula model penagihan tersebut dilakukan dengan bentuk kekerasan berupa ancaman penyebaran foto pribadi. Sepanjang tahun 2018, Kominfo sendiri setidaknya telah memblokir 738 fintech illegal, umumnya mereka tidak memenuhi persyaratan yang ditentutan oleh Otoritas Jasa Keuangan (OJK), dan kerap melakukan penyalahgunaan data pribadi penggunanya.[38]

Ancaman kebocoran data pribadi juga kian mengemuka dengan kian berkembangnya sektor e-commerce di Indonesia. Gerakan 1000 Start Up yang diluncurkan oleh Presiden Joko Widodo, sebagai salah satu pilar dalam pengembangan ekonomi digital, setidaknya telah berhasil mendorong tumbuhnya empat startup Unicorn yang berasal dari Indonesia: Go-Jek, Tokopedia, Traveloka, dan Bukalapak. Tumbuhnya startup digital ini juga telah memicu pengumpulan data pribadi konsumen secara besar-besaran, tidak hanya data pribadi, tetapi juga data perilaku (belanja/aktivitas) dari konsumen. Mengacu pada term of services sejumlah e-commerce di Indonesia, mereka mengumpulkan data pribadi konsumen antara lain: nama, NIK, alamat, alamat email, nomor telepon, sebagian/potongan data dari anggota tubuh (biometric data). Sayangnya, belum adanya UU Perlindungan Data Pribadi berakibat pada tidak adanya standarisasi prinsip perlindungan data, yang menyebabkan minimnya pengakuan terhadap *right of data subject*. Penelitian Lembaga Studi dan Advokasi Masyarakat—ELSAM (2018), terhadap 10 perusahaan berbasis teknologi informasi dan komunikasi di Indonesia menemukan sejumlah temuan perihal kesenjangan antara kebijakan privasi dan term of services dari tiap-tiap platform, dengan prinsip-prinsip perlindungan data pribadi. Beberapa perusahaan yang berasal dari luar Indonesia memang sudah berusaha untuk setidaknya mengikuti peraturan data yang ada pada EU GDPR, namun sejumlah perusahaan lokal Indonesia justru belum sama sekali mengadopsi kebijakan perlindungan data pribadi dalam kebijakan internalnya. Belum adanya UU Perlindungan Data Pribadi menjadi alasan utama mereka belum selaras dengan aturan perlindungan data, selain juga masalah rendahnya pemahaman perusahaan mengenai konsep privasi dan perlindungan data konsumen. Padahal, menurut Menteri Komunikasi dan Informatika, Rudiantara, percepatan proses pembahasan RUU Perlindungan Data Pribadi diperlukan, agar e-commerce Indonesia juga dapat mengembangkan pasarnya, hingga negara-negara yang telah mempersyaratkan perlindungan data pribadi, dalam hubungan dagangnya.[39]

***

[38] Lihat: https://www.moneysmart.id/738-fintech-ilegal-diblokir-pemerintah-sepanjang-2018/.
[39] Lihat: "Industri e-commerce terganggu bila RUU perlindungan data pribadi belum rampung", at https://nasional.kontan.co.id/news/industri-e-commerce-terganggu-bila-ruu-perlindungan-data-pribadi-belum-rampung. Lihat juga: "Pasar Indonesia akan sulit diakses bila UU perlindungan data pribadi belum rampung", at https://nasional.kontan.co.id/news/pasar-indonesia-akan-sulit-diakses-bila-uu-perlindungan-data-pribadi-belum-rampung.