"Dharmasisya" Jurnal Program Magister Hukum FHUI

Volume 2 *"Dharmasisya" Jurnal Fakultas Hukum Universitas Indonesia*

Article 28

December 2022

PERBANDINGAN PENGATURAN PENEMPATAN DATA PRIBADI PADA DATA CENTER (DATA LOCALIZATION) ANTARA INDONESIA DENGAN AUSTRALIA

Finna Claudia Ikhsan
finna.claudia@ui.ac.id

PERBANDINGAN PENGATURAN PENEMPATAN DATA PRIBADI PADA DATA CENTER (DATA LOCALIZATION) ANTARA INDONESIA DENGAN AUSTRALIA

Cover Page Footnote

Chandra Gian Asmara. Alasan Menteri Rudiantara Bolehkan Data Center di Luar Negeri. 30 Oktober 2018 diakses pada 15 Agustus 2019, Pukul 14.00 Kementerian Komunikasi dan Informatika. Rudiantara Sebut Data Center Tak Perlu di Indonesia. diakses pada 1 Oktober 2019, pukul 15.00 WIB. Indonesia, Peraturan Pemerintah Nomor 71 Tahun 2019., Ps 20 (3). Ibid., Ps 21 (1). PP PSTE, Ps. 14 (5). PP PSTE, Ps. 24 (3). Permen 28 c Permen 20/2016. DLA Piper “Data Protection Laws of the World” (last modified 3 February 2020). Ibid. Ibid. Ibid. Ibid. Ibid. Cindy Mutia Annur dan Desy Setyowati, “Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman” < https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman> Ibid. Ibid. Informasi itu disampaikan oleh Samuel Christian Hendrawan melalui akun Twitter-nya @hendralm. Cindy Mutia Annur dan Desy Setyowati, “Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman” Ibid. Ibid., Senada dengan Damar, program coordinator ICT Watch Indriyatno Banyumurti berharap regulasi itu bisa segera diluncurkan. Kemudian lima hal terkait UU Perlindungan Data Pribadi. Pertama, ia berharap tidak ada ego sektoral dalam pembuatan regulasi itu. Kedua, meminta perhatian serius dari Presiden Joko Widodo (Jokowi) dan jajarannya terkait aturan ini. Ketiga, pembahasan dengan mengedepankan asas transparansi, akuntabilitas, dan profesionalisme. Keempat, adanya literasi digital, advokasi kebijakan dan peningkatan kapasitas untuk kepentingan majemuk. Terakhir, adanya peran yang lebih signifikan dari pengampu kebijakan. Di antaranya OJK, Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Dalam Negeri (Kemendagri), dan Aparat Penegak Hukum. Data Protection Laws of the World, DLA Piper, (last modified 3 Februari 2020). . ZDNet, “Over 10 Million People Hit in Single Australia Data Breach: OAIC” < https://www.zdnet.com/article/over-10-million-people-hit-in-single-australian-data-breach-oaic/> Ibid. Webber (Insurance Services), “Data Breach in Australia for 2018, 2019, and 2020” < https://www.webberinsurance.com.au/data-breaches-list#twenty> H Jacqueline Brehmer, “Data Localization The Unintended Consequences of Privacy Litigation” American University Washington College of Law, 2018. P. 964 - 968. Ibid. Ibid. Ibid. Ibid.

UNIVERSITAS INDONESIA
Veritas, Probitas, Iustitia
DHARMASISYA
JURNAL HUKUM MAGISTER HUKUM
FAKULTAS HUKUM
UNIVERSITAS INDONESIA

DHARMASISYA

Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

PERBANDINGAN PENGATURAN PENEMPATAN DATA PRIBADI PADA *DATA CENTER* (*DATA LOCALIZATION*) ANTARA INDONESIA DENGAN AUSTRALIA

Finna Claudia Ikhsan
Fakultas Hukum Universitas Indonesia
Korespondensi: finnacikhsan@gmail.com; finna.claudia@ui.ac.id

Abstrak

Indonesia memiliki ketentuan terkait penempatan data pribadi pada *data center*. Peraturan yang dituangkan dalam PP 71/2019 yang secara spesifik membagi menjadi penyelenggara sistem elektronik lingkup publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem elektronik dan data elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri sedangkan penyelenggara sistem elektronik lingkup privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem elektronik dan data elektronik di wilayah indonesia dan/atau di luar wilayah indonesia. Australia memiliki pengaturan terkait *data localization* secara terbatas. Berdasarkan APP, Australia membentuk *Office of the Australian Information Commissioner* (OAIC) yang memiliki fungsi privasi, fungsi kebebasan informasi dan fungsi kebijakan informasi pemerintah. Untuk mengetahui pengaturan terkait penempatan data pribadi pada *data center* di Indonesia dan Australia dan implementasi penempatan data *center* di Indonesia sesuai dengan praktik internasional, menggunakan metode penelitian yuridis-normatif terhadap peraturan perundang – undangan yang mendasarinya. Berdasarkan pendekatannya, penelitian ini tergolong penelitian pendekatan komparatif atau perbandingan hukum (*comparative approach*) dan preskriptif. Metode analisis data yang diterapkan adalah kualitatif. Bentuk akhir penelitian ini adalah deskriptif-analitis. Indonesia belum memiliki pengaturan data privasi yang bersifat umum dan mengatur mengatur sanksi yang konkrit. Australia memiliki undang-undang privasi yang kuat serta OAIC yang menjaga privasi dan mengawal hak kebebasan informasi. Undang – undang perlindungan data pribadi di Indonesia secara fundamental perlu mengatur bahwa data pribadi dapat dipindahkan ke luar Indonesia, tetapi hanya jika yurisdiksi tempat penerima berada setingkat dengan dengan tetap menjamin kedaulatan dan keamanan data bagi penduduknya.
Kata Kunci: Data Pribadi; Perlindungan Data; Data Localization; Indonesia; Australia

Abstract

Indonesia has provisions related to the placement of personal data in data centers. Regulations set forth in GR 71/2019 that specifically divide the electronic system provider in the public sector can manage, process, and/or store electronic systems and electronic data outside the territory of Indonesia in the event that storage technology is not available in the country while the electronic system provider in the private sector can perform the management, processing, and/or storage of electronic systems and electronic data in the territory of Indonesia and / or outside the territory of Indonesia. Australia has limited data localization regulations. Based on the APP, Australia established the Office of the Australian Information Commissioner (OAIC) which has privacy controls, freedom of information functions and government information policy functions. To determine the arrangements related to the placement of personal data in data centers in Indonesia and Australia and the implementation of data center placement in Indonesia in accordance with international practice, using juridical-normative research methods against the underlying laws and regulations. Based on its approach, this research is classified as comparative approach research and prescriptive approach. The data analysis method applied is qualitative. The final form of this research is descriptive-analytical. Indonesia does not yet have general privacy data settings and regulates concrete sanctions. Australia has strong privacy laws and an OAIC that safeguards privacy and safeguards freedom of information rights. The protection of personal data in Indonesia is fundamentally necessary to regulate that personal data may be transferred outside Indonesia, but only if the jurisdiction in which the recipient is located is at the same level while ensuring the sovereignty and security of the data for its inhabitants.
Keywords: Personal Data; Data protection; Data Localization; Indonesia; Australia

I. PENDAHULUAN

Sebagaimana yang diatur pada Pasal 28 G ayat (1) Undang – Undang Dasar Negara Republik Indonesia Tahun 1945 bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Berdasarkan Undang – undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan ("UU 23/2006") sebagaimana telah beberapa kali diubah terakhir dengan Undang – undang Nomor 24 Tahun 2013 tentang Perubahan Atas UU 23/2006 bahwa data pribadi meliputi keterangan tentang cacat fisik dan/atau mental, sidik jari, iris mata, tanda tangan dan elemen data lainnya yang merupakan aib seseorang.

Berdasarkan Pasal 1 ayat (29) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE") definisi data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik. Sedangkan definisi data pribadi berdasarkan Pasal 1 ayat (1) Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik ("Permen Kominfo 20/2016") adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Kementerian Komunikasi dan Informatika (Kemenkominfo) membuka peluang bagi perusahaan untuk menempatkan *Data Center* (pusat data) di luar Indonesia.[1] Mantan Menteri Komunikasi dan Informatika Rudiantara pada tanggal 28 September 2018 mengatakan bahwa penempatan pusat data tidak perlu di Indonesia karena dinilai tidak efisien.[2] Pemerintah melalui PP 71/2019 mengatur secara eksplisit terkait peluang penempatan data pribadi pada *data center* di luar wilayah Indonesia, yaitu sebagai berikut:

> "Penyelenggara Sistem Elektronik Lingkup Publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri".[3]

Selanjutnya pengaturan Data Center atau Pusat Data terkait dengan sector privat ditentukan sebagai berikut:

> "Penyelenggara Sistem Elektronik Lingkup Privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia".[4]

Berdasarkan uraian di atas maka terdapat dua permasalahan yang ingin di bahas yaitu: Pertama, bagaimana pengaturan terkait penempatan data pribadi pada data center di Indonesia dan Australia? dan Kedua, bagaimana implementasi penempatan data center di Indonesia sesuai dengan praktik internasional?

II. PEMBAHASAN

Pasal 14 (5) PP PSTE mengatur bahwa, jika terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya, penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut.[5] Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap sistem elektronik, penyelenggara sistem elektronik wajib mengamankan informasi elektronik dan/atau dokumen elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan kementerian atau lembaga terkait.[6] Sebagaimana diatur pada Pasal 90 PP PSTE, bahwa pemerintah memiliki peran antara lain:

1. memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan peraturan perundang-undangan;

---

[1] Chandra Gian Asmara. *Alasan Menteri Rudiantara Bolehkan Data Center di Luar Negeri.* 30 Oktober 2018 <https://kominfo.go.id/content/detail/15220/alasan-menteri-rudiantara-bolehkan-data-center-di-luar-negeri/0/sorotan_mediadiakses> diakses pada 15 Agustus 2019, Pukul 14.00

[2] Kementerian Komunikasi dan Informatika. *Rudiantara Sebut Data Center Tak Perlu di Indonesia.*<https://kominfo.go.id/content/detail/14742/rudiantara-sebut-data-center-tak-perlu-di-indonesia/0/sorotan_media> diakses pada 1 Oktober 2019, pukul 15.00 WIB.

[3] Indonesia, *Peraturan Pemerintah Nomor 71 Tahun 2019*., Ps 20 (3).

[4] *Ibid*., Ps 21 (1).

[5] PP PSTE, Ps. 14 (5).

[6] PP PSTE, Ps. 24 (3).

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

2. melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan;
3. melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan; dan
4. menetapkan Instansi atau institusi yang memiliki Data Elektronik strategis yang wajib dilindungi.

Peran Pemerintah untuk memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud dalam Pasal 90 angka 1 meliputi:

1. penetapan kebijakan;
2. pelaksanaan kebijakan;
3. fasilitasi infrastruktur;
4. promosi dan edukasi; dan
5. pengawasan.

Fasilitasi infrastruktur meliputi sarana pengamanan Sistem Elektronik untuk pencegahan serangan terhadap infrastruktur informasi vital pada sektor strategis. Pemerintah menetapkan Instansi atau institusi yang memiliki Data Elektronik strategis yang wajib dilindungi, yang meliputi:

1. sektor administrasi pemerintahan;
2. sektor energi dan sumber daya mineral;
3. sektor transportasi;
4. sektor keuangan;
5. sektor kesehatan;
6. sektor teknologi informasi dan komunikasi;
7. sektor pangan;
8. sektor pertahanan; dan
9. sektor lain yang ditetapkan oleh Presiden.

Instansi atau institusi yang memiliki Data Elektronik strategis harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data. Ketentuan lebih lanjut mengenai kewajiban membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu diatur dalam peraturan kepala lembaga yang membidangi urusan keamanan siber. Pasal 28 c Permen 20/2016 menjelaskan lebih lanjut bahwa setiap penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi jika terjadi kegagalan perlindungan rahasia data pribadi dalam sistem elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut:[7]

1. Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia data pribadi;
2. Dapat dilakukan secara elektronik jika pemilik data pribadi telah memberikan persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan data pribadinya;
3. Harus dipastikan telah diterima oleh pemilik data pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan
4. Pemberitahuan tertulis dikirimkan kepada pemilik data pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut.

Entitas dengan kewajiban untuk mematuhi APP berdasarkan *Privacy Act* harus mematuhi persyaratan pelaporan wajib di bawah rezim pemberitahuan pelanggaran data wajib

[7] Permen 28 c Permen 20/2016.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

(*mandatory data breach notification regime*).[8] Pemberitahuan pelanggaran data wajib mencakup pelanggaran dengan data yang terkait dengan:[9]

1. Informasi pribadi;
2. Informasi pelaporan kredit;
3. Informasi kelayakan kredit;
4. Nomor file pajak.

Singkatnya, pengaturan ini mengharuskan organisasi untuk memberitahu OAIC dan orang – orang yang terkena dampak "pelanggaran data yang memenuhi syarat" (sesuai dengan isi pemberitahuan yang disyaratkan). Apabila tidak praktis untuk memberitahu individu yang terkena dampak secara individu, organisasi yang telah mengalami pelanggaran data yang memenuhi syarat harus membuat pernyataan publik di situs webnya yang berisi informasi tertentu seperti yang dipersyaratkan dalam *Privacy Act*. "Pelanggaran yang memenuhi syarat" terjadi ketika kondisi berikut dipenuhi sehubungan dengan informasi pribadi, informasi pelaporan kredit, informasi kelayakan kredit atau informasi file pajak. Kedua kondisi berikut dapat dipenuhi apabila terdapat akses tidak sah atau pengungkapan informasi yang tidak sah. Orang yang beralasan akan menyimpulkan bahwa akses atau pengungkapan akan cenderung mengakibatkan kerusakan serius pada individu manapun yang terkait dengan informasi tersebut. Informasi hilang dalam keadaan di mana kedua hal berikut berlaku:[10]

1. Akses yang tidak sah, atau pengungkapan, atau pengungkapan yang tidak sah, informasi yang kemungkinan terjadi;
2. Dengan asumsi bahwa akses yang tidak sah atau pengungkapan akses yang tidak sah terjadi, orang yang beralasan akan menyimpulkan bahwa akses atau pengungkapan tersebut akan cenderung mengakibatkan kerusakan serius pada individu manapun yang terkait dengan informasi tersebut.

Sementara kerugian "serius" tidak didefinisikan dalam undang – undang, OAIC telah merilis panduan tentang bagaimana bahaya serius dapat ditafsirkan dan dinilai oleh organisasi ada sejumlah kriteria kunci diperiksa ketika menentukan apakah kerusakan "serius" dimungkinkan disebabkan oleh pelanggaran yang harus dinilai secara holistic dan mempertimbangkan: jenis-jenis informasi, sensitivitas, langkah-langkah keamanan yang melindungi informasi, sifat dari kerugian (yaitu, kerugian fisik, psikologis, emosional, keuangan atau reputasi) dan jenis orang yang dapat memperoleh informasi.[11]

Pengaturan ini juga mengenakan kewajiban pada organisasi untuk menilai dalam 30 hari kalender apakah pelanggaran data yang memenuhi syarat telah terjadi di mana organisasi mencurigai (dengan alasan yang masuk akal) bahwa pelanggaran data yang memenuhi syarat telah terjadi, tetapi kecurigaan itu tidak berarti alasan yang masuk akal meyakini bahwa suatu pelanggaran data yang memenuhi syarat harus terjadi. Ada berbagai pengecualian terhadap persyaratan untuk memberitahu individu yang terkena dampak dan/atau OAIC tentang pemberitahuan pelanggaran data termasuk dalam kasus dimana kegiatan terkait penegakan hukum sedang dilakukan atau di mana ada deklarasi tertulis oleh Komisaris Privasi.[12]

Pengenalan peraturan ini telah menghasilkan banyak organisasi yang membutuhkan kewajiban kontrak terperinci dengan pemasok pihak ketiga sehubungan dengan keamanan siber dan perlindungan informasi pribadi pelanggan/klien mereka. Memuji pengaturan ini, OAIC

[8] DLA Piper "Data Protection Laws of the World" *(last modified 3 February 2020).* <https://www.dlapiperdataprotection.com/index.html?t=law&c=AU>

[9] *Ibid.*

[10] *Ibid.*

[11] *Ibid.*

[12] *Ibid.*

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

juga telah merilis beberapa catatan panduan yang berkaitan dengan pengaturan yang mencakup topik – topik seperti keamanan informasi pribadi, sementara ini tidak mengikat secara hukum, mereka dianggap praktik terbaik industri. Lebih lanjut, organisasi mungkin memiliki kewajiban tambahan untuk memberitahu regulator lain tentang pelanggaran data dalam keadaan tertentu termasuk di bawah *Prudential Standard CPS 234 Information Security* ("CPS 234") yang bertujuan untuk memperkuat ketahanan entitas yang diatur APRA terhadap insiden keamanan informasi (termasuk serangan siber), dan kemampuan mereka untuk merespons dengan cepat dan efektif jika terjadi pelanggaran. CPS 234 berlaku untuk semua entitas yang diatur oleh APRA yang antara lain diminta untuk memberi tahu APRA dalam waktu 72 jam "setelah mengetahui" adanya kontrol keamanan informasi material. Kelemahan diharapkan entitas tidak akan dapat diatasi tepat waktu."[13]

Di bawah ini akan diuraikan kasus penyalahgunaan data pribadi yang merugikan orang akibat adanya kebocoran data pribadi pada pusat data, bagaimana dijelaskan berikut ini. Southeast Asia Freedom of Expression Network (SAFEnet) mencatat, ada tiga motif pelanggaran data pribadi di Indonesia yakni ekonomi, politik, dan ancaman.[14] Karena itu, SAFEnet berharap pemerintah segera merilis Undang – Undang Perlindungan Data Pribadi. Pertama, ada jual beli data pribadi masyarakat Indonesia secara ilegal. Direktur Eksekutif SAFEnet Damar Juniarto mengatakan, potensi keuntungan dari perdagangan informasi ini sangat besar. Ia mencontohkan, perusahaan teknologi finansial (*fintech*) baik pembayaran maupun pinjaman (*lending*) memiliki data transaksi pengguna. Informasi ini bisa saja diperdagangkan.[15] Berdasarkan data Lembaga Hukum (LBH) pun ada sekitar 3 ribu laporan terkait penyalahgunaan data oleh *fintech* pinjaman. Namun, Damar tidak merinci apakah keluhan itu mengenai perusahaan yang terdaftar di Otoritas Jasa Keuangan (OJK) atau ilegal.[16] Selain itu, yang teranyar, viral kasus transaksi jual beli data Nomor Induk Kependudukan (NIK) dan Kartu Keluarga (KK).[17] Kedua**,** mengumpulkan data pribadi untuk diperlihatkan ke publik. Pelanggaran seperti ini biasanya terkait politik. "Misalnya, lawan politik dibuka datanya. Sebenarnya pelanggaran data pribadi, bentuknya *doxing* (melacak identitas)".[18] Ketiga**,** menggunakan data pribadi untuk mengancam orang lain. SAFEnet mencatat, pelanggaran seperti ini sudah terjadi sejak 2017. Berkaca dari ketiga motif ini lah menurutnya UU Perlindungan Data Pribadi menjadi sangat krusial dan perlu segera dirilis.[19] Damar berharap, regulasi tersebut tidak hanya memuat tentang perkara jual beli data. UU Perlindungan Data Pribadi harus mengatur pelanggaran dari segi keamanan dan keselamatan pengguna, ia juga menyampaikan banyak juga pelanggaran data pribadi untuk politik dan keamanan.[20]

---

[13] *Ibid.*

[14] Cindy Mutia Annur dan Desy Setyowati, "Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman" < https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

[15] *Ibid.*

[16] *Ibid.*

[17] Informasi itu disampaikan oleh Samuel Christian Hendrawan melalui akun Twitter-nya @hendralm. <https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

[18] Cindy Mutia Annur dan Desy Setyowati, "Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman" <https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

[19] *Ibid.*

[20] *Ibid.,* Senada dengan Damar, program coordinator ICT Watch Indriyatno Banyumurti berharap regulasi itu bisa segera diluncurkan. Kemudian lima hal terkait UU Perlindungan Data Pribadi. **Pertama,** ia berharap tidak ada ego sektoral dalam pembuatan regulasi itu. **Kedua,** meminta perhatian serius dari Presiden Joko Widodo (Jokowi) dan jajarannya terkait aturan ini. **Ketiga,** pembahasan dengan mengedepankan asas transparansi,

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

Data pribadi (disebut sebagai 'informasi pribadi' di Australia) berarti informasi atau pendapat tentang individu yang diidentifikasi, atau individu yang dapat diidentifikasi secara wajar, apakah informasi atau pendapat itu benar atau tidak, dan apakah informasi atau opini tersebut dicatat dalam bentuk material atau tidak. Data sensitif: ras atau etnis, opini politik, keanggotaan asosiasi politik, keyakinan atau afiliasi agama.[21]

Berdasarkan APP, Australia membentuk Office of the Australian Information Commissioner (OAIC) yang memiliki peran fungsi privasi, fungsi kebebasan informasi dan fungsi kebijakan informasi pemerintah, mengaudit privasi terhadap lembaga pemerintah Australia dan organisasi lain juga bisa dilakukan OAIC dalam keadaan tertentu. Laporan pelanggaran data triwulan terbaru dari OAIC telah mengungkapkan bahwa lebih dari 10 juta orang memiliki informasi mereka dikompromikan dalam satu insiden tunggal. Populasi Australia saat ini adalah sekitar 25,4 juta.[22] Pelanggaran tersebut diungkapkan kepada OAIC di bawah skema pelanggaran data yang dapat diakui (NDB) antara 1 Januari 2019, dan 31 Maret 2019 dan dilaporkan dalam *Quarterly Statistics Report*. Sementara laporan tersebut tidak merinci asal-usul pelanggaran yang mempengaruhi lebih dari 10 juta orang, itu menunjukan bahwa jumlah paling banyak orang yang terkena dampak dari satu pelanggaran terkait keuangan adalah kurang dari 500.000 dan tiga pelanggaran dampak paling berat di sektor kesehatan yang terkena dampak kurang dari masing – masing 5.000 orang. Secara total, OAIC menerima 215 pemberitahuan pelanggaran data, turun dari 262 yang dilaporkan pada periode Oktober hingga Desember 2018. 62 pelanggaran dilaporkan pada bulan Januari, 67 pada bulan Februari, dan 86 pada bulan Maret.

Dari 215, 131 – 61% dikaitkan dengan serangan jahat atau kriminal, sementara kesalahan manusia menyumbang 75 pelanggaran data, dan sembilan dilabeli sebagai kesalahan sistem. Informasi pribadi paling berpengaruh selama kuartal ini adalah informasi kontak dengan total 186 pelanggaran yang mempengaruhi data tersebut. 98 NDB terkait individu, sementara 55 berisi informasi identitas.[23] Pelanggaran data terjadi ketika informasi rahasia, pribadi, atau sensitif lainnya diakses tanpa otorisasi atau hilang. Pelanggaran data dapat terjadi secara tidak sengaja, atau sebagai akibat dari serangan yang disengaja, berikut ini merupakan daftar kasus yang terjadi di Australia pada tahun 2018, 2019 dan 2020, antara lain:[24]

Tabel 1
Data Breach in Australia for 2018, 2019, and 2020

No.	2018	2019	2020
1	Data medis nasabah Commonwealth Bank terekspos dalam potensi pelanggaran privasi –	Kartu kredit dan perincian lain dari pemohon persewaan Perth mungkin telah dipublikasikan selama 21 bulan	Kantor pusat Retailer IN SPORT terkena *ransomware* - Membangun kembali sistem tetapi kehilangan beberapa data

akuntabilitas, dan profesionalisme. **Keempat,** adanya literasi digital, advokasi kebijakan dan peningkatan kapasitas untuk kepentingan majemuk. **Terakhir,** adanya peran yang lebih signifikan dari pengampu kebijakan. Di antaranya OJK, Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Dalam Negeri (Kemendagri), dan Aparat Penegak Hukum.

[21] *Data Protection Laws of the World, DLA Piper, (last modified 3 Februari 2020).* <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=AU>.

[22] ZDNet, "Over 10 Million People Hit in Single Australia Data Breach: OAIC" < https://www.zdnet.com/article/over-10-million-people-hit-in-single-australian-data-breach-oaic/>

[23] *Ibid.*

[24] Webber (Insurance Services), "Data Breach in Australia for 2018, 2019, and 2020" < https://www.webberinsurance.com.au/data-breaches-list#twenty>

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

	Commonwealth Bank sedang menyelidiki potensi pelanggaran data yang mungkin telah memberi stafnya akses ke informasi medis sensitif nasabah.		
2	*Humble Bundle* Menjadi Korban Pelanggaran Data 'Sangat Terbatas'	Kamera Amazon Ring terus diretas.	Sistem Rekam *My Health* terkena upaya peretasan
3	Email *News Corp* mengaburkan pelajaran pahit dalam privasi data	800 warga Australia dalam pelanggaran data Vistaprint - Raksasa web-to-print Vistaprint telah menemukan sekitar 800 pelanggannya di Australia berada pada pelanggaran data online yang pertama kali diungkapkan di eksklusif Australia oleh Print21 minggu lalu, dan pada saat itu dianggap tidak menyertakan konsumen lokal.	Layanan NSW terkena serangan kompromi email | Agensi mencoba mencari tahu apa yang mereka akses

Tabel 2
Perbandingan Penyimpanan Data Pribadi di Indonesia, Uni Eropa, dan Australia

	Indonesia	**Australia**
Peraturan	1. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE); 2. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen Kominfo 20/2016).	*Australian Privacy Principles* (APPs)
Penempatan Data/*Data Localization*	1. **Penyelenggara sistem elektronik lingkup publik ("PSE Lingkup Publik")** wajib melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem elektronik dan data elektronik di wilayah Indonesia. Penyelenggara sistem elektronik lingkup publik dapat melakukan pengelolaan, pemrosesan dan/atau penyimpanan sistem elektronik dan data elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri.	Walau tidak ada persyaratan *data localization* secara umum, sehubungan data pribadi, aturan spesifik dalam bidang industri berlaku sebagai berikut: 1. Terkait *Data Localization* perusahaan telekomunikasi harus menyediakan titik intersepsi di Australia. 2. Kategori tertentu dari data yang dihasilkan pemerintah tunduk pada peraturan yang melarang penyimpanan di luar Australia. 3. Informasi kredit konsumen tertentu dan kategori terbatas dari informasi kesehatan

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

	2. **Penyelenggara sistem elektronik lingkup privat ("PSE Lingkup Privat")** dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem elektronik dan data elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia. Dalam hal sistem elektronik dan data elektronik dilakukan pengelolaan, pemrosesan, dan/atau penyimpanan di luar wilayah Indonesia, penyelenggara sistem elektronik lingkup privat wajib memastikan efektivitas pengawasan oleh kementerian atau lembaga dan penegakan hukum. 3. Penyelenggara Sistem Elektronik Lingkup Publik tidak termasuk Penyelenggara Sistem Elektronik Lingkup Publik yang merupakan otoritas pengatur dan pengawas sektor keuangan. 4. Penyelenggara sistem elektronik lingkup privat di sektor keuangan diatur lebih lanjut oleh otoritas pengatur dan pengawasan sektor keuangan	dilarang untuk diakses di luar Australia.
Data Transfer	Diperbolehkan dengan mengacu pada ketentuan bahwa pengiriman data pribadi yang dikelola oleh penyelenggara sistem elektronik (PSE) pada instansi pemerintah dan pemerintah daerah serta masyarakat atau swasta yang berdomisili di dalam wilayah negara Republik Indonesia ke luar wilayah negara Republik Indonesia harus berkoordinasi dengan Menteri atau pejabat/lembaga yang diberi wewenang untuk itu, yang berupa: a. Melaporkan rencana pelaksanaan pengiriman data pribadi, paling sedikit memuat nama jelas negara, tujuan, nama jelas subyek penerima, tanggal pelaksanaan, dan alasan/tujuan pengiriman; b. Meminta advokasi, jika diperlukan; dan c. Melaporkan hasil pelaksanaan kegiatan.	Informasi pribadi hanya dapat diungkapkan kepada organisasi di luar Australia di mana entitas telah mengambil langkah-langkah yang wajar untuk memastikan bahwa penerima di luar negeri tidak melanggar APP (selain APP 1) terkait dengan informasi pribadi.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

Sebagaimana yang dijabarkan oleh H. Jacqueline Brehmer mengenai dampak *data localization* terhadap keamanan data, bahwa:[25]

1. Saat ini, perusahaan mempekerjakan serangkaian teknis dan non-teknis kontrol untuk mengidentifikasi ancaman, mempertahankan diri dari serangan, dan merespons intrusi jaringan. Kontrol teknis dasar umumnya termasuk *firewall* dan sistem deteksi intrusi dan pemantauan ke mengidentifikasi akses tidak sah atau eksfiltrasi data. Non-teknis pengendalian terdiri dari kebijakan dan prosedur, seperti penggunaan hak istimewa terendah, pengembangan rencana tanggapan terhadap insiden, dan kepatuhan terhadap kebijakan manajemen. Program keamanan informasi yang terstruktur dengan baik akan memanfaatkan kontrol teknis dan nonteknis untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi untuk melindungi data dari pelaku jahat, mencegah perubahan yang disengaja, dan memastikan akses.[26]
2. *Data Localization* akan membutuhkan server baru, orang, dan alat di masing-masing yurisdiksi tempat perusahaan beroperasi atau memiliki pengguna. Replikasi sistem ini akan menciptakan jaringan terfragmentasi yang terkait dengan territorial batas-batas dalam suatu perusahaan. Dengan hanya melakukan peregangan dan segmentasi jaringan perusahaan, *data localization* akan mengurangi kemanjuran keamanan praktik dan alat untuk mendeteksi dan menanggapi ancaman keamanan siber. Sebaliknya, dengan memusatkan data di beberapa pusat data utama di seluruh dunia, perusahaan dapat menerapkan praktik pertahanan yang mendalam dan mengurangi redundansi. Dengan melakukan itu, perusahaan dapat memastikan manajemen sistem yang seragam, prediksi dan deteksi skala teknologi untuk mengamankan jumlah data pengguna yang lebih tinggi, dan memanfaatkan arsitektur terdistribusi dari internet untuk memastikan ketersediaan data Replikasi sistem ini tidak hanya mahal untuk dibangun tetapi juga sulit untuk dikelola karena menciptakan praktik keamanan yang tidak seragam Dengan mendesentralisasikan tata kelola dan respons, *data localization* pada dasarnya menciptakan sistem federasi dalam perusahaan yang lebih besar, mempercayakan setiap negara dengan otonomi atas sistemnya sendiri. Sebagai hasilnya, setiap yurisdiksi dapat memilih jenis perangkat keras yang akan digunakan digunakan, cara mengklasifikasikan insiden, dan cara mengelola hak istimewa.[27]
3. Selain itu, sistem keamanan terpusat memungkinkan perusahaan untuk melakukannya lebih efektif dalam memanfaatkan teknologi prediksi dan deteksi. Sistem teknologi informasi terpusat memungkinkan suatu perusahaan untuk memiliki wawasan yang lebih luas tentang lingkungannya, dan juga memungkinkan perusahaan untuk mengumpulkan informasi dari seluruh jaringan ke menentukan tren dan mengidentifikasi penyalahgunaan. Dengan menggunakan "*big data*" solusi untuk keamanan TI, perusahaan dapat mendeteksi insiden dengan lebih cepat dan mengurangi waktu antara intrusi dan deteksi.[28]
4. *Data localization* membatasi kemampuan perusahaan untuk memastikan ketersediaan sistem dan data dengan memanfaatkan infrastruktur terdistribusi internet. Karena data dapat dipecah, disalin, dan dipindahkan, perusahaan dapat memanfaatkan infrastruktur internet untuk mendistribusikan data ke server di berbagai negara bagian, negara, atau wilayah. Perusahaan mampu meningkatkan efisiensi distribusi dan keamanan mengelilingi informasi dengan membagi data, menyeimbangkan bebannya di seluruh server, dan mencadangkannya di banyak area. Hal ini memungkinkan perusahaan untuk lebih efektif

[25] H Jacqueline Brehmer, "Data Localization The Unintended Consequences of Privacy Litigation" American University Washington College of Law, 2018. P. 964 - 968.

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

menanggapi vektor ancaman tertentu, seperti halnya serangan penolakan layanan terdistribusi, dan juga mengurangi pemadaman sistem dari serangan. *Data localization* membatasi gerakan ini mengamanatkan bahwa salinan data tetap berada dalam yurisdiksi itu sendiri Jadi, setiap penyeimbangan atau pergerakan data harus terjadi di dalamnya jaringan, pada dasarnya mengurangi kekuatan respons jaringan.[29]

III. KESIMPULAN

Indonesia telah melonggarkan ketentuan *data localization* di Indonesia dengan merevisi PP 82/2012 dengan PP 71/2019. *Data Localization* memiliki pro dan kontra, begitu pula membuka penyimpanan data di luar Indonesia. Saat ini Indonesia mewajibkan data *localization* terhadap data publik namun data tersebut juga dapat ditempatkan di luar apabila teknologi penyimpanan tidak tersedia di dalam negeri. Indonesia belum memiliki pengaturan data privasi yang bersifat umum dan mengatur mengatur sanksi yang konkrit atas ketidakpatuhan pada prosedur penyimpanan data. Ketiadaan pengaturan tersebut khususnya terhadap data pribadi di Indonesia membuat tidak efektifnya pengaturan penempatan data. Sehingga RUU PDP perlu untuk segera disahkan. Seperti Australia yang memiliki undang-undang privasi yang kuat serta OAIC yang menjaga privasi dan mengawal hak kebebasan informasi, dengan prinsip-prinsip privasi yang ditata dengan jelas. Uundang – undang perlindungan data pribadi di Indonesia secara fundamental perlu mengatur bahwa data pribadi dapat dipindahkan ke luar Indonesia, tetapi hanya jika yurisdiksi tempat penerima berada setingkat dengan Indonesia dengan tujuan untuk menghindari tindakan proteksionisme dan hambatan berinvestasi, namun tetap menjamin kedaulatan dan keamanan data bagi penduduknya.

Daftar Pustaka

Buku

Black's Law Dictionary, Eight Edition, West Publishing Co, St. Paul, 1999.

Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi: Regulasi dan Konvergensi, (Bandung: PT Refika Aditama, 2010).

Darji Darmodihardjo dan Sidharta, *Pokok-pokok Filsafat Hukum: Apa dan Bagaimana Filsafat Hukum di Indonesia*, (Jakarta: PT Gramedia Pustaka Utama, 2006).

Data & Communications Working Group of the IBA Communication Law Committee, Data Localisation guide: A report on global data isolationism [April – 2019].

Data Localization in a Globalised World, An Indian Perspective - The Dialogue.

Data Localization in India: Questioning the means and ends, Rishab Bailey and Smriti Parsheera

H Jacqueline Brehmer, "Data Localization The Unintended Consequences of Privacy Litigation" American University Washington College of Law, 2018.

Lotte Spreeuwenberg, Justifying a Right to Privacy (Tilburg University: Philosophy, Science and Society 11 October 2016).

Robert L.Hayman Jr, *op.cit.,* hlm 6-8. Lihat pula Austin Chinhengo, *Essential Jurisprudence*, (Great Britain: Cavendish Publishing Limited, 2000).

Scott Confer, Philologia Volume: IX, A Socialist Theory of Privacy in the Internet Age: An Interdisciplinary Analysis.

[29] *Ibid.*

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

Sinta Dewi Rosadi, "Perlidungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia" (Fakultas Hukum: Universitas Padjajaran).

Soerjono Soekanto, Pengantar Penelitian Hukum, Universitas Indonesia Press, (Jakarta, 2015).

Artikel

Data Protection Laws of the World, DLA Piper, (last modified 3 Februari 2020). <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=AU>

Chandra Gian Asmara. *Alasan Menteri Rudiantara Bolehkan Data Center di Luar Negeri.* 30 Oktober 2018 <https://kominfo.go.id/content/detail/15220/alasan-menteri-rudiantara-bolehkan-data-center-di-luar-negeri/0/sorotan_mediadiakses> diakses pada 15 Agustus 2019, Pukul 14.00

Kementerian Komunikasi dan Informatika. *Rudiantara Sebut Data Center Tak Perlu di Indonesia.*<https://kominfo.go.id/content/detail/14742/rudiantara-sebut-data-center-tak-perlu-di-indonesia/0/sorotan_media> diakses pada 1 Oktober 2019, pukul 15.00 WIB.

DLA Piper 'Data Protection Laws of the World" *(last modified 3 February 2020).* <https://www.dlapiperdataprotection.com/index.html?t=law&c=AU>

Cindy Mutia Annur dan Desy Setyowati, "Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman" < https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

Informasi itu disampaikan oleh Samuel Christian Hendrawan melalui akun Twitter-nya @hendralm. <https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

Cindy Mutia Annur dan Desy Setyowati, "Pelanggaran Data Pribadi di Indonesia: Diperdagangkan hingga Ancaman" <https://katadata.co.id/berita/2019/08/02/pelanggaran-data-pribadi-di-indonesia-diperdagangkan-hingga-ancaman>

Data Protection Laws of the World, DLA Piper, (last modified 3 Februari 2020). <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=AU>

ZDNet, "Over 10 Million People Hit in Single Australia Data Breach: OAIC" < https://www.zdnet.com/article/over-10-million-people-hit-in-single-australian-data-breach-oaic/>

Webber (Insurance Services), "Data Breach in Australia for 2018, 2019, and 2020" < https://www.webberinsurance.com.au/data-breaches-list#twenty>

H Jacqueline Brehmer, "Data Localization The Unintended Consequences of Privacy Litigation" American University Washington College of Law, 2018. P. 964 - 968.

Peraturan Perundang-Undangan

Australian Privacy Principles (APP).

Indonesia, Undang – Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58) sebagaimana diubah Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang – Undang Nomor 19 Tahun 2016 (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).

Indonesia, Undang – Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124) sebagaimana diubah dengan Undang – Undang Republik Indonesia Nomor 24

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 2 Nomor 1 (Maret 2022) 363-374
e-ISSN: 2808-9456

Tahun 2013 tentang Aministrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232).

Indonesia, Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185).

Indonesia, Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Lembaran Negara Republik Indonesia Nomor 1829).

Indonesia, Peraturan Otoritas Jasa Keuangan Nomor 69/POJK.05/2016 Tahun 2016 tentang Penyelenggaraan Usaha Perusahaan Asuransi, Perusahaan Asuransi Syariah, Perusahaan Reasuransi, dan Perusahaan Reasuransi Syariah. (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 302) sebagaimana diubah dengan Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 38/POJK.05/2020 Tahun 2020 (Lembaran Negara 2020 Nomor 149).

Information Act 2002 (Northern Territory).

Information Privacy Act 2009 (Queensland).

Information Privacy Act 2014 (Australian Capital Territory).

Personal Information Protection Act 2004 (Tasmania).

Privacy and Data Protection Act 2014 (Victoria).

The Federal Privacy Act 1988 (Cth).

Naskah Akademik RUU Perlindungan Data Pribadi.