KONFLIK YURISDIKSI DALAM ALIH DATA PRIBADI LINTAS NEGARA: ANALISIS HUKUM PERDATA INTERNASIONAL DAN HAK KONSTITUSIONAL ATAS PRIVASI DI INDONESIA

Made Agus Danendra, Fakultas Hukum Universitas Udayana, e-mail: agussdanendraa177@gmail.com
Komang Widiana Purnawan, Fakultas Hukum Universitas Udayana, e-mail: widhianapurnawan@unud.ac.id

DOI: KW.2026.v16.i5.p3

ABSTRAK

Alih data pribadi lintas negara telah menjadi tantangan serius dalam perkembangan hukum di Indonesia seiring meningkatnya penggunaan layanan digital global, termasuk media sosial, *cloud computing*, dan platform komersial lintas batas. Data pribadi warga negara Indonesia diproses di berbagai yurisdiksi secara simultan, sehingga memunculkan persoalan hukum yang tidak dapat diselesaikan hanya melalui pendekatan sektoral atau administratif. Penelitian ini bertujuan menganalisis konflik yurisdiksi dan pilihan hukum dalam transfer data internasional berdasarkan perspektif Hukum Perdata Internasional (HPI), serta mengkaji keterkaitan antara alih data global dan perlindungan hak konstitusional atas privasi sebagaimana dijamin Pasal 28G ayat (1) UUD NRI 1945. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan perundang-undangan, pendekatan kasus, dan pendekatan konseptual, penelitian ini menemukan bahwa UU Perlindungan Data Pribadi (UU PDP) belum menyentuh aspek-aspek fundamental HPI. Ketiadaan aturan mengenai *connecting factor*, *adequacy decision*, *cross-border enforcement*, dan batasan terhadap *choice of law* berbasis kontrak mengakibatkan ketidakpastian hukum dan lemahnya perlindungan privasi warga negara. Penelitian ini menegaskan bahwa pembentukan kerangka HPI digital, harmonisasi dengan standar internasional seperti GDPR, serta penguatan peran negara sebagai penjaga hak privasi merupakan langkah strategis untuk menjamin perlindungan data pribadi secara efektif dan transnasional.
Kata Kunci: Alih Data Pribadi; Hukum Perdata Internasional; Yurisdiksi Digital; Privasi Konstitusional; UU PDP.

ABSTRACT

Cross-border transfer of personal data has become a critical legal challenge in Indonesia due to the growing reliance on global digital platforms, including social media, cloud computing, and cross-border commercial services. Indonesian citizens' personal data are simultaneously processed across multiple jurisdictions, creating legal complexities that cannot be fully addressed through sectoral or administrative approaches alone. This study aims to examine jurisdictional conflicts and choice-of-law issues in international data transfers from the perspective of Private International Law (PIL), and to assess the interaction between global data flows and the constitutional right to privacy guaranteed under Article 28G(1) of the 1945 Constitution. Using a normative legal research method supported by statutory, case-based, and conceptual approaches, this study finds that Indonesia's Personal Data Protection Law (PDP Law) does not adequately regulate fundamental PIL elements. The absence of rules on connecting factors,

adequacy decisions, cross-border enforcement mechanisms, and limitations on contract-based choice of law has resulted in legal uncertainty and insufficient protection of citizens' privacy rights. This study concludes that establishing a comprehensive digital PIL framework, harmonizing domestic regulations with international standards such as the GDPR, and strengthening the role of the state as the guardian of privacy are essential measures to ensure effective and transnational protection of personal data.
Keywords: *Cross-Border Data Transfer; Private International Law;Digital Jurisdiction, Constitutional Privacy;Data Protection Law.*

I. Pendahuluan

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi dalam dua dekade terakhir telah mengubah secara radikal cara negara, masyarakat, dan korporasi global memandang data pribadi. Jika dahulu data diperlakukan sebagai catatan administratif yang bersifat pasif, kini data pribadi telah menjadi komoditas ekonomi, instrumen politik, serta objek hukum lintas negara dengan dampak yang sangat luas.[1] Digitalisasi yang semakin cepat menyebabkan data tidak lagi berada pada ruang geografis yang tetap. Data pribadi warga negara Indonesia dapat dikumpulkan di dalam negeri, diproses di Singapura, disimpan dalam server perusahaan Amerika Serikat, dan dianalisis oleh algoritma milik perusahaan teknologi berbasis Tiongkok.[2]

Transformasi inilah yang kemudian melahirkan fenomena ***"borderless data environment"***, di mana data melintasi yurisdiksi tanpa batas dan tanpa mekanisme kontrol negara. Dalam konfigurasi ini, individu kehilangan kendali terhadap informasi pribadinya, sementara negara menghadapi tantangan serius dalam memperluas jangkauan hukum nasionalnya. Ketika data bergerak, hukum nasional tidak selalu mengikuti.[3]

Pada kenyataannya, hukum Indonesia belum siap menghadapi kompleksitas tersebut. Indonesia tidak memiliki Undang-Undang Hukum Perdata Internasional (HPI**)** yang berfungsi sebagai *lex generalis* bagi seluruh hubungan privat lintas negara. Akibatnya, konflik yurisdiksi yang muncul dari aktivitas pemrosesan data lintas negara tidak memiliki kerangka penyelesaian yang memadai. UU Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022 masih berorientasi domestik-administratif dan belum mengatur isu fundamental HPI seperti *connecting factor*, *choice of forum*, atau *recognition of foreign law*.[4]

Masalah semakin kompleks ketika perusahaan digital global menggunakan klausul kontrak baku (*standard form contract*) yang menetapkan hukum asing sebagai dasar hubungan hukum. Dalam *Terms of Service* Google, Meta, TikTok, dan beberapa penyedia cloud, sering kali tercantum klausul "***Governing Law: California***" atau "***Singapore Law applies***", yang secara faktual mengalihkan yurisdiksi dari Indonesia ke negara lain. Pengguna Indonesia tidak memiliki daya tawar untuk menegosiasikan klausul ini, sehingga hubungan hukum bersifat sepihak.[5] Hal ini menciptakan privatisasi yurisdiksi yang melemahkan kedaulatan hukum nasional.

---

1 Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), 31.

2 Ramli, Afifah. "Cross-Border Data Flows in Southeast Asia." Journal of Asian Law and Policy 12 (2021): 45–67.

3 Paul Schwartz, "Global Data Privacy: The EU Way." NYU Law Review 94 (2019): 771–818.

4 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

5 Google LLC, Terms of Service (California, 2023).

Lebih jauh, terdapat persoalan konstitusional yang tidak dapat diabaikan. Pasal 28G ayat (1) UUD 1945 menegaskan bahwa hak atas perlindungan diri pribadi merupakan hak fundamental warga negara. Putusan Mahkamah Konstitusi juga telah menegaskan bahwa data pribadi termasuk dalam ranah perlindungan konstitusional.[6] Namun ketika data diproses oleh perusahaan asing di luar negeri, negara kehilangan kapasitas untuk menjamin perlindungan hak ini. Dengan kata lain, terdapat jurang antara jaminan konstitusional dan realitas digital global.

Indonesia juga belum memiliki standar "*adequacy*" seperti GDPR yang mensyaratkan bahwa data hanya boleh ditransfer ke negara dengan perlindungan setara. Tanpa standar ini, data warga Indonesia dapat dipindahkan ke negara yang memiliki perlindungan rendah, meningkatkan risiko penyalahgunaan, kebocoran, atau akses ilegal oleh otoritas asing, seperti yang dimungkinkan oleh CLOUD Act Amerika Serikat.[7] Situasi ini membuat perlindungan hak privasi menjadi rapuh dan rentan.

Di sisi lain, perkembangan hukum global menunjukkan adanya pergeseran besar menuju konsep ***digital sovereignty***—negara wajib memastikan bahwa data warganya tetap berada di bawah perlindungan hukum nasional, meskipun diproses di luar negeri. Uni Eropa, India, Tiongkok, dan bahkan Brasil telah membangun rezim hukum yang memberikan yurisdiksi ekstrateritorial pada hukum datanya.[8] Indonesia belum berada pada posisi tersebut. Tanpa adopsi prinsip serupa, Indonesia akan terus menjadi *importer* standar hukum negara lain tanpa kemampuan menegakkan perlindungan data pribadinya sendiri.

Selain itu, literatur mutakhir menunjukkan bahwa data pribadi tidak lagi sekadar isu teknis, melainkan isu geopolitik dan hak asasi manusia. Data dapat digunakan untuk manipulasi perilaku (*behavioral manipulation*), pengaruh politik (political microtargeting), dan eksploitasi ekonomi melalui iklan tertarget.[9] Dalam konteks demikian, alih data lintas negara tidak hanya menimbulkan persoalan yuridis, tetapi juga ancaman terhadap demokrasi dan integritas data nasional.

Oleh sebab itu, urgensi penelitian ini berpijak pada kebutuhan untuk menjembatani keterputusan antara perkembangan teknologi yang sangat cepat dan perkembangan hukum yang lebih lambat. Penelitian ini diperlukan untuk: menganalisis kompleksitas konflik yurisdiksi; mengkaji perlindungan hak privasi dalam konteks ekstrateritorial; merumuskan kerangka HPI digital yang mampu menjawab tantangan global. Dengan demikian, latar belakang masalah penelitian ini tidak hanya mencerminkan kebutuhan akademik, tetapi juga kebutuhan praktis negara dalam melindungi warga negara Indonesia dalam dunia digital yang semakin tanpa batas. Penelitian global menunjukkan bahwa regulasi modern seperti GDPR Uni Eropa telah mengadopsi prinsip: *extraterritoriality adequacy decision data sovereignty enforcement cooperation*

Namun sebagian besar penelitian di Indonesia masih berkisar pada analisis administratif UU PDP tanpa menyentuh aspek HPI lintas negara. Penelitian komparatif oleh beberapa sarjana menunjukkan bahwa negara-negara maju telah mengembangkan doktrin yurisdiksi digital yang memungkinkan penegakan hukum terhadap perusahaan asing, sedangkan Indonesia belum memiliki perangkat hukum setara.[10] tanpa mekanisme yuridis yang jelas Data dapat diakses negara asing melalui

6 Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016.

7 U.S. Congress, CLOUD Act (2018).

8 Anu Bradford, "The Brussels Effect." Northwestern University Law Review 107 (2019): 1–67.

9 Zeynep Tufekci, "Algorithmic Harms," Journal of Digital Ethics 5 (2020): 45–67.

10 European Data Protection Board, Guidelines on International Transfers (2022).

UU seperti CLOUD Act AS. Perusahaan global memonopoli yurisdiksi melalui kontrak baku Pengguna Indonesia terjebak dalam *take it or leave it contract*. UU PDP belum menyediakan mekanisme HPI digital Tidak ada aturan lex datae originis, adequacy, SCC/BCR, atau cross-border enforcement. Karena itu, diperlukan rekonstruksi HPI digital yang melindungi hak privasi konstitusional dan menjamin kepastian hukum dalam ruang digital transnasional. Urgensi penelitian ini berpijak pada kebutuhan untuk menjembatani keterputusan antara perkembangan teknologi yang sangat cepat dan perkembangan hukum yang lebih lambat. Secara metodologis, kajian ini bersandar pada pemikiran Terry Hutchinson yang menekankan pentingnya analisis doktrinal guna menemukan koherensi antara norma nasional dan internasional dalam menjawab tantangan hukum lintas negara[11]. Selain itu, penelitian ini melengkapi pandangan Andri Gunawan Wibisana mengenai ambiguitas tanggung jawab dalam tata kelola digital di Indonesia[12] , serta pemikiran Kadek Agus Sudiarawan yang menegaskan perlunya sinkronisasi nilai keadilan substantif dalam penegakan hukum di era globalisasi[13]. Meskipun penelitian mengenai perlindungan data telah banyak dilakukan, namun sebagian besar masih berkisar pada analisis administratif UU PDP tanpa menyentuh aspek Hukum Perdata Internasional (HPI) secara lintas negara. Dengan demikian, penelitian ini hadir untuk mengisi celah hukum terkait interaksi antara HPI, privasi konstitusional, dan dinamika transfer data global yang belum dibahas secara mendalam dalam literatur terdahulu

1.2. Rumusan Masalah

1. Bagaimana bentuk dan karakter konflik yurisdiksi dalam alih data pribadi lintas negara menurut perspektif HPI?
2. Bagaimana hubungan antara transfer data global dan hak privasi konstitusional?
3. Bagaimana rekonstruksi HPI digital yang ideal untuk Indonesia?

1.3. Tujuan Penelitian

1. Menguraikan konflik yurisdiksi dan konflik norma dalam alih data lintas negara.
2. Menganalisis perlindungan hak privasi dalam konteks global.
3. Merumuskan konsep HPI digital yang dapat diterapkan di Indonesia.

II. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang berfokus pada analisis norma hukum yang berlaku, prinsip-prinsip hukum, dan doktrin akademik untuk menjawab isu hukum yang mengandung unsur lintas negara. Penelitian hukum normatif ini tidak sekadar mengkaji teks perundang-

[11] Terry Hutchinson, "Valuable Free-Range Research: Developing Appropriate Legal Research Methodologies," *Utrecht Law Review* 11, no. 1 (2015): 10-23;

Andri Gunawan Wibisana, "Tanggung Jawab Hukum dalam Pengelolaan Data Digital," *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 112;

Kadek Agus Sudiarawan, "The Future of Digital Law Enforcement in Indonesia," *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45.

[12] Andri Gunawan Wibisana, "Tanggung Jawab Hukum dalam Pengelolaan Data Digital," *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 112;

Kadek Agus Sudiarawan, "The Future of Digital Law Enforcement in Indonesia," *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45.

[13] Kadek Agus Sudiarawan, "The Future of Digital Law Enforcement in Indonesia," *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45.

undangan secara tekstual, melainkan melakukan pendalaman terhadap koherensi norma guna menemukan keadilan substantif. Secara khusus, kerangka metodologi dalam penelitian ini mengacu pada doktrin *doctrinal research* yang dikembangkan oleh Terry Hutchinson, yang menekankan pentingnya interpretasi sistematis untuk menjamin validitas argumentasi hukum dalam isu lintas negara[14]. Pendekatan ini kemudian disinkronkan dengan pemikiran Andri Gunawan Wibisana mengenai perlunya ketajaman analisis terhadap ambiguitas tanggung jawab dalam regulasi sektoral guna menghindari kekosongan hukum[15]. Selain itu, untuk menjawab tantangan penegakan hukum di era global, penelitian ini juga mengadopsi perspektif Kadek Agus Sudiarawan yang menekankan bahwa efektivitas hukum digital sangat bergantung pada sinkronisasi nilai hukum yang berlaku secara transnasional[16] **Pendekatan Perundang-Undangan (*Statute Approach*)** Digunakan untuk menganalisis keterkaitan dan konflik antara: UU Perlindungan Data Pribadi, UUD 1945 (Pasal 28G ayat (1)), GDPR Uni Eropa, PDPA Singapura, dan CLOUD Act Amerika Serikat. Pendekatan ini penting karena konflik yurisdiksi muncul dari ketidakharmonisan regulasi internasional dan nasional.[17] **Pendekatan Kasus *(Case Approach)*** Melibatkan studi atas kasus-kasus kebocoran data besar seperti: Kasus Tokopedia (2020), Kasus BPJS Kesehatan (2021), Kebocoran data Indihome (2022), Penggunaan data oleh platform global seperti Meta dan TikTok. Melalui pendekatan ini, dapat dilihat pola bagaimana yurisdiksi asing mengungguli yurisdiksi nasional.[18] **Pendekatan Konseptual (*Conceptual Approach*)** Menggunakan teori-teori HPI klasik dan modern sebagai dasar untuk menganalisis dan merumuskan rekonstruksi hukum: *Teori connecting factor Savigny Doctrine of proper law of the contract Extraterritoriality (GDPR) Adequacy decision Digital sovereignty* Pendekatan ini digunakan untuk membangun paradigma hukum baru dalam perlindungan data lintas negara.[19] **Jenis dan Sumber Bahan Hukum** Primer: UUD 1945, UU PDP, GDPR, CLOUD Act, PDPA Singapura, Sekunder: Buku teori HPI, jurnal internasional, artikel privasi digital, Tersier: Kamus hukum, ensiklopedia hukum, laporan internasional OECD/EDPB

III. Hasil dan Pembahasan

Alih data pribadi lintas negara memperkenalkan tipe konflik yurisdiksi yang tidak dikenal dalam Hukum Perdata Internasional (HPI) klasik. Pada masa Savigny, penentuan hukum yang berlaku masih sangat bergantung pada *seat of the legal relationship* yang dapat ditentukan melalui faktor-faktor teritorial tertentu. Namun pada era digital, data pribadi tidak memiliki lokasi tetap (*placeless data*), sehingga prinsip *lex situs* atau *lex loci actus* menjadi tidak memadai.[20]

Data pribadi bergerak melintasi server yang tersebar di banyak negara tanpa campur tangan pengguna. Ketika seorang warga Indonesia menggunakan layanan TikTok atau Google Photos, datanya dapat dikumpulkan di Indonesia, diproses di Singapura, disimpan di Amerika Serikat, dan dianalisis di pusat data berbasis

[14] Terry Hutchinson, "Valuable Free-Range Research: Developing Appropriate Legal Research Methodologies," *Utrecht Law Review* 11, no. 1 (2015): 10-23

[15] Andri Gunawan Wibisana, "Tanggung Jawab Hukum dalam Pengelolaan Data Digital," *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 112

[16] Kadek Agus Sudiarawan, "The Future of Digital Law Enforcement in Indonesia," *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45.

[17] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

[18] Tempo Magazine, Investigasi Kebocoran Data Tokopedia (2020).

[19] Friedrich Carl von Savigny, Private International Law (1869).

[20] Savigny, Private International Law (1869), 44.

Tiongkok.[21] Dalam situasi multi-yurisdiksi seperti ini, tidak satu pun negara dapat mengklaim yurisdiksi absolut. Yang muncul justru adalah *overlapping jurisdiction*—setiap negara yang bersentuhan dengan aliran data memiliki klaim kewenangan masing-masing.

Lebih jauh, konflik yurisdiksi juga muncul akibat sifat hubungan kontraktual yang asimetris antara pengguna dan platform digital. Perusahaan global menggunakan perjanjian baku dengan klausul *choice of law* sepihak seperti ***"This Agreement is governed by California Law"*** *atau* ***"Singapore Law shall apply"***. Pengguna Indonesia tidak memiliki peluang negosiasi, sehingga secara faktual tunduk pada yurisdiksi asing.[22] Prinsip *party autonomy* dalam HPI menjadi tidak relevan ketika kontrak disusun oleh satu pihak (platform) dan diterima secara pasif oleh pihak lain (pengguna), tanpa proses kesepakatan substantif.

Konflik semakin tajam karena perbedaan standar perlindungan data antarnegara. GDPR Uni Eropa menerapkan prinsip ketat mengenai *extraterritorial jurisdiction*, yang memberikan hak kepada warga UE meskipun datanya diproses di luar wilayah Eropa. Sebaliknya, Amerika Serikat menganut model perlindungan berbasis kepentingan bisnis, sehingga akses pemerintah terhadap data perusahaan dapat dilakukan melalui CLOUD Act.[23] Singapura menerapkan PDPA yang bersifat moderat. Sementara Indonesia, melalui UU PDP, masih mengedepankan mekanisme administratif yang belum mencakup norma pilihan hukum internasional.

Akibatnya, pengguna Indonesia menghadapi situasi ketidakpastian hukum yang serius. Data mereka dapat diakses oleh negara asing, tunduk pada hukum asing, dan dilindungi oleh standar hukum yang berbeda, tanpa mekanisme kontrol dari negara asal data.

3.1.1. Konflik Norma dan Potensi Pelanggaran Hak Konstitusional atas Privasi[24]

Secara konstitusional, perlindungan data pribadi di Indonesia berakar pada Pasal 28G ayat (1) UUD 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda[25]. Namun, harus diakui bahwa pengaturan hak privasi dalam konstitusi Indonesia masih bersifat implisit dan sangat umum. Hal ini berkaitan erat dengan karakteristik UUD 1945 sebagai konstitusi yang bersifat rigid (kaku), di mana norma-norma yang terkandung di dalamnya hanya meletakkan prinsip-prinsip dasar (*fundamental principles*) tanpa rincian operasional yang mendetail[26]. Sifat kaku ini bertujuan untuk menjaga stabilitas nilai dasar negara, namun di sisi lain menciptakan tantangan dalam merespons kecepatan transformasi digital yang memerlukan perlindungan teknis spesifik.

Ketertinggalan regulasi ini semakin nyata jika dibandingkan dengan dinamika hukum internasional. Di Uni Eropa, perlindungan data telah bertransformasi menjadi hak asasi yang sangat eksplisit melalui ***General Data Protection Regulation*** **(GDPR)**, sementara dalam ranah *soft law* internasional, instrumen seperti ***Tallinn Manual*** telah memberikan panduan detail mengenai kedaulatan negara dan batas-batas intervensi di

[21] Zuboff, Age of Surveillance Capitalism (2019), 33.
[22] Google LLC, Terms of Service (2023).
[23] U.S. CLOUD Act (2018).
[24] Putusan MK No. 20/PUU-XIV/2016.
[25] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Ps. 28G ayat (1).
[26] Jimly Asshiddiqie, *Konstitusi dan Konsep Negara Hukum* (Jakarta: Rajawali Pers, 2009), h. 88.

European Data Protection Board, *Guidelines on International Transfers* (2022);

ruang siber[27]. Oleh karena itu, Indonesia memerlukan rekonstruksi hukum yang mampu menerjemahkan hak privasi yang bersifat implisit dalam konstitusi menjadi instrumen perlindungan yang konkret dan ekstrateritorial guna menghadapi fenomena alih data lintas negara."

Konflik yurisdiksi dalam transfer data lintas negara tidak hanya memunculkan ketegangan antarnegara, tetapi juga menimbulkan konflik konstitusional, terutama terkait hak privasi. Pasal 28G ayat (1) UUD 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi. Mahkamah Konstitusi telah menegaskan bahwa data pribadi merupakan bagian dari hak privasi yang tidak dapat dikurangi oleh tindakan sewenang-wenang, termasuk oleh korporasi swasta. Ketika data warga Indonesia diproses di luar negeri, negara kehilangan kemampuan untuk menjalankan kewajiban konstitusionalnya dalam melindungi hak privasi. Perusahaan global sering mengalihkan data ke yurisdiksi dengan standar perlindungan rendah demi efisiensi biaya. Dalam kondisi ini, pengguna Indonesia dapat mengalami pelanggaran privasi, seperti: Karena Indonesia tidak memiliki *extraterritorial enforcement*, korban tidak memiliki forum penyelesaian sengketa yang jelas. Hak privasi dalam konstitusi akhirnya menjadi hak yang tidak memiliki mekanisme perlindungan efektif. UU PDP belum memberi mekanisme penegakan hukum lintas negara. Tidak ada kewajiban bagi perusahaan asing untuk tunduk pada standar privasi Indonesia ketika memproses data di yurisdiksi lain. Tidak ada pasal mengenai *adequacy decision*, *binding corporate rules*, atau *standard contractual clauses* seperti yang diatur GDPR.[28] Dengan demikian, terdapat ketidakseimbangan antara hak konstitusional dan realitas digital transnasional.

3.1.2 Rekonstruksi HPI Digital untuk Mengisi Kekosongan Hukum Nasional

Untuk mengatasi konflik yurisdiksi, Indonesia memerlukan UU HPI Digital yang berfungsi sebagai lex generalis bagi seluruh peristiwa hukum lintas negara, termasuk alih data pribadi. Tanpa UU HPI, persoalan lintas batas tidak dapat diselesaikan melalui UU sektoral seperti UU PDP, UU ITE, atau KUHPerdata karena semuanya bersifat domestik dan tidak memiliki kekuatan ekstrateritorial. Kelemahan mendasar dari regulasi saat ini terletak pada ketergantungan terhadap undang-undang sektoral seperti UU PDP, UU ITE, dan KUHPerdata yang bersifat domestik sehingga tidak memiliki kekuatan ekstrateritorial dalam menghadapi dinamika digital global. Sebagai solusinya, Indonesia memerlukan rekonstruksi HPI Digital yang komprehensif melalui adopsi beberapa konsep fundamental. Pertama, penerapan prinsip *lex datae originis* yang menjamin bahwa setiap data pribadi warga negara Indonesia, di manapun diproses, wajib tunduk pada standar perlindungan nasional sebagaimana doktrin *data subject jurisdiction* yang berlaku dalam GDPR[29]. Kedua, diperlukan pengaturan tegas terhadap klausul pilihan hukum yang menyatakan bahwa setiap kesepakatan yang menyingkirkan hak privasi konstitusional adalah tidak sah dan tidak mengikat secara hukum. Ketiga, Indonesia harus menetapkan *adequacy standard* guna mengklasifikasikan negara-negara yang dianggap aman untuk menerima alih data berdasarkan standar privasi yang setara. Keempat, rekonstruksi ini harus mencakup mekanisme *cross-border enforcement* yang memungkinkan adanya kerja sama antar-regulator, pengakuan putusan administratif asing, serta kemampuan melakukan

[27] Michael N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

[28] GDPR, EU Regulation 2016/679.

[29] European Data Protection Board, *Guidelines on Territorial Scope* (2020).

penyelidikan lintas negara[30]. Sebagai pilar penutup, pembentukan Otoritas Perlindungan Data Independen menjadi syarat mutlak untuk menjalankan fungsi pengawasan, penuntutan, dan negosiasi perjanjian data internasional guna menjaga kedaulatan digital dan melindungi kepentingan warga negara di ruang siber transnasional[31].

3.1.3. Negara sebagai Penjaga Hak Privasi (*Guardian of Privacy)*

Dalam konteks rezim Hukum HAM Internasional, hingga saat ini belum terdapat sebuah instrumen hukum global tunggal yang bersifat mengikat secara universal khusus mengenai hak privasi digital. Namun, perlindungan hak privasi telah diakui secara fundamental dalam Pasal 17 *International Covenant on Civil and Political Rights* (ICCPR) yang melarang interferensi sewenang-wenang terhadap privasi seseorang[32]. Di tingkat regional, Uni Eropa telah memelopori standar emas melalui GDPR yang memiliki dampak ekstrateritorial secara global, sementara dalam ranah *soft law* internasional, *Tallinn Manual* telah memberikan kerangka interpretatif mengenai bagaimana hukum internasional dan hak asasi manusia diaplikasikan dalam operasi siber dan ruang digital[33]. Keberadaan instrumen-instrumen ini menunjukkan adanya pergeseran global untuk menempatkan privasi bukan sekadar sebagai hak administratif, melainkan sebagai hak asasi manusia yang harus dilindungi melampaui batas-batas yurisdiksi negara[34].

Namun tanpa kerangka hukum lintas negara, negara tidak dapat melindungi data pribadi yang diproses di luar negeri. Dalam upaya menjalankan kewajiban konstitusional untuk menghormati, melindungi, dan memenuhi hak privasi warga negara, negara tidak dapat lagi sekadar mengandalkan instrumen hukum yang bersifat pasif. Transformasi peran negara sebagai *guardian of privacy* di era digital menuntut serangkaian langkah strategis dan proaktif. Hal ini harus diwujudkan melalui pembentukan Undang-Undang HPI Digital sebagai *lex generalis* yang memberikan kepastian hukum dalam peristiwa lintas batas, yang dibarengi dengan penguatan substansi UU PDP agar lebih responsif terhadap dinamika teknologi[35]. Selain itu, negara memiliki tanggung jawab intervensi untuk membatasi dominasi kontrak baku yang selama ini sering kali memaksakan pilihan hukum asing secara sepihak kepada pengguna di Indonesia. Langkah tersebut perlu diperluas ke ranah internasional dengan menjalin kerja sama bilateral yang spesifik terkait perlindungan data guna mempermudah penegakan hukum lintas yurisdiksi. Pada akhirnya, seluruh upaya regulasi tersebut harus bermuara pada komitmen negara untuk membangun kesadaran kedaulatan digital secara kolektif[36]. Dengan integrasi kebijakan ini, negara tidak hanya hadir sebagai regulator administratif, tetapi juga sebagai pelindung

[30] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2019).

[31] Christopher Kuner, "Data Protection, the GDPR, and the Internet," *International Data Privacy Law* 8, no. 1 (2018): 1-15.

[32] International Covenant on Civil and Political Rights (ICCPR), Art. 17.

[33] Michael N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017).

[34] Jimly Asshiddiqie, Konstitusi dan Konsep Negara Hukum (Jakarta: Rajawali Pers, 2009).

[35] Andri Gunawan Wibisana, "Tanggung Jawab Hukum dalam Pengelolaan Data Digital," *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 112.

[36] Kadek Agus Sudiarawan, "The Future of Digital Law Enforcement in Indonesia," *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45.

kedaulatan identitas digital warganya di tengah arus globalisasi data yang tanpa batas[37]. Upaya tersebut menjadi syarat utama keberhasilan negara dalam melindungi identitas digital warganya.

3.2 Mekanisme Pengawasan dan Penegakan Hukum Lintas Batas dalam Transfer Data Pribadi

Salah satu kelemahan terbesar sistem perlindungan data pribadi Indonesia adalah tidak adanya mekanisme penegakan hukum lintas batas (*cross-border enforcement*). Dalam ekosistem digital berbasis jasa global, sebagian besar perusahaan yang memproses data warga negara Indonesia beroperasi di luar wilayah hukum Indonesia. Ketika terjadi pelanggaran data, kebocoran, atau penyalahgunaan, negara seringkali tidak memiliki kewenangan maupun kemampuan teknis untuk menegakkan hukum terhadap pelaku yang berdomisili di yurisdiksi asing.[38]

Hal ini terjadi karena pemrosesan data bersifat *offshore*, kontrak baku memilih hukum asing, dan negara tujuan data memiliki standar perlindungan yang tidak selalu sejalan dengan kepentingan hukum Indonesia. Tanpa mekanisme penegakan lintas batas, hak privasi sebagai hak konstitusional menjadi tidak efektif dan hanya bersifat deklaratif. Oleh karena itu, negara perlu membangun arsitektur penegakan hukum transnasional yang mampu menjawab tiga tantangan utama: (1) lokasi pelaku yang berada di luar negeri, (2) tidak adanya kewajiban kepatuhan hukum Indonesia bagi perusahaan asing, dan (3) ketidakmampuan aparat nasional mengakses bukti digital lintas negara.[39]

3.2.1 *Mutual Recognition and Cross-Border Enforcement*

Sistem mutual recognition merupakan mekanisme paling umum yang digunakan dalam kerja sama internasional. Dalam konteks data pribadi, mutual recognition terjadi ketika suatu negara mengakui standar perlindungan privasi negara lain sebagai setara. GDPR menerapkan prinsip "adequacy decision" untuk menentukan negara mana yang dianggap aman.[40] Indonesia belum memiliki mekanisme serupa. Tanpa itu, negara lain tidak berkewajiban mematuhi ketentuan UU PDP, dan putusan administratif Indonesia tidak memiliki kekuatan hukum di luar yurisdiksi nasional. Membangun perjanjian dua pihak (bilateral agreements) atau perjanjian kawasan akan memungkinkan Indonesia mengeksekusi putusan administratif atau sanksi terhadap entitas asing yang memproses data rakyat Indonesia. Dalam lingkup ASEAN, mekanisme ini dapat diselaraskan dengan ASEAN Data Management Framework sebagai bagian dari integrasi ekonomi digital kawasan.[41] Kedaulatan digital Indonesia tidak dapat dilepaskan dari dinamika di Asia Tenggara. **Afifah Ramli** menyoroti bahwa aliran data lintas batas di ASEAN memerlukan mekanisme kolaboratif yang mampu menjembatani perbedaan standar perlindungan data antar-negara anggota. Indonesia perlu melakukan interoperabilitas dengan *ASEAN Data Management Framework* untuk memastikan kedaulatan data nasional tetap terjaga tanpa menghambat integrasi ekonomi digital kawasan. Hal ini krusial mengingat negara tetangga seperti Singapura melalui PDPA telah memiliki

37 Jimly Asshiddiqie, Konstitusi dan Konsep Negara Hukum (Jakarta: Rajawali Pers, 2009), h. 92.
38 Syafrinaldi, HPI Globalisasi (2019), 133.
39 Huala Adolf, Sengketa Internasional (2019), 88.
40 GDPR, EU Regulation 2016/679.
41 ASEAN Secretariat, Digital Masterplan 2025 (2021).

panduan alih data yang lebih moderat namun tetap protektif terhadap kepentingan subjek data.

3.2.2. Mutual Legal Assistance (MLA) dalam penyidikan digital

Hukum internasional telah lama mengenal *Mutual Legal Assistance Treaties (MLATs)* untuk membantu penyidikan lintas batas. Namun MLA tradisional biasanya terbatas pada kasus pidana, sedangkan kasus perlindungan data seringkali bersifat administratif atau keperdataan. Indonesia perlu mendorong pembentukan MLA versi digital—Digital MLA (D-MLA)—yang memungkinkan:

permintaan data log, metadata, atau audit trail kepada negara lain;

1. penyitaan bukti digital yang berada di pusat data luar negeri;
2. investigasi bersama dengan otoritas perlindungan data asing;
3. pengungkapan pelanggaran data oleh perusahaan global.[42]

Tanpa MLA digital, penyidikan kasus kebocoran data seperti BPJS dan Tokopedia akan selalu terhambat.

3.2.3 Harmonisasi Mekanisme Investigasi dan Sanksi Lintas Negara

Negara-negara Eropa telah mengembangkan mekanisme kolaboratif antar-otoritas perlindungan data melalui lembaga seperti European Data Protection Board (EDPB). Mekanisme ini memungkinkan koordinasi investigasi dan harmonisasi sanksi terhadap pelanggaran privasi lintas negara.[43]

Indonesia belum memiliki mekanisme serupa. UU PDP mengatur pembentukan otoritas perlindungan data, tetapi tidak memberikan kewenangan melakukan investigasi lintas wilayah, apalagi memberi akses ke pusat data di luar negeri. Untuk itu, Indonesia perlu:

1. menetapkan prosedur joint investigation;
2. membangun protokol cross-border penalty execution;
3. mensyaratkan perusahaan asing menunjuk local representative di Indonesia sebagai titik kontak yuridis;
4. menetapkan kewajiban audit privasi reguler untuk perusahaan yang mengirim data ke luar negeri.[44]
5.

3.2.4.Penyelesaian Sengketa Digital Lintas Negara

Salah satu kelemahan terbesar dalam transfer data adalah tidak adanya forum penyelesaian sengketa yang dapat diakses korban. Klausul baku *choice of forum* biasanya menunjuk pengadilan atau *arbitrase* asing. Untuk melindungi warga negara, Indonesia perlu menetapkan: *Digital Dispute Resolution Mechanism (DDRM)* yaitu forum sengketa nasional untuk kasus pelanggaran data internasional; Arbitrase Privasi Digital bekerja sama dengan negara lain dan organisasi internasional; Model Ombudsman Data Pribadi sebagai badan mediasi non-litigasi. Negara-negara seperti Inggris dan Kanada telah mengembangkan model data ombudsman dengan kewenangan luas untuk menangani sengketa privasi lintas batas.[45]

Pengawasan lintas batas tidak dapat dilakukan oleh hukum nasional saja. Dibutuhkan strategi diplomasi digital jangka panjang yang melibatkan: penyusunan perjanjian internasional tentang pertukaran data; membangun posisi Indonesia dalam pembentukan standar ASEAN; memperkuat kedaulatan data sebagai bagian dari keamanan nasional; mendorong interoperabilitas dengan GDPR sehingga Indonesia diakui sebagai "adequate jurisdiction". Dengan langkah strategis ini, Indonesia dapat

[42] OECD, Cross-Border Cooperation in Digital Enforcement (2020).
[43] EDPB, Guidelines on Cooperation Mechanisms (2022).
[44] PDPC Singapore, Cross-Border Data Transfer Guidelines (2021).
[45] UK ICO, Cross-Border Enforcement Framework (2020).

keluar dari posisi ketergantungan pada perusahaan global dan mulai membangun ekosistem hukum digital yang memadai untuk melindungi warga negara dalam konteks global.

IV. Kesimpulan sebagai Penutup

4. Kesimpulan

Penelitian ini menunjukkan bahwa alih data pribadi lintas negara telah menciptakan konfigurasi baru hubungan hukum yang tidak dapat dijelaskan oleh kerangka hukum nasional maupun teori Hukum Perdata Internasional (HPI) klasik secara memadai. Karakter data pribadi yang tidak berlokasi tetap, bergerak lintas batas secara otomatis, dan diproses oleh banyak aktor internasional sekaligus menyebabkan munculnya konflik yurisdiksi yang bersifat kompleks, berlapis, dan multidimensional. Konflik ini tidak hanya terjadi antara negara asal data dan negara tempat data diproses, tetapi juga melibatkan yurisdiksi negara domisili korporasi global yang memanfaatkan posisi dominannya untuk menetapkan hukum dan forum penyelesaian sengketa secara sepihak. Hasil penelitian memperlihatkan bahwa UU Perlindungan Data Pribadi (UU PDP) belum mampu mengatasi persoalan lintas negara ini. UU PDP masih bersifat administratif dan tidak menyediakan norma fundamental yang dibutuhkan dalam HPI, seperti *connecting factor*, batasan terhadap *choice of law*, mekanisme *adequacy decision*, atau prosedur *cross-border enforcement*. Ketidakadaan Undang-Undang HPI di Indonesia semakin memperbesar kekosongan hukum, karena negara tidak memiliki kerangka normatif untuk menentukan hukum mana yang berlaku, negara mana yang berwenang, dan bagaimana putusan dapat dieksekusi ketika data diproses di luar negeri. Dalam konteks perlindungan hak konstitusional atas privasi, penelitian ini menegaskan bahwa negara memiliki kewajiban konstitusional untuk melindungi data pribadi warganya tanpa batas teritorial. Namun tanpa kerangka hukum yang memberikan kewenangan lintas negara, negara tidak dapat menjamin perlindungan hak privasi warga negara ketika data mereka berada di yurisdiksi asing. Dengan demikian, perlindungan hak privasi dalam ruang digital masih bersifat deklaratif dan belum diikuti dengan mekanisme operasional yang memadai. Rekonstruksi hukum menjadi kebutuhan mendesak. Pengembangan HPI digital Indonesia harus memuat prinsip *lex datae originis*, yurisdiksi digital berbasis subjek data, standar *adequacy*, mekanisme pengakuan hukum asing, serta tata cara penegakan lintas negara. Harmonisasi UU PDP dengan standar internasional seperti GDPR dan penerapan prinsip-prinsip konstitusional atas privasi merupakan langkah strategis untuk memperkuat posisi Indonesia dalam ekosistem digital global. Negara juga perlu memperkuat peran otoritas perlindungan data pribadi dan membangun kerja sama internasional dalam pertukaran data dan penyelesaian sengketa.Dengan demikian, penelitian ini menyimpulkan bahwa perlindungan data pribadi lintas negara hanya dapat dicapai melalui integrasi antara HPI digital, UU PDP yang diperkuat, dan penegasan peran negara sebagai penjaga hak privasi. Tanpa reformasi hukum yang komprehensif, warga negara Indonesia akan terus berada pada posisi rentan dalam menghadapi perusahaan global yang memproses data lintas yurisdiksi.

DAFTAR PUSTAKA

A. Buku

Asshiddiqie, Jimly. *Konstitusi dan Konsep Negara Hukum*. Jakarta: Rajawali Pers, 2009.

Dicey, A.V., dan J.H.C. Morris. *The Conflict of Laws*. Edisi ke-15. London: Sweet & Maxwell, 2012. North, Peter, dan James Fawcett. *Cheshire and North's Private International Law*. Edisi ke-14. Oxford: Oxford University Press, 2008. Savigny,

Friedrich Carl von. *Private International Law and the Retrospective Operation of Statutes*. London: T. & T. Clark, 1869.
Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. Z
uboff, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2019.

B. Jurnal Ilmiah

Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107, no. 1 (2019): 1-67.
Cohen, Julie E. "Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20, no. 1 (2019): 1-32.
De Hert, Paul, dan Vagelis Papakonstantinou. "The New General Data Protection Regulation: A Critical Review." *Computer Law & Security Review* 34 (2018): 119-124.
Greenleaf, Graham. "Global Data Privacy Laws 2023: Strengthening of Privacy Principles." *Privacy Laws & Business International Report* 180 (2023): 1-12.
Hutchinson, Terry. "Valuable Free-Range Research: Developing Appropriate Legal Research Methodologies." *Utrecht Law Review* 11, no. 1 (2015): 10-23.
Kuner, Christopher. "Data Protection, the GDPR, and the Internet." *International Data Privacy Law* 8, no. 1 (2018): 1-15.
Lin, Frederick. "Data Localization Laws in Asia: Comparative Trends." *Asian Journal of Comparative Law* 17, no. 2 (2022): 22-48.
Meltzer, Joshua. "Digital Trade, Data Flows, and Privacy Protection." *Brookings Working Paper* (2020): 1-43.
Ramli, Afifah. "Cross-Border Data Flows in Southeast Asia." *Journal of Asian Law and Policy* 12, no. 2 (2021): 45-67.
Schwartz, Paul. "Global Data Privacy: The EU Way." *NYU Law Review* 94 (2019): 771-818. Sudiarawan,
Kadek Agus. "The Future of Digital Law Enforcement in Indonesia." *Substantive Justice International Journal of Law* 3, no. 1 (2020): 45-60.
Tufekci, Zeynep. "Algorithmic Harms in a Datafied Society." *Journal of Digital Ethics* 5, no. 1 (2020): 45-67.
Wibisana, Andri Gunawan. "Tanggung Jawab Hukum dalam Pengelolaan Data Digital." *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 112-130.

C. Peraturan Perundang-undangan & Dokumen Internasional

ASEAN Secretariat. ASEAN Digital Masterplan 2025. Jakarta:
ASEAN, 2021. European Data Protection Board. Guidelines on International Transfers. 2022.
European Union. General Data Protection Regulation (EU) 2016/679 (GDPR). OECD.
Cross-Border Cooperation in Digital Enforcement. Paris: OECD Publishing, 2020. Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
Republic of Singapore. Personal Data Protection Act (PDPA).
U.S. Congress. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). 2018.

D. Sumber Daring Resmi

Google LLC. “Terms of Service.” 2023. https://policies.google.com/terms. Meta Platforms Inc. “Data Policy.” 2023. https://www.facebook.com/policy. TikTok Global. “Privacy Policy.” 2023. https://www.tiktok.com/legal/page