REFLEKSI HUKUM

Jurnal Ilmu Hukum

p-ISSN 2541-4984 | e-ISSN 2541-5417
Volume 9 Nomor 2, April 2025, Halaman 195-214
DOI: https://doi.org/10.24246/jrh.2025.v9.i2.p195-214
Open access at: http://ejournal.uksw.edu/refleksihukum
Penerbit: Fakultas Hukum Universitas Kristen Satya Wacana

PELINDUNGAN DATA PRIBADI DALAM BISNIS KOMPUTASI AWAN DI INDONESIA: TRANSFER DATA LINTAS NEGARA DAN AKSES OLEH OTORITAS PUBLIK

PERSONAL DATA PROTECTION IN CLOUD COMPUTING BUSINESSES IN INDONESIA: CROSS-BORDER DATA TRANSFERS AND ACCESS BY PUBLIC AUTHORITIES

Konrardus Elias Liat
LDS & Partners *Attorney at Law*
Jl. Jenderal Sudirman, Kav 52-53, Jakarta Selatan 12190, Indonesia
Email: eliasborowosy@gmail.com
Sih Yuliana Wahyuningtyas
Universitas Katolik Indonesia Atma Jaya
Jalan Jenderal Sudirman 51, Jakarta Selatan 12930, Indonesia
Email: yuliana.siswartono@atmajaya.ac.id | Penulis Korespondensi

A R T I C L E I N F O

Article history:
Received
18 Juli 2024
Revised
3 Juli 2025
Accepted
18 November 2025

Kata-kata Kunci:

Data pribadi, komputasi awan, otoritas publik, transfer data

Abstrak

Komputasi awan adalah model layanan komputasi yang mengandalkan sumber daya dengan akses mudah karena layanan yang fleksibel, elastis, dilakukan sesuai permintaan, dan upaya manajemen yang rendah. Selain membawa berbagai keuntungan, terdapat pula risiko terhadap data pribadi pengguna ketika akses oleh otoritas publik tidak diatur. Penelitian ini menggunakan metode normatif yuridis untuk menganalisis legalitas permintaan akses data pribadi pengguna oleh otoritas publik dan mekanisme kepatuhan perusahaan komputasi awan untuk melindungi data pribadi dalam transfer data lintas batas. Studi menunjukkan bahwa perusahaan bertanggung jawab untuk memastikan keamanan data pribadi yang berada di bawah kendali mereka dan tidak ada akses ilegal oleh pihak ketiga, termasuk otoritas publik. Penelitian ini dimaksudkan untuk mengisi gap antara kebutuhan pelindungan data pribadi dengan semakin berkembangnya bisnis komputasi awan dan kekosongan regulasi, dan secara teoretis berkontribusi pada pengembangan teori mengenai pelindungan data pribadi melalui pendekatan perundang-undangan dan perbandingan hukum.

Abstract

Cloud computing is a computing service model that relies on easily accessible resources due to its flexibility, elasticity, ability to perform on-demand services, and low management effort. While offering various advantages, it poses risks to users' personal data, such as access to such data by a public authority in the absence of a legal framework to limit such access. The research employs juridical normative methods. The study shows that companies are responsible for ensuring the security of personal data under their control and preventing unauthorized access by third parties, including public authorities. This research aims to bridge the gap between the need for personal data protection and the growing cloud computing business, as well as the regulatory vacuum, and theoretically contribute to the development of theories on personal data protection through a legislative and comparative law approach.

Keywords: personal data, cloud computing, public authority, transfer data

PENDAHULUAN

Salah satu fenomena yang krusial dalam perkembangan ekosistem industri digital saat ini adalah dapat terhubungnya beragam sumber daya dalam satu sistem untuk dapat digunakan oleh industri dengan lebih efektif dan efisien dalam rangka mendukung pertumbuhan produktivitas, salah satunya melalui komputasi awan *(cloud computing)*. Teknologi ini membawa perubahan mendasar pada cara kita mengatur produksi dan penciptaan nilai,[1] dengan atribut utamanya (i) *on-demand self-service*;[2] (ii) *broad network access*; (iii) *invisible resource pooling*; (iv) *rapid elasticity*; dan (v) *metered services*. Secara sederhana, komputasi awan merupakan alih daya untuk penyimpanan dan pemrosesan.[3] Komputasi awan dapat dianggap sebagai infrastruktur dan model bisnis dimana penyimpanan secara lokal di server[4] dan akses data dilakukan secara *real time* melalui internet, alih-alih dalam suatu perangkat keras komputer.[5] Beberapa elemen penting dari komputasi awan sebagai suatu model layanan untuk komputasi adalah kemudahan akses sumber-sumber daya secara fleksibel, elastis, dapat dilakukan atas permintaan, dan dengan biaya pengelolaan yang rendah.[6]

Seiring dengan perkembangan pasar digital yang pesat, layanan komputasi awan semakin banyak digunakan di Indonesia. Peraturan Menteri Komunikasi dan

---

1 Christian Burmeister, Dirk Lüttgens and Frank T. Piller, 'Business Model Innovation for Industrie 4.0: Why the 'Industrial Internet' Mandates a New Perspective on Innovation' (2016) 72 (2) Die Unternehmung 124, 125.

2 Maziar Peihani, 'Financial Regulation And Disruptive Technologies: The Case Of Cloud Computing In Singapore' [2017] Singapore Journal of Legal Studies 77.

3 Shalin Parikh, et al, 'Securiåty and Privacy Issue in Cloud, Fog and Edge Computing' (2019) 160 Procedia Computer Science 734, 735.

4 Jack Newton, 'Is Cloud Computing Green Computing?' (2010) 27 (8) GPSolo 28, 29.

5 Mohd Javaida, et al, 'Evolutionary Trends in Progressive Cloud Computing Based Healtcare: Ideas, Enablers, and Barriers' (2022) 3 International Journal of Cognitive Computing in Engineering 124, 125.

6 Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, 'Cloud Computing-Software as Service', (2012) 1 (1), International Journal of Cloud Computing and Services Science (IJ-CLOSER) 11, 13.

Informasi Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (Permenkominfo No. 5 Tahun 2020) dalam Pasal 1 Angka 9 mendefinisikan komputasi awan sebagai '… model penyediaan akses jaringan yang merata, mudah, berdasarkan permintaan untuk sekumpulan sumber daya komputasi yang dapat dikonfigurasi bersama antara lain jaringan, server, penyimpanan, aplikasi dan layanan yang dapat disediakan dan dirilis dengan cepat dan dengan daya manajemen atau interaksi penyediaan layanan minimal.

Namun demikian, penggunaan komputasi awan juga mengandung risiko bagi data pribadi dan persoalan keamanan (*security issues*). Penyedia layanan komputasi memiliki kemampuan untuk mengumpulkan data pribadi subjek data ketika subjek data menggunakan/mengakses *platform* (komputasi) yang ditawarkan, termasuk melalui layanan pemerintah. Setiap informasi subjek data yang dikumpulkan oleh penyedia layanan komputasi akan digunakan untuk tujuan komersial termasuk menyediakan iklan kepada subjek data (menganalisa perilaku pasar) yang berujung pada persoalan keamanan.[7]

Urgensi penelitian ini adalah untuk merespon sejumlah kesulitan signifikan dalam praktik yang secara substansial menyentuh pemenuhan syarat persetujuan pengguna antara lain ketika terdapat permintaan dari otoritas publik bagi perusahaan komputasi awan untuk memberikan akses data pribadi pengguna untuk beragam alasan. Kepentingan umum lazim digunakan sebagai salah satu alasannya. Persoalannya, tidak terdapat definisi yang jelas mengenai kepentingan umum, sehingga penerapannya bergantung pada penafsiran. Perumusan ketentuan pemrosesan data untuk kepentingan umum dalam UU PDP[8] juga masih terlalu luas tanpa batasan ruang lingkup yang terukur dan jelas.

Urgensi berikutnya adalah berkaitan dengan fungsinya yang secara *inherent* memungkinkan transfer data melintasi batas-batas negara *(cross border data flow, CBDF)*, tanggung jawab perusahaan komputasi awan sebagai *data steward* dalam hal adanya permintaan akses terhadap data pribadi pelanggan oleh sektor publik dan syarat-syarat untuk data pribadi dapat ditransfer ke negara lain yang harus dilakukan mengikuti mekanisme kepatuhan perusahaan komputasi awan.

Proses ini berimplikasi pada kewajiban kepatuhan terhadap persyaratan pelindungan data. Tanpa adanya kepatuhan tersebut, maka transfer data lintas batas negara yang akuntabel tidak dapat dilakukan. Sementara itu, ketika perusahaan komputasi awan berintensi dan berupaya untuk memenuhi kepatuhan namun berhadapan dengan permintaan akses dari otoritas publik, terdapat pula risiko pelanggaran bukan hanya hak subjek data melainkan juga pelanggaran regulasi negara lain. Regulasi negara lain tersebut dapat berlaku terhadap perusahaan komputasi awan di Indonesia karena misalnya diprosesnya data pribadi warga negara asing tersebut sehingga menghidupkan sifat ekstrateritorial regulasi negara bersangkutan. Dengan demikian, pelanggaran atas regulasi negara asing tersebut dapat menimbulkan konsekuensi pengenaan sanksi, sehingga juga

---

7 Joshua S. Parker, 'Lost In The Cloud: Protecting End-User Privacy In Federal Cloud Computing Contracts' (2012) 41 (2) Public Contract Law Journal 385, 386.

8 Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, diundangkan di Jakarta pada tanggd 17 Oktober 2022, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

merugikan perusahaan tersebut. Analisis dalam penelitian ini didasarkan pada teori. Lebih lanjut, teori tersebut diimplementasikan dalam kerangka hukum fundamental dalam pelindungan data pribadi yang memuat prinsip-prinsip keabsahan pemrosesan data pribadi, keadilan dan transparansi, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, integritas dan kerahasiaan (keamanan), dan akuntabilitas. [9]

Letak kebaruan penelitian ini adalah belum adanya penelitian yang secara spesifik mengkaji kerangka regulasi yang menyediakan batasan untuk akses otoritas publik terhadap data pengguna komputasi awan. Batasan tersebut merupakan implementasi hak subjek data atas kendali penuh terhadap data pribadinya. Penelitian ini bertujuan untuk menyajikan analisis mendalam guna menjawab permasalahan penelitian sebagaimana dituangkan di bawah ini dan menyampaikan rekomendasi dari hasil analisis tersebut.

Penelitian yang dilakukan merupakan penelitian yuridis normatif yang merupakan penelitian hukum yang dilakukan terhadap data sekunder yang diperoleh melalui studi pustaka dan data primer. Dengan metode ini, penulis mengumpulkan data berupa norma, kaidah, asas, dan prinsip hukum yang terdapat dalam literatur berupa baik buku maupun artikel jurnal, dan peraturan perundang-undangan maupun peraturan nasional. Pendekatan penelitian yang digunakan dalam penelitian adalah kualitatif untuk memahami secara mendalam suatu fenomena secara deskriptif dengan menggunakan tafsir, nalar dan argumentasi rasional.

PEMBAHASAN

Pelindungan Data Pribadi dalam Konteks Komputasi Awan

Di Indonesia, layanan komputasi awan tunduk pada kerangka regulasi yang mengatur informasi dan transaksi elektronik sebagaimana dimuat dalam Undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE),[10] berikut regulasi turunannya, dalam hal ini Peraturan Pemerintah terkait Penyelenggaraan Sistem dan Transaksi Elektronik[11] dan regulasi turunannya, Permen Kominfo No. 5 Tahun 2020.[12]

Selain itu, sebagaimana dijelaskan dalam bagian sebelumnya di atas, layanan komputasi awan yang merupakan teknologi disruptif yang melibatkan pula data

---

9 Dawei Sun, Guiran Changb, Lina Suna, dan Xingwei Wang, 'Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments' (2011) Procedia Engineering 2853, 2853.

10 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana Diubah oleh Undang Undang Republik Indonesia Nomor 19 Tahun 2016 dan Undang-Undang Repubiik Indonesia Nomor 1 Tahun 2024, diundangkan di Jakarta pada tanggal 21 April 2008, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

11 Pasal 1 ayat (1) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, diundangkan di Jakarta, pada Tanggal 10 Oktober 2019, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

12 Pasal 9 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, diundangkan di Jakarta, pada Tanggal 24 November 2020, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

pribadi penggunanya karena model bisnisnya yang telah mengakar ke industri teknologi informasi.[13] Oleh karena itu, berlakulah pula dalam konteks ini UU PDP. Ketika data pribadi ditransmisikan melalui internet, maka terdapat potensi munculnya ancaman atau risiko bagi subjek data untuk kehilangan kendali atas data mereka. Oleh karena itu, penyelenggara komputasi awan wajib memiliki tata kelola informasi elektronik dan dokumen elektronik antara lain minimal memuat (i) hak pengguna dan kewajiban perusahaan komputasi awan guna memastikan pelindungan bagi pengguna layanan (ii) pengoperasioan komputasi awan, dan (iii) penyimpanan informasi elektronik dan dokumen elektronik pada komputasi awan.[14]

Dalam implementasinya, PP No. 71/2019 mengatur bahwa untuk memitigasi ancaman, risiko, dan potensi penyalahgunaan data pribadi pengguna serta dalam rangka pengawasan secara berkala terhadap penyelenggara komputasi awan (Pasal 21 Permenkominfo 5/2020) penegakan hukum, atas nama kepentingan umum, dan kondisi yang mendesak atau darurat, kementerian, lembaga, atau aparat penegak hukum berdasarkan aturan perundangan dapat meminta akses terhadap sistem elektronik dan/atau data elektronik kepada penyelenggara komputasi awan (lingkup privat) dan informasi elektronik dan/atau dokumen elektronik yang disimpan di komputasi awan oleh penyelenggara komputasi awan. Dalam hal demikian ini, perusahaan komputasi awan yang diminta untuk memberikan akses memikul kewajiban untuk memberikan akses tersebut dalam lima hari kalender setelah memperoleh permohonan tertulis.[15] Oleh karena tidak diatur standar baku untuk menilai dan mengukur akuntabilitas dari 'kondisi mendesak' dalam ketentuan tersebut di atas, maka justifikasi permintaan data pribadi oleh otoritas publik mengandalkan pada subjektivitas kementerian, lembaga, atau penegak hukum dan hal ini berpotensi merugikan subjek data.

Pada sisi lain, persetujuan subjek data merupakan prasyarat untuk pemrosesan data pribadi yang dalam kasus sebagaimana disampaikan di atas, menjadi diabaikan. Oleh karena itu, permintaan akses oleh otoritas publik atas data pribadi pengguna komputasi awan yang mengesampingkan persyaratan persetujuan subjek data pada satu sisi membatasi hak subjek data dan pada sisi lain, menempatkan perusahaan komputasi awan pada risiko hukum yang dapat timbul karena tidak terpenuhinya syarat persetujuan subjek data sebelum pemrosesan data, dalam hal ini dengan diberikannya akses kepada pihak ketiga.[16] Dapat dipahami bahwa dalam hal-hal tertentu dibutuhkan pengecualian. Namun demikian, pengecualian tersebut tidak boleh lebih luas daripada ketentuan yang dikecualikannya. Dengan kata lain, pengecualian harus spesifik, terukur, terbatas, dan kasuistis. Lebih lanjut, untuk memastikan bahwa tidak terjadi pelanggaran atas hak subjek data, maka perlu adanya pengaturan dalam undang-undang, mengingat

---

13 Peihani (n 2) 77.

14 Pasal 21 Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, diundangkan di Jakarta, pada Tanggal 24 November 2020, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

15 Pasal 9 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, diundangkan di Jakarta, pada Tanggal 24 November 2020, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

16 Thomas F. Brier Jr., 'Defining the Limits of Govermental Access to Personal Data Stored in the Cloud' (2017) 7 Journal of Information Policy 327, 357.

pembatasan atas hak fundamental individu tidak dapat dilakukan semata-mata atas diskresi dari otoritas publik.

Demikian pula, dalam undang-undang tersebut harus dimuat pula mekanisme untuk mengukur adanya kesesuaian antara kebutuhan akan akses terhadap data pribadi yang dikendalikan oleh perusahaan komputasi awan dengan langkah-langkah yang diambil untuk itu. Keseluruhan mekanisme tersebut harus transparan,[17] terukur, dan dapat dibuktikan. Dengan demikian, harus terdapat pula rekaman kepatuhan[18] terhadap kewajiban tersebut oleh otoritas publik untuk menjaga penatalayanan dan standar tata kelola data itu sendiri.

Meskipun komputasi awan memungkinkan penghematan biaya yang signifikan dan peningkatan efisiensi dengan memungkinkan penggunaan skala ekonomi secara luas,[19] bukan berarti Pemerintah *c.q* Lembaga Negara mengabaikan kewajibannya untuk mengatur dan mengendalikan pengendali penyedia layanan komputasi awan. Seharusnya Pemerintah *c.q* Lembaga Negara menciptakan ekosistem pelindungan untuk mengatasi berbagai risiko keamanan dan privasi yang mungkin timbul akibat kerentanan sistem pelindungan komputasi awan. Kekosongan-kekosongan ini dapat saja menimbulkan pertanyaan akan keseriusan pemerintah dalam melindungi hak-hak subjek hukum.

Merujuk kepada uraian penulis tersebut di atas dan mengingat perkembangan dan semakin maraknya permasalahan kebocoran data baik di Indonesia maupun negara lain, penyalahgunaan data pribadi subjek data serta kemampuan penyedia layanan komputasi awan untuk mengumpulkan berbagai informasi pribadi subjek data untuk komersialisasikan, maka penting bagi Pemerintah untuk melakukan pembaharuan terhadap Permenkominfo No. Tahun 2020.

Dalam Permenkominfo No. 5 Tahun 2020 tidak ditemukan bagian yang mengatur hak penyelenggara komputasi awan untuk menolak atau setidak-tidaknya mengajukan keberatan atau mempersoalkan justifikasi atas permintaan akses atas data pribadi yang berada di bawah kendalinya. Mekanisme untuk mempertanyakan, mengajukan keberatan, atau menolak tersebut seharusnya diatur sehingga memungkinkan perusahaan komputasi awan memenuhi kewajibannya untuk memastikan pelindungan atas data pribadi yang dikendalikannya terutama dalam hal terdapat pertimbangan bahwa akses atas data pribadi tersebut mengandung risiko penyalahgunaan atau terlalu luas diterapkan.

Meskipun hubungan antara subjek data dan penyedia layanan komputasi awan terletak pada perjanjian komputasi awan yang memiliki komponen berupa waktu aktif layanan, keamanan server dan data, tanggapan terhadap insiden dan rencana pengakhiran (*exit plan*).[20] Penulis berpandangan bahwa komponen tersebut tidak cukup ketika peranan negara tidak tercermin melalui pengaturan pada aturan perundang-undangan, *c.q.* Permenkominfo No. 5 Tahun 2020.

Permenkominfo No. 5 Tahun 2020 juga tidak memberikan pelindungan kepada penyelenggara komputasi awan (PSE Lingkup Privat) ketika terdapat gugatan ganti

---

17 David Plotkin, Data Stewardship - an actionable Guide to Effective Data Management and Data Governance (2nd edition, Academic Press is an imprint of Elsevier 2021) 120.

18 Josephine Wolff dan Nicole Atallah, 'Early GDPR Penalties - Analysis of Implementation and Fines Through May 2020' (2021) 11 Journal of Information Police 65, 69.

19 Parker (n 7) 385-386.

20 Parker (n 7) 386.

rugi dari subjek data karena tindakan penyelenggara komputasi awan yang memberikan akses kepada kementerian, lembaga dan/atau penegak hukum yang tidak sesuai peruntukan dan persetujuan subjek data. Jika merujuk pada Pasal 5 UU PDP, telah dimuat pengaturan mengenai hak subjek data untuk meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi dan akuntabilitas pihak yang meminta data pribadi. Pasal 5 UU PDP berbunyi: "Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi."

Sejalan dengan prinsip transparansi adalah prinsip dasar tata kelola demokrasi, Pemerintah diwajibkan oleh hukum untuk secara rutin menyediakan informasi tertentu kepada publik. Salah satu cara mereka melakukannya adalah dengan menanggapi permintaan informasi yang diajukan sesuai dengan Undang-Undang. Menjadikan data tersedia secara lebih luas bagi pemerintah menjanjikan peningkatan transparansi organisasi, peningkatan fungsi pemerintah, dorongan keterlibatan masyarakat, dukungan evaluasi keputusan pemerintah, dan jaminan akuntabilitas lembaga publik. Rilis data pemerintah juga mendorong pertumbuhan di sektor swasta dengan memandu investasi dan keputusan komersial lainnya, mendukung inovasi di sektor teknologi, dan mendorong pembangunan ekonomi dan persaingan secara luas. Namun demikian, dalam praktiknya, prinsip tersebut sangat sulit diterapkan dan cenderung disalahgunakan. penanganan privasi dan keamanan informasi yang tidak efektif telah menjadi hambatan utama terhadap akses dan penggunaan data yang efisien. ancaman terhadap privasi; kerentanan yang memperburuk ancaman tersebut; kemungkinan pengungkapan informasi mengingat ancaman dan kerentanan tersebut; dan tingkat, keparahan, dan kemungkinan kerugian yang timbul dari pengungkapan tersebut.[21]

Sebagaimana yang disampaikan oleh *National Institute of Standards and Technology (NIST)* bahwa komputasi awan sebagai paradigma yang terus berkembang,[22] maka Penyelenggara komputasi awan (PSE Lingkup Privat) dalam melakukan pemrosesan data pribadi, harus (i) sepengetahuan dan persetujuan dari subjek data, (ii) sesuai tujuan, akurat, lengkap, tidak menyesatkan, mutakhir dan dapat dipertanggungjawabkan, (iii) menjamin hak subjek data, (iv) melindungi keamanan subjek data dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah serta pengubahan atau perusakan data pribadi, dan berkewajiban untuk melaksanakan prinsip pelindungan data. Sayangnya, dalam UU PDP dimuat pula ketentuan pengecualian yang masih terlalu luas, misalnya untuk kepentingan penegakan hukum atau kepentingan umum.

Pengelolaan data dan kepercayaan publik terkadang tidak seimbang.[23] Untuk mengakomodir ketidakpastian pengaturan pemrosesan data, penulis berpandangan

---

21 Micah Altman, Alexandra Wood, David R. O'Brien, Salil Vadhan, and Urs Gasser, 'Towards a Modern Approach to Privacy-Aware Government Data Releases' (2015) 3 Berkeley Technology Law Journal 1967, 1970 – 1973.

22 Parker (n 7) 388.

23 Christine L. Borgman, 'Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier' (2018) 33 Berkeley Technology Law Journal 365, 368.

bahwa perlu dipedomani prinsip tata kelola data internasional yang terus berkembang, yaitu Prinsip TRUST (transparansi (TR), fokus (U)ser, keberlanjutan (S) berkelanjutan, dan teknologi) untuk Repositori Digital yang dirancang untuk respons terhadap Prinsip Panduan FAIR yang menekankan kepentingan kustodian dan pengurus data daripada pemilik dan pemangku kepentingan komunitas lainnya, atau 'pengguna'.[24]

Dalam rangka menjamin hak-hak warga negara, kita dapat belajar dari Australia dimana hampir semua otoritas mereka (Biro Statistik Australia, Institut Kesehatan dan Kesejahteraan Australia, Institut Studi Keluarga Australia, dan Departemen Layanan Sosial Persemakmuran) menerapkan kerangka kerja *Five Safes* yang awalnya dikembangkan oleh Kantor Statistik Nasional Inggris pada tahun 2003 sebagai seperangkat protokol untuk mengelola kondisi akses data, terutama dalam hal model tata kelola data berbasis. Kerangka kerja Five Safes paling berfokus pada peran dan fungsi penyimpanan data (penyimpanan data pemerintah dan non pemerintah yang beroperasi di berbagai tingkat yurisdiksi).[25]

Sebagai perbandingan, di Uni Eropa dengan berlakunya *the European Union General Data Protection Regulation (EU-GDPR),*[26] pemrosesan data pribadi warga negara Uni Eropa dengan dalil semata-mata untuk kepentingan penegakan hukum tidak memadai untuk mengecualikan berlakunya kewajiban terhadap pengendali data untuk pemenuhan prinsip-prinsip PDP. Pembatasan atas berlakunya EU-GDPR sebagaimana dimuat dalam Pasal 23 ayat (1) adalah untuk kepentingan berikut ini: (i) keamanan nasional; (ii) pertahanan; (iii) keamanan publik; (iv) pencegahan, penyidikan, pendeteksian atau penuntutan tindak pidana atau pelaksanaan hukuman pidana, termasuk pelindungan terhadap dan pencegahan ancaman terhadap keamanan publik; (v) tujuan penting lainnya dari kepentingan umum Uni Eropa atau Negara Anggota, khususnya kepentingan ekonomi atau keuangan penting Uni Eropa atau Negara Anggota, termasuk masalah moneter, anggaran dan perpajakan, kesehatan masyarakat dan jaminan sosial; (vi) pelindungan independensi peradilan dan proses peradilan; (vii) pencegahan, penyidikan, pendeteksian dan penuntutan pelanggaran etika profesi yang diatur; (viii) fungsi pemantauan, inspeksi atau pengaturan yang terkait, bahkan kadang-kadang, dengan pelaksanaan otoritas resmi dalam hal-hal yang disebutkan dalam poin (i) sampai (v) dan (vii); (ix) pelindungan subjek data atau hak dan kebebasan orang lain; dan (x) penegakan tuntutan hukum perdata.

Atas pembatasan berlakunya EU-GDPR tersebut, namun demikian, tetap dibatasi antara lain sebagaimana tertuang dalam Pasal 23 ayat (2) EU-GDPR yaitu harus memuat: (i) tujuan pemrosesan atau kategori pemrosesan; (ii) kategori data pribadi; (iii) ruang lingkup pembatasan yang diberlakukan; (iv) pelindungan untuk mencegah penyalahgunaan atau akses atau transfer yang melanggar hukum; (v) spesifikasi atau kategori pengendali data; (vi) periode penyimpanan dan

---

24 James Rose, Marcia Langton, Kristen Smith, and Darren Clinch, 'Indigenous Data Governance in Australia: Towards A National Framework' (2023) 14 (1) International Indigenous Policy Journal 1, 22.

25 *Ibid.*, 14.

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movements of such data, and repealing Directive 95/46/EC, OJ L 119/1.

pengamanan yang berlaku dengan mempertimbangkan sifat, ruang lingkup dan tujuan pemrosesan atau kategori pemrosesan; (vii) risiko terhadap hak dan kebebasan subjek data; dan (viii) hak subjek data untuk diberi tahu tentang pembatasan tersebut, kecuali hal itu dapat merugikan tujuan pembatasan tersebut.

Dalam hal isu tata kelola dan penatagunaan data harus mengedepankan asas transparansi dan akuntabilitas tanpa harus merusak atau mencederai privasi dan kerahasiaan.[27] Hal ini diimplementasikan antara lain dalam Directive (EU) 2016/680 dari Parlemen Eropa dan Dewan tahun 2016 yang mengatur tentang pelindungan individu sehubungan dengan pemrosesan data pribadi oleh otoritas publik untuk tujuan pencegahan, investigasi, deteksi, atau penuntutan tindak pidana atau pelaksanaan hukuman pidana, dan bagaimana ruang gerak perpindahan data semacam itu.[28] Di dalam Pasal 4 ayat (1) disyaratkan bahwa pemrosesan data untuk tujuan tersebut tetap tunduk pada kewajiban untuk memenuhi sejumlah prinsip, yaitu (i) sah dan adil; (ii) spesifik, eksplisit, dan, dapat dijustifikasi; (iii) secukupnya, relevan, dan tidak berlebihan; (iv) akurat, retensi terbatas; dan (v) aman.

Di Indonesia juga belum ada kejelasan kapan akan dibentuknya suatu otoritas PDP yang independen dengan tugas antara lain mengimplementasikan regulasi PDP, menetapkan syarat yang harus dipenuhi oleh penyelenggara sistem elektronik sebagai implementasi dari ketentuan-ketentuan yang umum dalam regulasi PDP, memberi persetujuan, dan memfasilitasi PDP dalam hal pemrosesan data dilakukan di luar wilayah Republik Indonesia.

Otoritas PDP yang independen paling tidak memiliki peran untuk (i) mengidentifikasi, memastikan kepatuhan terhadap manajemen pelindungan data baik bagi sektor publik maupun bagi sektor swasta termasuk di lingkungan bisnis; (ii) menentukan prosedur pengendalian pengelolaan data, (iii) mengelola risiko dengan menerapkan prosedur kontrol berbasis risiko (*risk-based control*) dan melaporkan setiap insiden keamanan dan kepatuhan; (iv) menentukan langkah-langkah keamanan pelindungan data (organisasi dan teknis tertentu)[29] seperti: kerahasiaan mencakup risiko atas pengungkapan secara tidak sah, integritas mencakup risiko atas kualitas data selaras dengan tujuan, akurat dan lengkap dan ketersediaan data mencakup risiko atas informasi yang tidak tersedia kepada pengguna.

Tanggung Jawab Pelindungan Data Pribadi dan Konsep *Data Stewardship*

Pasal 56 ayat (2) UU PDP mengatur bahwa pengendali data dapat melakukan transfer data pribadi ke luar wilayah hukum Negara Republik Indonesia dengan kewajiban memastikan negara kedudukan pengendali data pribadi dan/atau prosesor data pribadi yang menerima transfer data pribadi memiliki tingkat pelindungan data pribadi yang setara atau lebih tinggi dari yang diatur dalam UU

---

27 Borgman (n 23) 395-397.

28 Directive (EU) 2016/680 of the European Parliament an of the Council of 27 April 2016 in the Protection of Natural Person … Repealing Council Framework Decision 2008/977/JHA.

29 Francesco Ciclosi, and Fabio Massacci, 'The Data Protection Officer: A Ubiquitous Role That No One Really Knows' (2023) 21 (1) IEEE Security and Privacy 1, 11.

PDP. Pasal 56 ayat (2) UU PDP berbunyi: "Melakukan transfer Data Pribadi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib memastikan negara tempat kedudukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima transfer Data Pribadi memiliki tingkat Pelindungan Data Pribadi dalam yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini." Namun demikian, dalam UU PDP tidak diatur apa yang dimaksud dengan dan bagaimana standar untuk mengukur tingkat pelindungan data pribadi yang setara atau lebih tinggi dari yang diatur dalam UU PDP dalam rangka penegakan hukum.

Keseluruhan persyaratan tersebut harus dimuat dalam undang-undang karena adanya pembatasan terhadap hak fundamental individu, termasuk apakah dibutuhkan adanya surat perintah pengadilan sebagai syarat permintaan akses tersebut, seperti halnya juga dalam hal dilakukannya penyadapan. Data pribadi yang diakses juga haruslah spesifik dan relevan dengan tujuan penegakan hukum yang dimaksud, jadi tetap ada batasannya.

Pemrosesan data pribadi sekurang-kurangnya harus menetapkan tujuan dan prosedur untuk menjaga integritas dan kerahasiaan data pribadi termasuk pemusnahan sehingga terjaminnya pemprosesan dan potensi penyalahgunaan dan kesewenang-wenangan. Jika hanya melampirkan dasar kewenangan, maksud dan tujuan, sistem elektronik, tindak pidana yang sedang disidik, dituntut atau disidang sebagaimana dimaksud dalam Pasal 39 Permen Kominfo No. 5 Tahun 2020 tentu tidaklah memadai karena tidak dapat serta merta menunjukkan relevansi dan keterukuran antara tujuan dengan tindakan dan jenis data yang diminta.

Kekosongan pengaturan Permen Kominfo No. 5 Tahun 2020 tersebut di atas juga termasuk pengaturan kewajiban penyedia layanan komputasi awan untuk menyediakan informasi yang harus disampaikan kepada subjek data. Apabila dibandingkan dengan Pasal 42 Directive (EU) 2016/680 yang pada intinya mengatur informasi minimal yang wajib disampaikan kepada subjek data, maka penyedia layanan komputasi awan wajib menyampaikan: (i) identitas pengendali data, (ii) keberadaan operasi pemrosesan, (iii) tujuan pemrosesan, (iv) hak untuk mengajukan keluhan, (v) dan keberadaan hak untuk meminta dari pengendali akses ke dan perbaikan atau penghapusan data pribadi atau pembatasan pemrosesan termasuk dalam kasus-kasus tertentu informasi mengenai dasar hukum pemrosesan dan berapa lama data akan disimpan, sejauh mana informasi diperoleh, untuk menjamin pemrosesan adil dan berdasarkan hukum.

Hal di atas menunjukan bahwa norma pengaturan dalam Permen Kominfo No. 5 Tahun 2020 cenderung merugikan subjek data dan PSE lingkup privat, termasuk penyedia layanan komputasi awan. Subjek data tidak mendapatkan informasi atas data pribadinya yang 'diberikan akses' dan PSE lingkup privat dapat saja dikenakan sanksi jika tidak memberikan akses terhadap informasi dan data elektronik yang diminta penegak hukum dalam jangka waktu paling lambat 5 hari kalender, setelah dilaporkan kepada Menteri.

Dalam hal ini, dapat disampaikan dua hal. Pertama, Permen Kominfo No. 5 Tahun 2020 dibuat sebelum lahirnya UU PDP. Oleh karena itu, dapat terjadi bahwa ketentuan di dalam Permen Kominfo No. 5 Tahun 2020 tidak selaras atau bahkan bertentangan dengan UU PDP. Dalam konteks penyusunan suatu peraturan perundang-undangan sangat penting ditempuhnya langkah harmonisasi untuk

memastikan bahwa peraturan perundang-undangan yang ada tidak saling berbenturan atau tumpang tindih.

Kedua, oleh karena dari stratanya Permen Kominfo No. 5 Tahun 2020 merupakan peraturan yang berada dalam tingkat yang lebih rendah dari UU PDP sebagai undang-undang, maka perlu ditempuh penyesuaian dan revisi atas Permenkominfo No. 5 Tahun 2020 agar peraturan tersebut dapat selaras dengan UU PDP. Penyesuaian atau revisi tersebut perlu sesegera mungkin dilakukan agar dapat memberikan kepastian hukum bagi semua pihak dan mencegah timbulnya kerugian yang semestinya dapat dihindarkan.

Dalam Permen Kominfo No. 5 Tahun 2020 perlu dimuat syarat-syarat minimal pelindungan data pribadi mencakup (i) prinsip terkait kualitas data; (ii) kriteria untuk pemrosesan data; (iii) hak subjek data untuk mengakses data; dan (iv) hak subjek data untuk mengajukan keberatan.[30] Hal ini sejalan dengan semangat UU PDP yaitu menjamin hak warga negara, menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi.[31]

Tata kelola data yang baik untuk keberhasilan manajemen data dilakukan sejalan dengan konsep *data stewardship* bahwa terdapat penatalayan yang bertanggung jawab dan prosedur yang mengharuskan penatalayan melakukan konsultasi tentang keputusan-keputusan data yang dikelola.[32] Aspek penting dalam *data stewardship* adalah mengumpulkan dan mendokumentasikan metadata sesuai standar untuk kualitas data (*data governance*).

Hal itu dimaksudkan untuk memelihara hubungan kepercayaan *(fiduciary duty)* untuk kepentingan subjek data (individu atau entitas) yang datanya disimpan di dan dikelola oleh sistem (*fit for use*).[33]

Penyedia layanan komputasi awan tersebut di atas dalam memberikan layanan atau melakukan tugasnya harus dilandaskan pada prinsip-prinsip komunikasi privasi daring (*fair information practice*), dimana pada intinya harus melindungi nilai-nilai dasar setiap orang pada perkembangan teknologi. Prinsip-prinsip tersebut antara lain *notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress,*[34] *lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, integrity* dan *confidentiality*.

Prinsip-prinsip tersebut secara garis besar adalah sebagai berikut: (i) *awfulness, fairness, and transparency*; (ii) *purpose limitation* yang merujuk pada syarat bahwa pengumpulan data pribadi harus didasarkan pada tujuan yang spesifik, eksplisit, dan sah, dan tidak boleh diproses lebih lanjut menyimpang atau melampaui tujuan tersebut; (iii) d*ata minimization* yang mengacu pada prinsip

---

30 Bart Custers, and Helena Vrabec, 'Tell Me Something New: Data Subject Rights Applied to Inferred Data and Profiles (2024) 52 Computer Law and Security Review 1, 6.

31 Huruf b Bagian Menimbang Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, diundangkan di Jakarta pada tanggal 17 Oktober 2022, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

32 Plotkin (n 17) 78.

33 W. Van Donge, N. Bharosa, and M. F.W.H.A. Janssen, 'Data-Driven Government: Cross-Case Comparison of Data Stewardship in Data Ecosystems' (2022) 39 (2) Government Information Quarterly 1, 2.

34 April D. Lambert, Michelle Parker, and Masooda Bashir, 'Library Patron Privacy in Jeopardy an Analysis of the Privacy Policies of Digital Content Vendors' (Proceedings of the Association for Information Science and Technology, Januari 2015) 3-4.

bahwa data pribadi yang diproses haruslah secukupnya, relevan, dan terbatas pada apa yang diperlukan untuk mencapai tujuan sebagaimana disebutkan dalam prinsip sebelumnya; (iv) a*ccuracy,* artinya data pribadi yang diproses haruslah akurat; (v) *Integrity and confidentiality*, artinya pemrosesan data pribadi harus memenuhi prinsip-prinsip PDP untuk menjamin keamanan atas data pribadi.[35]

Selain berasaskan pada prinsip-prinsip komunikasi privasi daring tersebut di atas, seluruh data (pribadi) yang disimpan menggunakan fasilitas *cloud* juga harus dikelola dengan baik (tata kelola data) oleh pengelola data (*data steward*) secara akuntabilitas dengan melakukan hal-hal sebagai berikut[36] (1) dalam penyimpanan data (*in data warehousing*), minimal harus memastikan (i) dimensi apa yang dibutuhkan dan apa artinya, (ii) fakta apa yang dibutuhkan dan pada dimensi apa mereka bergantung, bagaimana mendefinisikan fakta dan aturan *derivative* dan *agregasi*; (iii) siapa yang harus bertanggung jawab atas elemen data yang membentuk dimensi dan fakta; (2) dalam manajemen data induk (*in data master management*), minimal harus menentukan: (i) apa entitas *data master* (pelanggan produk, vendor, dan lain-lain); (ii) atribut apa yang diperlukan untuk mengidentifikasi dan mengimplementasikan resolusi indetitas; (iii) sensitifitas apa yang menentukan keunikan identitas (*sensitivity to false positive and false negative*); (3) dalam peningkatan kualitas data (*in data quality improvement*), minimal harus menentukan (i) tingkat kualitas data apa yang dibutuhkan untuk tujuan tertentu; (ii) apa yang harus di-profilkan untuk memeriksa nilai-nilai yang diharapkan dari data (jangkauan, nilai spesifik, tipe data, distribusi data, dan pola); (iii) kemungkinan-kemungkinan yang menyebabkan data berkualitas buruk; (iv) persyaratan-persyaratan apa yang perlu diberikan kepada penyelenggara teknologi informasi untuk memperbaiki akan penyebab kualitas data termasuk membersikan data; (4) dalam pengembangan sistem (*in system development*), minimal harus memastikan data yang digunakan oleh suatu sistem yang terdefinisi dengan baik, memenuhi standar.

Di Uni Eropa, berdasarkan GDPR, penyedia layanan komputasi awan bertanggung jawab atas apa yang diproses dan bagaimana layanan, platform, atau infrastrukturnya memenuhi standar peraturan terkait privasi baik itu untuk sektor publik maupun swasta,[37] memungkinkan pemrosesan data untuk operasi sistem, dan membatasi akses data serta menghapus data pribadi juga tidak lagi digunakan (*the right to be forgotten*).[38] Penyedia layanan komputasi awan sebagai pengendali data bertanggung jawab atas kerusakan yang disebabkan oleh pemrosesan data ketika dalam melaksanakan tugasnya tidak mematuhi kewajiban dalam GDPR.

Selain itu, ketika pemrosesan data dilakukan untuk kepentingan publik, maka harus dilakukan dengan terlebih dahulu menentukan persyaratan yang lebih spesifik untuk pemrosesan data tersebut termasuk cara untuk memastikan

---

35 Paul Voigt dan Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Cham, Pringer 2017) 308.

36 Plotkin (n 17) 13.

37 M. P. Schwartz, 'Information Privacy in The Cloud' (2013) 161 (6) University of Pennsylvania Law Review 1623, 1634-1635.

38 Angelo Maietta, 'The Right to Be Forgotten' (2020) 12 (2) Revista de Estudos Constitucionais, Hermeneutica e Teoria Do Direito (RECHTD) 207, 217.

pemrosesan dilakukan secara sah dan adil.[39] Penyimpangan dimungkinkan pula dalam situasi tertentu namun hal tersebut telah diidentifikasi dan diantisipasi dari awal dengan mekanisme yang terukur sehingga dapat menghindarkan pengurangan atas hak dari subjek data.[40] Keseluruhan proses tersebut merupakan langkah-langkah yang harus ditempuh untuk menghormati hak atas PDP dan untuk melindungi kepentingan dasar dari subjek data.

Pelindungan Data Pribadi dalam Transfer Data Internasional melalui Komputasi Awan

Perkembangan TIK yang ditandai dengan adanya layanan *cloud,* menghadirkan kompleksitas terutama dalam transfer data lintas batas dan dalam memberikan pelindungan transfer data yang menjadi tanggung jawab penyedia layanan komputasi awan.[41] Transfer data lintas batas negara memiliki peran yang sangat penting, antara lain, peran yang memungkinkan *e-commerce* dapat berlangsung dan terselenggaranya ekonomi global.[42] UNCTAD menjelaskan bahwa transfer data lintas batas memiliki risiko karena minimnya undang-undang pelindungan data dan karenanya partisipasi pemerintah dalam *Intergovernmental Organization* berupaya menetapkan aturan, kebijakan, undang-undang dan standar-standar umum dalam rangka menekan risiko dimaksud.[43]

Aliran data lintas batas negara pada dasarnya berkaitan dengan keamanan informasi dan karenanya terdapat dua spektrum penting untuk penilaian risiko, yaitu manajemen keamanan informasi dan teknologi keamanan informasi.[44] Selain itu, pengelolaan aliran data melintasi batas negara memerlukan penanganan terkait sistem hukum dan regulasi, sistem tanggung jawab, dan jaminan keamanan.[45]

Agar data dapat ditransfer lintas batas negara, maka harus terlebih dahulu dipastikan bahwa negara penerima data pribadi memiliki regulasi yang memberikan pelindungan yang memadai *(adequate)* terhadap data yang akan ditransfer dan subjek datanya. Apabila dibandingkan dengan EU-GDPR, terdapat ketentuan yang lebih rinci mengenai kontrak tersebut yang menentukan bahwa kontrak tersebut memuat ketentuan untuk memastikan kepatuhan terhadap persyaratan pelindungan data pribadi dan hak-hak subjek data, termasuk hak untuk memperoleh ganti rugi, serta tunduk pada kewajiban kerahasiaan dan prinsip kekhususan dan tidak dipergunakan untuk tujuan lain (paragraf 71 Directive (EU) 2016/680).

---

39 Christos Karageorgiou Kaneen, et al, 'Towards Evaluating GDPR Compliace in IoT Applications' (2020) 176 Procedia Computer Science 2989, 2989.

40 Voigt dan Busschen (n 35) 308.

41 Zerui Zhao, 'The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia' (2024) 11 (4) Asian Journal of Law and Society 1, 4.

42 W. Gregory Voss, 'Cross-Border Data Flows, The GDPR, and Data Governance' (2020) 29 (3) Washington International Law Journal 485, 487.

43 Jandhyala, Srividya, and Anupama Phene, 'The Role of Intergovernmental Organizations in Cross-Border Knowledge Transfer and Innovation' (2015) 60 (4) Administrative Science Quarterly 712, 716.

44 Jin Li et al, 'Development of A Risk Index for Cross-Border Data Movement' (2022) 5 (3) Data Science and Management 97, 99.

45 *Ibid.*

Sebagai perbandingan, dalam konteks transfer data antara Uni Eropa dan Amerika Serikat, dengan berlakunya EU-GDPR terdapat pula sejumlah penyesuaian regulasi di Amerika Serikat. Salah satunya adalah dibentuknya undang-undang federal yang disebut dengan *the CLOUD Act*[46] pada tahun 2018 yang mengamandemen *Stored Communications Act (SCA)* tahun 1986. *The CLOUD Act* mengatur cara untuk melaksanakan untuk perintah pengadilan nasional untuk transfer data elektronik. Undang-undang tersebut dibuat untuk merespon keraguan yang muncul berkenaan dengan kewajiban yang terbit dari SCA untuk mentransfer data elektronik yang disimpan di *cloud* oleh suatu entitas di AS kepada otoritas penegak hukum sebagaimana dalam kasus Microsoft vs Amerika Serikat. Dalam kasus tersebut, data secara fisik berada di negara lain dan transfer yang diwajibkan tersebut dapat mengakibatkan pelanggaran norma hukum yurisdiksi asing. Dengan diterbitkannya undang-undang tersebut, maka penegak hukum federal dapat memaksa perusahaan teknologi yang berbasis di Amerika Serikat melalui surat perintah atau panggilan pengadilan untuk memberikan data yang diminta yang disimpan di server tanpa mempersoalkan apakah data tersebut disimpan di Amerika Serikat ataukah tidak. Namun demikian, entitas yang berkewajiban untuk melakukan transfer data tersebut dapat mengajukan mosi untuk membatalkan atau mengubah surat perintah tersebut apabila terpenuhi dua syarat secara bersamaan: (i) terdapat kecurigaan yang masuk akal bahwa surat perintah tersebut dikeluarkan sehubungan dengan orang bukan berkewarganegaraan Amerika Serikat yang tidak bertempat tinggal di Amerika Serikat, dan (ii) apabila terdapat risiko yang substansial akan terjadinya pelanggaran terhadap hukum negara ketiga. Selain itu, *the CLOUD Act* juga memfasilitasi perjanjian internasional bilateral yang memungkinkan transfer lintas batas bukti elektronik untuk keperluan proses pidana yang sedang berlangsung.[47]

Oleh karena itu, penyedia layanan *cloud* harus memiliki proses autentikasi, otorisasi, akuntabilitas, dan pengelolaan dokumen yang tepat. UNCTAD menjelaskan bahwa Meksiko adalah salah satu negara yang mengadopsi ketentuan khusus *cloud* dalam kaitannya dengan pelindungan data dalam mengatasi transparansi dan Republik Korea Selatan juga mengusulkan undang-undang khusus tentang komputasi awan.[48]

Sebagai perbandingan, di Uni Eropa, dalam GDPR diatur pelindungan atas data pribadi warga negara yang ditransfer dari negara anggota Uni Eropa ke negara lain baik di dalam dan luar Uni Eropa.[49] Sementara untuk transfer data pribadi ke negara lain dalam Uni Eropa berlaku regulasi yang sama, yaitu GDPR, maka untuk memastikan PDP dalam hal transfer data pribadi ke negara lain di luar Uni Eropa harus dipenuhi hal-hal sebagai berikut: [50] (i) transfer data dapat dilakukan apabila

---

46 M. Rojszczak, 'Cloud Act Agreements from an EU Perspective' (2020) 38 Computer Law and Security Review 1.

47 *Ibid.*, 3-5.

48 Seogjun Lee, Youngjin Choi, Jonghei Ra, Jongwoo Kim, dan Kelly Ashihara, 'Impact of Cloud Computing Service in Korea Government Organization' (2020) 11 (3), International Conference Information Commissioners 313, 313-314.

49 A. Mattoo & Meltzer, J. P, 'International data flows and privacy: The Conflict and Its Resolution' (2019) 4 Journal of International Economic Law 1, 3-4.

50 *Ibid.*

telah ada keputusan mengenai memadai atau tidaknya regulasi PDP di negara tujuan *(adequacy decision)*; (ii) transfer data dilakukan berdasarkan *Binding Corporate Rules (*BCR*)*, artinya harus mematuhi aturan transfer data internal untuk perusahaan multinational termasuk memfasilitasi dan jika memastikan kepatuhan terhadap regulasi PDP di Uni Eropa sehubungan dengan transfer data antar-perusahaan, atau menggunakan Klausul Kontrak Standar (SCC) untuk transaksi bisnis tertentu, mencantumkan klausula kontrak standar yang melindungi data pribadi, hanya dapat dilakukan untuk satu kali transfer atau untuk beberapa kali transfer data maka harus terdapat kode etik yang dipatuhi, dan adanya mekanisme sertifikasi untuk menyatakan pelindungan berdasarkan ketentuan yang telah ditetapkan; (iii) untuk transfer data pertama kali, perlu adanya persetujuan dari komisioner dan kode etik *European Data Protection Board*; (iv) apabila transfer data dilakukan dalam untuk melindungi kepentingan vital subjek data, kepentingan yang sah subjek data, mencegah ancaman terhadap keamanan publik negara, hak dan kebebasan subjek data terjamin maka transfer data tersebut dapat dilakukan berdasarkan pengaturan dalam Pasal 38 *Directive* (EU) 2016/680; (v) adanya kompensasi yang diberikan subjek data dirugikan karena pemrosesan data secara tidak sah.[51]

Dalam rangka memfasilitasi ekonomi digital dan transfer data di lingkungan ASEAN, ketentuan *Model Contractual Clauses (MCC)* sebagai perwujudan *ASEAN Framework on Personal Data Protection*[52] dapat digunakan sebagai rujukan untuk mengidentifikasi isu-isu utama bagi pihak-pihak dalam perjanjian yang mengikat para pihak saat mentransfer data pribadi lintas batas negara. MCC harus mengandung prinsip-prinsip yang memberikan pelindungan di ASEAN sebagaimana disepakati dalam *the 19 th ASEAN Telecommunications and Information Technology Ministers Meeting* antara lain (i) data pribadi tidak boleh dikumpulkan, digunakan, atau diungkapkan tanpa pemberitahuan dan persetujuan dari subjek data, (ii) pengumpulan dan pengungkapan data harus memiliki tujuan yang dianggap tepat oleh orang yang berakal sehat; (iii) data harus akurat dan lengkap untuk tujuan yang diusulkan.[53] Selain itu, dalam memberikan pelindungan, MCC juga mengatur mengenai klausula bahwa transfer data dilakukan sesuai prinsip dan persyaratan regulasi PDP di negara anggota ASEAN yang setara, adanya persetujuan subjek data, kode etik yang sebanding, aturan perusahaan yang mengikat, dan sertifikasi seperti seri ISO yang berkaitan dengan keamanan dan teknik privasi.

PENUTUP

---

51 Taupitz, J., and J. Weigel, 'The Necessity of Broad Consent and Complementary Regulations for the Protection of Personal Data in Biobanks: What Can We Learn from the German Case?' (2012) 15 (5) Public Health Genomics 265, 266.

52 Handayani Nasution 'Conclusion and Recommendation' (2021) Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025. Center for Indonesian Policy Studies 1, 8-22. <https://www.econstor.eu/bitstream/10419/251310/1/CIPS-PolicyPaper46.pdf>.

53 Robert Brian Smith, Mark Perry, and Nucharee Nuchkoom Smith, 'Three Shades of Data: Australia, Philippines, Thailand' [2021] Singapore Journal of Legal Studies 76, 80.

Berdasarkan pembahasan di atas, dapat disimpulkan, pertama, tanggung jawab perusahaan komputasi awan sebagai data steward dalam hal adanya permintaan akses terhadap data pribadi pelanggan oleh sektor publik adalah memastikan: (i) batasan kewenangan, (ii) jangka waktu mengakses data pribadi, (iii) mekanisme akuntabilitas dan kepatuhan atas prinsip-prinsip PDP dalam bentuk rekaman kepatuhan otoritas publik terhadap kewajiban mekanisme untuk mengukur adanya kesesuaian antara kebutuhan akan akses terhadap data pribadi yang dikendalikan oleh perusahaan komputasi awan, dan (iv) memastikan bahwa jenis data pribadi apa yang diminta (spesifik).

Kedua, sebagai syarat untuk data pribadi dapat ditransfer ke negara lain, maka transfer data pribadi tersebut harus dilakukan mengikuti mekanisme kepatuhan perusahaan komputasi awan, antara lain: (i) harus terlebih dahulu memastikan negara penerima data memiliki aturan yang memberikan pelindungan yang memadai atas data pribadi yang ditransfer; (ii) harus dilakukan mengikuti (a) prinsip pemrosesan secara sah, adil dan transparan, pengumpulan data hanya dapat dilakukan atas persetujuan subjek data, untuk tujuan yang ditentukan, memadai, relevan dan terbatas, akurat dan penyimpanan data pribadi sejauh diperlukan untuk mengidentifikasi subjek data untuk tujuan yang ditetapkan dan (b) adanya pelindungan yang ditandai dengan adanya instrumen hukum yang mengikat, terdapat kategori-kategori transfer data yang harus disampaikan kepada otoritas berwenang, dan justifikasi dan alasan transfer data.

Sebagai rekomendasi, penulis mengusulkan untuk segera dapat diterbitkannya peraturan turunan untuk melaksanakan UU PDP. Pertama-tama, peraturan tersebut dalam bentuk Peraturan Pemerintah (PP), dan berikutnya, untuk hal-hal spesifik terkait komputasi awan, dapat disusun regulasi di bawah PP, misalnya setingkat dengan Peraturan Menteri. Selain itu, perlu segera dibentuk Otoritas Pelindungan Data Pribadi dengan salah satu kewenangannya selain untuk memberikan pendampingan dan konsultasi, juga dapat menyusun dan menerbitkan Pedoman untuk pelaksanaan UU PDP dalam tingkat yang lebih praktis dan implementatif.

DAFTAR REFERENSI

Buku

Plotkin D, *Data Stewardship - an Actionable Guide to Effective Data Management and Data* Governance (2nd edition, Academic Press is an imprint of Elsevier 2021).

Voigt P, dan Bussche AVD, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham, Pringer 2017).

Jurnal

Altman M, Wood A, O'Brien DR, Vadhan S, dan Gasser U, 'Towards a Modern Approach to Privacy-Aware Government Data Releases' (2015) 3 Berkeley Technology Law Journal.

Burmeister C, Lüttgens D, dan Piller FT, 'Business Model Innovation for Industrie 4.0: Why the 'Industrial Internet' Mandates a New Perspective on Innovation' (2016) 72 (2) Die Unternehmung.

Borgman CL, 'Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier' (2018) 33 Berkeley Technology Law Journal.

Custers B, dan Vrabec H, 'Tell Me Something New: Data Subject Rights Applied to Inferred Data and Profiles (2024) 52 Computer Law and Security Review.

Ciclosi F, dan Massacci F, 'The Data Protection Officer: A Ubiquitous Role That No One Really Knows' (2023) 21 (1) IEEE Security and Privacy.

Donge WV, Bharosa N, dan Janssen MFWHA, 'Data-Driven Government: Cross-Case Comparison of Data Stewardship in Data Ecosystems' (2022) 39 (2) Government Information Quarterly.

Voss WG, 'Cross-Border Data Flows, The GDPR, and Data Governance' (2020) 29 (3) Washington International Law Journal.

Brier TF, 'Defining the limits of Govermental Access to Personal Data Stored in the Cloud' (2017) 7 Journal of Information Policy.

Taupitz J, and Weigel J, 'The Necessity of Broad Consent and Complementary Regulations for the Protection of Personal Data in Biobanks: What Can We Learn from the German Case?' (2012) 15 (5) Public Health Genomics.

Jandhyala S, and Phene A, 'The Role of Intergovernmental Organizations in Cross-Border Knowledge Transfer and Innovation' (2015) 60 (4) Administrative Science Quarterly.

Javaida M, et al, 'Evolutionary Trends in Progressive Cloud Computing Based Healtcare: Ideas, Enablers, and Barriers' (2022) 3 International Journal of Cognitive Computing in Engineering.

Kaneen CK, et al 'Towards Evaluating GDPR Compliace in IoT Applications' (2020) 176 Procedia Computer Science.

Kulkarni G, Gambhir J, Palwe R, 'Cloud Computing-Software as Service' (2012) 1 (1) International Journal of Cloud Computing and Services Science (IJ-CLOSER).

Li J et al, 'Development of A Risk Index for Cross-Border Data Movement' (2022) 5 (3) Data Science and Management.

Lee S, Choi Y, Ra J, Kim J, dan Ashihara K, 'Impact of Cloud Computing Service in Korea Government Organization' (2020) 11 (3) International Conference Information Commissioners.

Maietta A, 'The Right to Be Forgotten' (2020) 12 (2) Revista de Estudos Constitucionais, Hermeneutica e Teoria Do Direito (RECHTD).

Mattoo A, dan Meltzer JP, 'International data flows and privacy: The conflict and its resolution' (2019) 21 (4) Journal of International Economic Law.

Newton J, 'Is Cloud Computing Green Computing?' (2010) 27 (8) GPSolo.

Parikh S, et al, 'Securiåty and Privacy Issue in Cloud, Fog and Edge Computing' (2019) 160 Procedia Computer Science.

Parker JS, 'Lost In The Cloud: Protecting End-User Privacy In Federal Cloud Computing Contracts' (2012) 41 (2) Public Contract Law Journal.

Peihani M, 'Financial Regulation And Disruptive Technologies: The Case Of Cloud Computing In Singapore' [2017] Singapore Journal of Legal Studies.

Rose J, Langton M, Smith K, dan Clinch D, 'Indigenous Data Governance in Australia: Towards A National Framework' (2023) 14 (1) International Indigenous Policy Journal.

Rojszczak M, 'CLOUD Act Agreements from An EU Perspective' (2020) 38 Computer Law & Security Review.

Schwartz MP, 'Information Privacy in The Cloud' (2013) 161 (6) University of Pennsylvania Law Review.

Smith RB, Perry M, and Smith NN, 'Three Shades of Data: Australia, Philippines, Thailand' [2021] Singapore Journal of Legal Studies 76, 80.

Sun D, Changb G, Suna L, dan Wang X, 'Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments' (2011) 15 Procedia Engineering.

Wolff J, dan Atallah N, 'Early GDPR Penalties - Analysis of Implementation and Fines Through May 2020' (2021) 11 Journal of Information Police.

Zhao Z, 'The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia', (2024) 11 (4) Asian Journal of Law and Society

Laporan Penelitian

Sri Handayani Nasution 'Conclusion and Recommendation' (2021) Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025. Center for Indonesian Policy Studies 1 <https://www.econstor.eu/bitstream/10419/251310/1/CIPS-PolicyPaper46.pdf>.

Proceeding

April D. Lambert, Michelle Parker, and Masooda Bashir, 'Library Patron Privacy in Jeopardy an Analysis of the Privacy Policies of Digital Content Vendors' (Proceedings of the Association for Information Science and Technology, Januari 2015) 3-4.

Peraturan Perundangan

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Sebagaimana Diubah Oleh Undang Undang Republik Indonesia Nomor 19 Tahun 2016 dan Undang-Undang Republik Indonesia Nomor 1 Tahun 2024, diundangkan di Jakarta pada tanggal 21 April 2008, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, diundangkan di Jakarta pada tanggd 17 Oktober 2022, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

The Lawful Use of Overseas Act of 2018, Pub. L. No. 115-141, 132 Stat., 348

Directive (EU) 2016/680 of the European Parliament an of the Council of 27 April 2016 in the Protection of Natural Person ... Repealing Council Framework Decision 2008/977/JHA

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movements of such data, and repealing Directive 95/46/EC, OJ L 119/1

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, diundangkan di Jakarta, pada Tanggal 10 Oktober 2019, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, diundangkan Di Jakarta, pada Tanggal 24 November 2020, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.