**Al-Zayn: Jurnal Ilmu Sosial & Hukum** e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.5760

# Kepastian Hukum dalam Transfer Data Lintas Negara: Tinjauan Terhadap Undang-Undang Perlindungan Data Pribadi di Indonesia

**Ari Andy Prastowo[1], Angga Faridi Algamar[2], Grace Yustisia Siahaan[3]**
Fakultas Hukum, Universitas Pelita Harapan Jakarta, Indonesia[1-3]
*Email Korespondensi: ariandyprastowo@gmail.com, a80angga@gmail.com, grace.siahaan@aol.com*

*Article received: 01 Januari 2026, Review process: 12 Januari 2026*
*Article Accepted: 22 Februari 2026, Article published: 28 April 2026*

***ABSTRACT***
*The rapid growth of the global digital economy has significantly increased the practice of cross-border data transfer, raising complex legal challenges, particularly in relation to personal data protection and legal certainty. This study aims to analyze the level of legal certainty in cross-border data transfer practices in Indonesia under Law Number 27 of 2022 on Personal Data Protection, as well as to identify the legal challenges arising from its implementation. This research employs a normative legal method using statutory and comparative approaches, relying on secondary data obtained through library research. The findings indicate that, at the normative level, the Law Number 27 of 2022 on Personal Data Protection has adopted global principles and mechanisms aligned with international standards, particularly through the framework of adequacy, safeguards, and consent as recognized in the European Union's data protection regime. However, in practice, several significant challenges remain, including the absence of comprehensive implementing regulations, unclear criteria for assessing the adequacy of data protection in recipient countries, the lack of operational instruments such as standard contractual clauses and binding corporate rules, and the incomplete establishment of an independent supervisory authority. Furthermore, regulatory fragmentation across sectors and jurisdictional limitations in cross-border enforcement contribute to legal uncertainty. Although Indonesia has moved in line with global trends, further strengthening in regulatory frameworks, institutional capacity, and implementation mechanisms is necessary to ensure effective legal certainty in cross-border data transfer practices.*
***Keywords:*** *Cross-Border Data Transfer; Personal Data Protection; PDP Law.*

***ABSTRAK***
*Perkembangan ekonomi digital global telah mendorong meningkatnya praktik cross border data transfer yang menimbulkan tantangan hukum, khususnya dalam aspek perlindungan data pribadi dan kepastian hukum. Penelitian ini bertujuan untuk menganalisis kepastian hukum dalam pelaksanaan transfer data lintas negara di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta mengidentifikasi berbagai tantangan hukum yang dihadapi dalam implementasinya. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan komparatif, serta memanfaatkan data sekunder yang diperoleh melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa secara normatif, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengadopsi prinsip dan mekanisme global yang sejalan dengan standar internasional, khususnya melalui pendekatan adequacy, safeguards, dan consent sebagaimana dikenal dalam rezim perlindungan data Uni*

 

*Eropa. Namun demikian, dalam praktiknya masih terdapat sejumlah kendala yang signifikan, antara lain belum lengkapnya peraturan pelaksana, belum jelasnya kriteria penilaian tingkat kesetaraan pelindungan data, belum tersedianya instrumen operasional seperti standard contractual clauses dan binding corporate rules, serta belum berfungsinya secara optimal otoritas pengawas independen. Selain itu, fragmentasi regulasi sektoral dan keterbatasan yurisdiksi dalam penegakan hukum lintas negara turut memperkuat ketidakpastian hukum. Meskipun Indonesia telah berada pada jalur yang selaras dengan tren global, diperlukan penguatan dalam aspek regulasi turunan, kelembagaan, serta implementasi untuk mewujudkan kepastian hukum yang efektif dalam transfer data lintas negara.*
***Kata Kunci:*** *Cross-Border Data Transfer; Perlindungan Data Pribadi; Undang-Undang PDP.*

## PENDAHULUAN

Transformasi digital yang berkembang secara eksponensial dalam beberapa dekade terakhir telah mengubah struktur dan dinamika masyarakat global secara fundamental (Ramli, 2004). Revolusi teknologi informasi tidak hanya mempengaruhi pola komunikasi, tetapi juga membentuk ulang sistem ekonomi, tata kelola pemerintahan, serta interaksi sosial. Data telah mengalami pergeseran makna yang signifikan, dari sekadar informasi menjadi komoditas strategis yang memiliki nilai ekonomi tinggi, bahkan sering disebut sebagai "*the new oil*" dalam ekonomi digital (Matheus & Gunadi, 2024). Data menjadi fondasi utama dalam pengambilan keputusan berbasis analitik, pengembangan kecerdasan buatan (*artificial intelligence*), serta inovasi berbagai layanan digital.

Seiring dengan meningkatnya ketergantungan terhadap data, arus pertukaran data lintas negara (*cross border data transfer*) menjadi fenomena yang tidak terpisahkan dari ekosistem digital global. Aktivitas ini mencakup pemindahan data pribadi maupun non-pribadi dari satu yurisdiksi ke yurisdiksi lain, baik untuk tujuan komersial, administratif, maupun teknis. Perusahaan-perusahaan multinasional, penyedia layanan digital, hingga institusi pemerintah secara rutin melakukan transfer data lintas negara dalam rangka menunjang operasional dan efisiensi sistem mereka. Infrastruktur digital seperti *cloud computing*, pusat data global (*data centers*), dan jaringan internet berkecepatan tinggi semakin mempercepat dan mempermudah proses tersebut (Liat & Wahyuningtyas, 2025).

Namun demikian, kemudahan dalam melakukan transfer data lintas negara tidak serta-merta diikuti dengan kesiapan kerangka hukum yang memadai. Perbedaan sistem hukum, standar perlindungan data, serta kepentingan nasional masing-masing negara menimbulkan kompleksitas yang signifikan dalam pengaturan *cross border data transfer*. Beberapa kasus data pribadi warga suatu negara dapat diproses atau disimpan di negara lain yang memiliki tingkat perlindungan hukum yang berbeda, bahkan lebih rendah. Kondisi ini menimbulkan potensi risiko yang serius, termasuk kebocoran data, penyalahgunaan informasi pribadi, pelanggaran hak privasi, hingga ancaman terhadap keamanan nasional.

Perlindungan data pribadi merupakan bagian integral dari hak atas privasi yang dijamin dalam berbagai instrumen hukum internasional maupun nasional. Hak atas privasi tidak hanya mencakup perlindungan terhadap kehidupan pribadi

 

individu, tetapi juga kontrol atas informasi pribadi yang dimilikinya (Mahdi & Triadi, 2025). Setiap bentuk pengolahan data, termasuk transfer lintas negara, harus dilakukan dengan memperhatikan prinsip-prinsip perlindungan data yang ketat, seperti persetujuan (*consent*), tujuan yang jelas (*purpose limitation*), serta keamanan data (*data security*) (Agusta, 2021).

Indonesia sebagai negara dengan populasi besar dan tingkat penetrasi internet yang terus meningkat menghadapi tantangan yang tidak kecil dalam mengatur praktik *cross border data transfer*. Pertumbuhan pesat sektor ekonomi digital di Indonesia, yang didorong oleh perkembangan *e-commerce*, *fintech*, *ride-hailing*, serta layanan berbasis aplikasi lainnya, telah meningkatkan volume pengumpulan dan pemrosesan data pribadi secara signifikan. Praktiknya banyak pelaku usaha digital di Indonesia yang menggunakan infrastruktur global untuk menyimpan dan mengelola data, sehingga transfer data ke luar negeri menjadi suatu keniscayaan.

Sebelum diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ("UU PDP"), pengaturan mengenai data pribadi di Indonesia bersifat fragmentaris dan sektoral. Beberapa ketentuan mengenai perlindungan data tersebar dalam berbagai regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik, peraturan di sektor perbankan, telekomunikasi, serta kesehatan. Namun, ketiadaan regulasi yang komprehensif dan terintegrasi menyebabkan adanya kekosongan norma dan ketidakpastian hukum, khususnya dalam mengatur transfer data lintas negara.

Disahkannya UU PDP menjadi tonggak penting dalam pembangunan rezim perlindungan data pribadi di Indonesia. Undang-undang ini mengadopsi berbagai prinsip perlindungan data yang diakui secara internasional, serta mengatur secara lebih sistematis mengenai hak dan kewajiban para pihak dalam pengolahan data pribadi. UU PDP menetapkan bahwa transfer data pribadi ke luar negeri hanya dapat dilakukan apabila negara tujuan memiliki tingkat perlindungan data yang setara atau lebih tinggi, atau apabila terdapat jaminan perlindungan yang memadai, atau berdasarkan persetujuan dari subjek data.

Meskipun demikian, keberadaan norma tersebut belum sepenuhnya menjawab persoalan kepastian hukum. Salah satu permasalahan utama terletak pada belum jelasnya parameter atau indikator yang digunakan untuk menilai kesetaraan tingkat perlindungan data di negara tujuan. Tanpa adanya kriteria yang objektif dan terukur, ketentuan tersebut berpotensi menimbulkan interpretasi yang berbeda-beda di antara para pemangku kepentingan. Hal ini pada akhirnya dapat menghambat aktivitas bisnis dan investasi, serta menimbulkan ketidakpastian bagi pelaku usaha dalam menentukan kepatuhan terhadap hukum. Selain itu, mekanisme penegakan hukum terhadap pelanggaran yang terjadi dalam konteks lintas yurisdiksi juga menjadi tantangan yang kompleks. Ketika terjadi pelanggaran data yang melibatkan pihak di luar negeri, yurisdiksi hukum Indonesia menjadi terbatas dalam menjangkau pelaku pelanggaran. Hal ini menimbulkan pertanyaan mengenai efektivitas perlindungan hukum yang diberikan oleh UU PDP, khususnya dalam menjamin hak-hak subjek data.

 

Dari perspektif komparatif, beberapa negara atau kawasan telah mengembangkan kerangka hukum yang lebih matang dalam mengatur *cross border data transfer*. Uni Eropa, misalnya, melalui General Data Protection Regulation (GDPR), menerapkan mekanisme *adequacy decision* untuk menentukan apakah suatu negara memiliki tingkat perlindungan data yang memadai. Selain itu, terdapat pula mekanisme lain seperti *standard contractual clauses* (yang untuk selanjutnya disebut dengan "**SCC**") dan *binding corporate rules* (yang untuk selanjutnya disebut dengan "**BCR**") yang memberikan fleksibilitas bagi pelaku usaha dalam melakukan transfer data lintas negara dengan tetap menjaga standar perlindungan data.

Pengembangan mekanisme serupa menjadi penting untuk memberikan kepastian hukum sekaligus menjaga daya saing ekonomi digital nasional (Sudarwanto & Kharisma, 2022). Tanpa adanya harmonisasi dengan standar internasional, Indonesia berisiko mengalami hambatan dalam arus data global (*data flow*), yang pada akhirnya dapat mempengaruhi pertumbuhan ekonomi digital. Di sisi lain, adopsi standar internasional juga harus disesuaikan dengan kepentingan nasional, termasuk dalam menjaga kedaulatan data (*data sovereignty*) dan keamanan informasi strategis.

Aspek kelembagaan juga tidak dapat diabaikan dalam membahas kepastian hukum *cross border data transfer*. Keberadaan otoritas pengawas yang independen, profesional, dan memiliki kewenangan yang jelas menjadi kunci dalam memastikan implementasi UU PDP berjalan efektif. Otoritas tersebut tidak hanya berfungsi sebagai regulator, tetapi juga sebagai pengawas dan penegak hukum yang mampu menangani sengketa serta pelanggaran yang terjadi, termasuk yang bersifat lintas negara. Lebih lanjut, kepastian hukum dalam transfer data lintas negara juga berkaitan erat dengan prinsip-prinsip hukum lainnya, seperti keadilan, kemanfaatan, dan proporsionalitas (Mertokusumo, 1993). Regulasi yang baik harus mampu menyeimbangkan antara perlindungan hak individu dan kepentingan publik, termasuk dalam mendorong inovasi dan pertumbuhan ekonomi. Pendekatan yang terlalu restriktif dapat menghambat perkembangan teknologi, sementara pendekatan yang terlalu permisif dapat mengorbankan perlindungan data pribadi.

Isu kepastian hukum dalam *cross border data transfer* merupakan isu yang kompleks dan multidimensional, yang melibatkan berbagai aspek hukum, teknologi, ekonomi, dan politik. Kajian terhadap UU PDP dalam konteks ini menjadi sangat relevan untuk menilai sejauh mana regulasi yang ada mampu memberikan perlindungan yang efektif sekaligus mendukung perkembangan ekonomi digital di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi dalam mengidentifikasi kelemahan dan kekuatan pengaturan yang ada, serta menawarkan rekomendasi untuk perbaikan di masa depan. Dengan adanya kepastian hukum yang memadai, diharapkan praktik transfer data lintas negara dapat berjalan secara aman, adil, dan berkelanjutan, serta mampu meningkatkan kepercayaan publik terhadap ekosistem digital di Indonesia (Van Donge et al., 2022).

 

## METODE

Penelitian ini merupakan penelitian hukum normatif atau doktriner yang berfokus pada pengkajian hukum sebagai norma tertulis, dengan menitikberatkan pada analisis terhadap peraturan perundang-undangan, asas, doktrin, serta prinsip-prinsip hukum yang berkaitan dengan kepastian hukum *cross border data transfer* berdasarkan UU PDP (Soekanto & Mamudji, 2014). Data sekunder yang diperoleh melalui studi kepustakaan (*library research*), yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan khususnya UU PDP beserta peraturan terkait lainnya; bahan hukum sekunder berupa buku-buku ilmiah, jurnal nasional maupun internasional, serta makalah ilmiah. Sedangkan bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan publikasi resmi. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan komparatif (*comparative approach*), yaitu dengan menelaah ketentuan hukum yang berlaku serta membandingkannya dengan pengaturan di negara lain atau standar internasional guna memperoleh praktik terbaik (*best practices*). Adapun analisis bahan hukum dilakukan secara kualitatif melalui penafsiran yang sistematis dan logis terhadap norma hukum dan doktrin yang relevan, sehingga dapat diperoleh kesimpulan yang komprehensif mengenai tingkat kepastian hukum dalam pengaturan transfer data lintas negara di Indonesia.

## HASIL DAN PEMBAHASAN

### *Tantangan Hukum yang Dihadapi dalam Pelaksanaan Cross Border Data Transfer di Indonesia*

Pelaksanaan *cross border data transfer* di Indonesia menghadapi berbagai tantangan hukum yang kompleks seiring dengan pesatnya perkembangan teknologi digital dan meningkatnya arus data lintas negara (Fahriawan et al., 2025). Meskipun Indonesia telah memiliki UU PDP sebagai landasan hukum utama, dalam praktiknya masih terdapat sejumlah persoalan yang mempengaruhi efektivitas pengaturan serta kepastian hukum dalam implementasinya.

**a. Kekosongan dan ketidakjelasan pengaturan turunan UU PDP**

Salah satu tantangan utama terletak pada aspek normatif, khususnya terkait dengan ketentuan mengenai transfer data pribadi ke luar wilayah hukum Indonesia. UU PDP pada prinsipnya mensyaratkan bahwa transfer data hanya dapat dilakukan apabila negara tujuan memiliki tingkat perlindungan data yang setara atau lebih tinggi, atau terdapat jaminan perlindungan yang memadai. Namun demikian, undang-undang ini belum memberikan kriteria yang jelas dan terukur mengenai standar "kesetaraan" tersebut. Ketiadaan parameter yang konkret berpotensi menimbulkan multitafsir di kalangan pelaku usaha maupun regulator, sehingga mengurangi kepastian hukum dalam praktik.

UU PDP telah memberikan kerangka dasar mengenai transfer data lintas negara, khususnya melalui ketentuan Pasal 55 dan Pasal 56 yang pada prinsipnya memperbolehkan pemindahan data kepada pengendali dan/atau prosesor di luar wilayah hukum Indonesia sepanjang memenuhi persyaratan tertentu, pengaturan tersebut masih menyisakan persoalan mendasar dalam tataran implementasi. Hal

 

ini disebabkan oleh belum lengkapnya peraturan pelaksana, terutama dalam bentuk peraturan pemerintah, yang seharusnya mengatur secara lebih rinci mengenai tata cara, mekanisme pengawasan, serta evaluasi terhadap kesetaraan tingkat perlindungan data di negara tujuan. Secara doktrinal, meskipun ketentuan dalam UU PDP telah mengadopsi prinsip *adequacy* atau kesetaraan perlindungan data sebagaimana dikenal dalam rezim internasional, ketiadaan pengaturan turunan justru menimbulkan kekosongan hukum (*legal vacuum*) yang berdampak pada ketidakjelasan mekanisme penetapan negara yang dianggap memiliki tingkat perlindungan setara, termasuk prosedur pengawasan dan evaluasinya. Kondisi ini pada akhirnya menimbulkan dilema bagi para pelaku usaha, karena di satu sisi mereka diwajibkan untuk mematuhi ketentuan normatif dalam UU PDP, namun di sisi lain tidak memiliki pedoman operasional yang jelas untuk memastikan dan membuktikan kepatuhan tersebut dalam praktik.

**b. Fragmentasi dan disharmoni regulasi sektoral**

Tantangan juga muncul dalam hal harmonisasi regulasi. Sebelum diberlakukannya UU PDP, pengaturan mengenai data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral, seperti di bidang perbankan, telekomunikasi, dan transaksi elektronik. Meskipun UU PDP hadir sebagai regulasi payung (*umbrella regulation*), dalam implementasinya masih diperlukan sinkronisasi dengan peraturan-peraturan sektoral tersebut. Ketidakharmonisan norma dapat menimbulkan konflik pengaturan yang pada akhirnya membingungkan pelaku usaha dalam menentukan standar kepatuhan hukum yang harus diikuti (Delia et al., 2026).

Sebelum diberlakukannya UU PDP pengaturan mengenai perlindungan data pribadi serta transfer data lintas negara di Indonesia telah tersebar dalam berbagai regulasi sektoral yang berdiri sendiri. Sebagai contoh, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik mengatur bahwa pengiriman data ke luar negeri hanya dapat dilakukan ke negara yang memiliki tingkat perlindungan data yang setara dengan Indonesia. Namun demikian, ketentuan tersebut dalam praktik sulit diimplementasikan karena hingga saat ini belum terdapat penetapan resmi mengenai daftar negara yang dianggap memenuhi standar kesetaraan tersebut. Di sisi lain, Peraturan Pemerintah Nomor 71 Tahun 2019 beserta peraturan pelaksananya di sektor penyelenggara sistem elektronik juga mengatur berbagai aspek terkait pengelolaan data, termasuk lokasi fasilitas komputasi, kewajiban akses untuk kepentingan penegakan hukum, serta standar keamanan sistem elektronik.

Permasalahan kemudian muncul setelah UU PDP diberlakukan sebagai rezim hukum yang bersifat *lex specialis* sekaligus *lex posterior* terhadap berbagai pengaturan sektoral tersebut, karena belum sepenuhnya terdapat kejelasan mengenai harmonisasi antar regulasi. Misalnya, terdapat kebutuhan untuk menyelaraskan konsep kesetaraan perlindungan data (*adequacy*) sebagaimana diatur dalam PP 80 Tahun 2019 dengan kerangka yang diatur dalam Pasal 56 UU PDP beserta peraturan pelaksananya. Selain itu, muncul pula persoalan dalam menafsirkan kewajiban untuk memberikan akses data kepada aparat penegak

 

hukum sebagaimana diatur dalam PP 71 Tahun 2019 dengan prinsip-prinsip perlindungan data pribadi dalam UU PDP, seperti pembatasan tujuan dan perlindungan hak subjek data. Fragmentasi pengaturan ini pada akhirnya berpotensi menimbulkan konflik norma (*regulatory conflict*) serta menciptakan beban kepatuhan yang berlapis bagi pelaku usaha yang beroperasi lintas sektor, sehingga semakin memperkuat urgensi harmonisasi hukum dalam pengaturan transfer data lintas negara di Indonesia.

**c. Risiko hak asasi dan kedaulatan digital dalam kerja sama dengan yurisdiksi "surveillance-heavy"**

Tantangan berikutnya berkaitan dengan aspek yurisdiksi dan penegakan hukum. Pelanggaran terhadap data pribadi seringkali melibatkan pihak yang berada di luar wilayah hukum Indonesia. Hal ini menimbulkan keterbatasan dalam penegakan hukum, mengingat otoritas nasional tidak memiliki kewenangan langsung terhadap entitas asing yang berada di yurisdiksi lain. Kondisi ini diperparah dengan belum optimalnya mekanisme kerja sama internasional dalam penanganan pelanggaran data lintas negara, sehingga perlindungan hukum bagi subjek data menjadi kurang efektif.

Transfer data lintas negara ke Amerika Serikat, sejumlah kajian akademik menunjukkan adanya persoalan mendasar terkait standar perlindungan data yang berlaku di negara tersebut. Amerika Serikat hingga saat ini belum memperoleh pengakuan sebagai negara dengan tingkat perlindungan data yang memadai (*adequate*) dari Uni Eropa, sebagaimana tercermin dalam putusan Schrems I dan Schrems II yang menyoroti adanya praktik pengawasan data secara luas tanpa mekanisme perlindungan yang efektif bagi warga negara asing. Selain itu, kerangka hukum di Amerika Serikat seperti CLOUD Act memungkinkan aparat penegak hukum untuk mengakses data yang dikuasai oleh perusahaan berbasis di AS, meskipun data tersebut disimpan di luar wilayah negara tersebut.

Ketentuan seperti FISA Section 702 dan Executive Order 12333 memberikan dasar hukum bagi pengumpulan data asing untuk kepentingan intelijen tanpa melalui mekanisme perintah pengadilan yang konvensional. Kondisi ini menimbulkan tantangan tersendiri dalam UU PDP, khususnya dalam menilai apakah tingkat perlindungan data di Amerika Serikat dapat dianggap "setara atau lebih tinggi" sebagaimana disyaratkan dalam Pasal 56. Lebih jauh, adanya potensi akses ekstrateritorial oleh otoritas asing juga meningkatkan risiko terhadap kedaulatan digital Indonesia, karena dapat mengurangi kontrol negara atas data pribadi warganya, sehingga berpotensi bertentangan dengan tujuan utama perlindungan data yang diusung oleh UU PDP.

**d. Ketiadaan otoritas pengawas PDP yang operasional**

Aspek kelembagaan juga menjadi tantangan yang signifikan. Efektivitas pengawasan terhadap pelaksanaan transfer data lintas negara sangat bergantung pada keberadaan otoritas pengawas yang independen dan memiliki kapasitas yang memadai. Penguatan kelembagaan masih menjadi pekerjaan rumah, baik dari segi kewenangan, sumber daya manusia, maupun koordinasi antar lembaga. Tanpa

 

dukungan kelembagaan yang kuat, implementasi norma hukum yang telah diatur dalam UU PDP berpotensi tidak berjalan secara optimal (Ciclosi & Massacci, 2023).

**e. Struktur persyaratan hierarkis yang sulit dipenuhi dalam praktik**

Tantangan hukum juga berkaitan dengan perbedaan standar perlindungan data antarnegara. Setiap negara memiliki pendekatan yang berbeda dalam mengatur perlindungan data pribadi, baik dari segi substansi maupun mekanisme penegakannya. Perbedaan ini menimbulkan kesulitan dalam memastikan bahwa data yang ditransfer ke luar negeri tetap mendapatkan perlindungan yang memadai. Negara-negara dengan standar perlindungan data yang tinggi cenderung menerapkan persyaratan yang ketat terhadap transfer data, yang dapat menjadi hambatan bagi negara berkembang seperti Indonesia dalam mengintegrasikan diri ke dalam arus data global.

Ketentuan Pasal 56 UU PDP sebagaimana dipahami dalam doktrin, pada dasarnya membangun suatu skema persyaratan yang bersifat hierarkis dalam pelaksanaan transfer data lintas negara. Pada tingkat pertama, pengendali data diwajibkan untuk memastikan bahwa negara tujuan memiliki tingkat perlindungan data yang setara atau lebih tinggi dibandingkan dengan standar yang ditetapkan dalam UU PDP (*adequacy*). Apabila persyaratan ini tidak dapat dipenuhi, maka pada tingkat kedua pengendali data diwajibkan untuk menyediakan jaminan perlindungan melalui mekanisme yang bersifat mengikat, seperti perjanjian antar-entitas, SCC, BCR, atau instrumen lain yang diakui oleh otoritas perlindungan data.

Selanjutnya, apabila kedua lapis persyaratan tersebut tidak dapat dipenuhi, maka pada tingkat ketiga pengendali data hanya dapat melakukan transfer setelah memperoleh persetujuan eksplisit dari subjek data. Meskipun secara konseptual pengaturan ini menunjukkan adanya upaya untuk mengadopsi standar internasional dalam perlindungan data, dalam praktiknya masih terdapat berbagai tantangan hukum dan operasional. Ketiadaan kriteria yang jelas dan terukur mengenai standar "setara atau lebih tinggi" menyebabkan sulitnya penerapan mekanisme kecukupan, terlebih lagi belum adanya daftar resmi negara yang diakui memenuhi standar tersebut. Pada tingkat kedua, efektivitas penggunaan instrumen kontraktual juga masih menghadapi kendala karena belum adanya kejelasan mengenai bentuk instrumen yang diakui serta mekanisme pengesahannya oleh otoritas yang berwenang, yang hingga kini belum sepenuhnya operasional.

Sementara itu, penggunaan persetujuan subjek data sebagai dasar transfer pada tingkat ketiga juga menimbulkan persoalan tersendiri, karena dalam kerangka UU PDP persetujuan tersebut diposisikan sebagai upaya terakhir (*last resort*), sehingga apabila tidak didukung oleh jaminan perlindungan lain, berpotensi menimbulkan ketidakpastian hukum, khususnya dalam hubungan kontraktual, serta meningkatkan risiko terjadinya sengketa di kemudian hari (Aulia, 2024).

**f. Kewajiban penilaian dampak dan tata kelola internal yang belum mapan**

Dari perspektif pelaku usaha, ketidakjelasan regulasi terkait *cross border data transfer* juga menimbulkan beban kepatuhan (*compliance burden*) yang tidak ringan. Perusahaan harus memastikan bahwa setiap transfer data memenuhi persyaratan

hukum yang berlaku, termasuk melakukan penilaian terhadap tingkat perlindungan di negara tujuan serta menyediakan mekanisme perlindungan tambahan apabila diperlukan. Tanpa panduan teknis yang jelas, proses ini dapat menjadi rumit dan berisiko menimbulkan pelanggaran hukum yang tidak disengaja.

Ketentuan Pasal 34 UU PDP mewajibkan pengendali data untuk melakukan penilaian dampak perlindungan data pribadi (*data protection impact assessment* atau DPIA) dalam hal pemrosesan data memiliki risiko tinggi, termasuk di antaranya pemrosesan data pribadi spesifik serta pemrosesan dalam skala besar yang pada praktiknya kerap melekat dalam skema transfer data lintas negara pada layanan digital berskala luas. Penilaian ini pada dasarnya dimaksudkan untuk mengidentifikasi potensi risiko serta merumuskan langkah mitigasi guna memastikan perlindungan terhadap hak subjek data sekaligus menjamin kepatuhan terhadap ketentuan UU PDP.

Namun demikian, dalam implementasinya masih terdapat berbagai kendala yang bersifat praktis maupun struktural. Banyak entitas bisnis belum memiliki kapasitas internal yang memadai, baik dari sisi sumber daya manusia maupun pemahaman teknis, untuk melaksanakan DPIA secara konsisten dan komprehensif. Selain itu, ketiadaan pedoman teknis nasional yang rinci mengenai standar pelaksanaan DPIA termasuk format, tingkat kedalaman analisis, serta tata cara pelaporan semakin memperbesar potensi ketidakseragaman dalam penerapannya, khususnya dalam konteks transfer data lintas negara.

Di sisi lain, Pasal 53 dan Pasal 54 UU PDP juga mewajibkan penunjukan pejabat atau petugas perlindungan data (*data protection officer* atau DPO) dalam kondisi tertentu, seperti pemrosesan data dalam skala besar, pemrosesan data pribadi spesifik, atau dalam penyelenggaraan pelayanan publik, di mana salah satu tugas utama DPO adalah memberikan saran serta melakukan pengawasan terhadap pelaksanaan DPIA. Akan tetapi, banyak organisasi di Indonesia yang belum siap secara kelembagaan untuk memenuhi kewajiban ini, sehingga implementasi ketentuan tersebut cenderung tertinggal dibandingkan dengan laju ekspansi bisnis digital lintas negara yang semakin pesat. Kondisi ini pada akhirnya memperlihatkan adanya kesenjangan antara norma hukum yang diatur dalam UU PDP dengan kesiapan praktis para pelaku usaha dalam melaksanakannya.

Di sisi lain, terdapat pula tantangan dalam menyeimbangkan antara perlindungan data pribadi dan kebutuhan ekonomi digital. Arus data lintas negara merupakan elemen penting dalam mendukung inovasi dan pertumbuhan ekonomi digital, sehingga pembatasan yang terlalu ketat dapat menghambat perkembangan tersebut. Namun, di sisi lain, kelonggaran yang berlebihan dapat meningkatkan risiko pelanggaran data dan merugikan masyarakat. Oleh karena itu, diperlukan keseimbangan yang tepat dalam merumuskan kebijakan hukum terkait *cross border data transfer*. Dengan demikian, dapat disimpulkan bahwa tantangan hukum dalam pelaksanaan *cross border data transfer* di Indonesia tidak hanya bersifat normatif, tetapi juga mencakup aspek kelembagaan, yurisdiksi, harmonisasi regulasi, serta dinamika global. Kompleksitas ini menunjukkan bahwa pengaturan yang ada masih memerlukan penguatan, baik melalui penyempurnaan regulasi, peningkatan kapasitas kelembagaan, maupun pengembangan kerja sama internasional. Hal ini

penting untuk memastikan terciptanya kepastian hukum sekaligus perlindungan yang optimal terhadap data pribadi dalam era digital.

***Perbandingan Pengaturan Perlindungan Data Cross Border Data Transfer di Indonesia dengan Rezim Hukum Internasional***

Pengaturan perlindungan data dalam konteks *cross-border data transfer* di Indonesia pada dasarnya telah berkembang mengikuti arus utama global, khususnya sebagaimana tercermin dalam rezim perlindungan data Uni Eropa melalui GDPR (Fitriyanti et al., 2025), meskipun masih menghadapi keterbatasan pada aspek instrumen teknis, keberadaan otoritas pengawas, serta kepastian operasional. Dari sisi dasar normatif, Indonesia melalui UU PDP telah menetapkan kerangka hukum utama yang secara eksplisit mengatur transfer data lintas negara, khususnya dalam Pasal 55 dan Pasal 56. Hal ini sejalan dengan praktik internasional, di mana GDPR sebagai rujukan utama juga mengatur mekanisme transfer lintas negara dalam Pasal 44 hingga Pasal 50, serta didukung oleh berbagai regulasi nasional di negara lain seperti Singapura, Tiongkok, dan Brasil. Selain itu, dalam hal prinsip umum perlindungan data, Indonesia telah mengadopsi prinsip-prinsip yang serupa dengan standar global, seperti prinsip pemrosesan yang sah, transparansi, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, serta integritas dan kerahasiaan data (Voigt & Bussche, 2017), yang secara implisit tercermin dalam Pasal 16 hingga Pasal 20 UU PDP. Prinsip-prinsip tersebut pada dasarnya identik dengan yang diatur secara eksplisit dalam Pasal 5 GDPR dan telah menjadi standar umum dalam berbagai rezim perlindungan data di dunia. Secara konseptual dapat dikatakan bahwa Indonesia telah mengadopsi kerangka prinsip global yang sama, sehingga dari sisi normatif tingkat tinggi, posisi Indonesia relatif selaras dengan perkembangan hukum internasional di bidang perlindungan data pribadi.

Jika dilihat dari sisi mekanisme dasar transfer data lintas negara dalam sistem hukum Indonesia pada prinsipnya telah mengadopsi struktur yang serupa dengan praktik internasional, khususnya sebagaimana diatur dalam rezim Uni Eropa melalui GDPR, yaitu melalui pendekatan berlapis yang mencakup *adequacy*, *safeguards*, dan *derogations*. Pasal 56 UU PDP membangun hierarki persyaratan yang dimulai dari kewajiban untuk memastikan bahwa negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi. Apabila persyaratan tersebut tidak dapat dipenuhi, maka pengendali data diwajibkan menyediakan langkah perlindungan yang memadai dan mengikat, seperti perjanjian antar-entitas, kebijakan korporasi yang mengikat, atau instrumen lain yang relevan. Selanjutnya, apabila kedua lapisan tersebut juga tidak dapat dipenuhi, maka transfer data hanya dapat dilakukan berdasarkan persetujuan eksplisit dari subjek data sebagai upaya terakhir. Struktur ini pada dasarnya sejalan dengan ketentuan dalam GDPR, yang melalui Pasal 44 hingga Pasal 49 mengatur mekanisme serupa, dimulai dari *adequacy decision*, penggunaan *appropriate safeguards* seperti SCC) dan BCR, hingga penggunaan *derogations* terbatas seperti persetujuan eksplisit atau kepentingan publik.

 

Namun demikian, meskipun secara desain normatif Indonesia telah mengadopsi pola yang sama, terdapat perbedaan signifikan dalam aspek implementasi. Dalam hal prinsip *adequacy*, misalnya, UU PDP memang mensyaratkan adanya tingkat perlindungan yang "setara atau lebih tinggi" di negara tujuan, tetapi hingga saat ini belum terdapat kriteria teknis yang rinci maupun daftar resmi negara yang diakui memenuhi standar tersebut. Hal ini berbeda dengan praktik di Uni Eropa, di mana Komisi Eropa secara aktif menetapkan daftar negara yang dianggap memiliki tingkat perlindungan yang memadai berdasarkan metodologi yang jelas, termasuk penilaian terhadap aspek *rule of law*, independensi otoritas pengawas, serta efektivitas penegakan hukum. Demikian pula dalam hal *safeguards* kontraktual dan struktural, meskipun UU PDP telah membuka ruang untuk penggunaan berbagai instrumen perlindungan, Indonesia belum memiliki standar nasional seperti SCC maupun mekanisme operasional untuk pengakuan BCR, sementara dalam rezim GDPR kedua instrumen tersebut telah diatur secara rinci dan digunakan secara luas, bahkan diadopsi oleh berbagai negara lain.

Adapun terkait persetujuan subjek data, UU PDP memposisikannya sebagai pilihan terakhir (*last resort*) apabila mekanisme *adequacy* dan *safeguards* tidak dapat dipenuhi, yang juga sejalan dengan pendekatan dalam GDPR yang menempatkan persetujuan sebagai bentuk pengecualian (*derogation*) yang terbatas dan tidak ideal untuk digunakan sebagai dasar utama dalam transfer data yang bersifat sistematis (Ayiliani & Farida, 2024). Secara konseptual Indonesia telah mengikuti pola global "*adequacy → safeguards → consent*" yang menjadi standar internasional dalam pengaturan transfer data lintas negara, namun secara praktis masih menghadapi kekurangan infrastruktur pendukung, seperti belum adanya daftar negara *adequate*, belum tersedianya instrumen kontraktual standar yang diakui secara resmi, serta belum adanya mekanisme operasional yang memadai untuk mendukung implementasi kerangka tersebut secara efektif.

Pada aspek kelembagaan dan otoritas pengawas, pengaturan perlindungan data di Indonesia menunjukkan adanya kesenjangan yang cukup signifikan jika dibandingkan dengan rezim internasional. UU PDP pada dasarnya telah mengantisipasi pembentukan suatu lembaga perlindungan data yang bersifat independen, yang memiliki kewenangan untuk menjatuhkan sanksi administratif serta menetapkan kebijakan teknis, termasuk dalam hal penilaian tingkat kecukupan (*adequacy*) perlindungan data di negara lain, sebagaimana tersirat dalam ketentuan mengenai sanksi administratif dan desain kelembagaan dalam undang-undang tersebut. Namun demikian, hingga saat ini lembaga pengawas tersebut belum beroperasi secara penuh, sehingga fungsi pengawasan, pengaturan teknis, dan penegakan hukum belum berjalan secara optimal. Kondisi ini berbeda dengan praktik dalam rezim internasional, khususnya di bawah GDPR, di mana setiap negara anggota diwajibkan memiliki otoritas pengawas independen yang memiliki kewenangan komprehensif, meliputi fungsi investigatif, korektif, otorisatif, dan konsultatif. Otoritas-otoritas tersebut, seperti di Uni Eropa maupun di berbagai negara lain seperti Singapura, Inggris, dan Prancis, secara aktif mengeluarkan

pedoman teknis, menyetujui instrumen seperti BCR, mengawasi penggunaan SCC, serta menjatuhkan sanksi yang signifikan terhadap pelanggaran.

Dalam hal mekanisme penetapan *adequacy* dan persetujuan terhadap instrumen perlindungan (*safeguards*), UU PDP pada prinsipnya menempatkan peran sentral pada lembaga pengawas untuk menetapkan daftar negara yang dianggap memiliki tingkat perlindungan data yang memadai serta untuk menyetujui penggunaan instrumen kontraktual seperti SCC atau BCR. Akan tetapi, hingga saat ini mekanisme tersebut belum dioperasionalkan secara konkret, sehingga menimbulkan kekosongan dalam implementasi. Sebaliknya, dalam rezim Uni Eropa, Komisi Eropa secara aktif mengeluarkan keputusan *adequacy*, sementara otoritas pengawas nasional bersama European Data Protection Board menyediakan panduan teknis yang rinci serta melakukan pengawasan terhadap praktik transfer data lintas negara, termasuk melalui proses peninjauan kontrak dan mekanisme sertifikasi. Dengan demikian, jika dibandingkan dengan standar internasional, kelemahan utama Indonesia terletak pada adanya *enforcement gap*, yaitu kondisi di mana norma hukum telah tersedia pada tingkat undang-undang, tetapi belum didukung oleh keberadaan otoritas pengawas yang aktif dan pedoman teknis yang memadai, sehingga efektivitas implementasi dan kepastian hukum dalam praktik masih belum optimal. Indonesia masih berada pada tahap transisi: norma tingkat UU sudah selaras dengan rezim internasional, namun perangkat pelaksana (peraturan pemerintah, otoritas, instrumen standar) dan kultur kepatuhan belum mencapai tingkat maturitas yang sama

## SIMPULAN

Pengaturan *cross border data transfer* di Indonesia melalui UU PDP secara konseptual telah mengadopsi prinsip-prinsip perlindungan data yang selaras dengan standar internasional, khususnya melalui mekanisme berlapis berupa *adequacy*, *safeguards*, dan *consent*. Hal ini menunjukkan bahwa dari sisi normatif, Indonesia telah berada pada arah yang tepat dalam membangun rezim perlindungan data yang modern dan kompatibel dengan perkembangan global. Namun demikian, dalam tataran implementasi, masih terdapat berbagai tantangan yang menghambat terciptanya kepastian hukum, antara lain belum lengkapnya peraturan pelaksana, belum jelasnya kriteria penilaian tingkat kesetaraan perlindungan data, belum tersedianya instrumen teknis seperti SCC dan BCR, serta belum optimalnya harmonisasi dengan regulasi sektoral yang telah ada sebelumnya. Selain itu, keterbatasan dalam aspek kelembagaan, khususnya belum beroperasinya secara penuh otoritas pengawas independen, serta kendala yurisdiksi dalam penegakan hukum lintas negara, semakin memperkuat adanya kesenjangan antara norma hukum dan praktik. Oleh karena itu, diperlukan langkah strategis berupa percepatan pembentukan dan penguatan otoritas perlindungan data, penyusunan regulasi turunan yang komprehensif, pengembangan instrumen teknis yang sesuai dengan standar internasional, serta peningkatan kapasitas dan kesadaran kepatuhan di kalangan pelaku usaha. Diharapkan kepastian hukum dalam pelaksanaan transfer data lintas negara di Indonesia dapat terwujud secara efektif dan mampu memberikan perlindungan yang optimal terhadap data pribadi masyarakat.

 

## DAFTAR RUJUKAN

Agusta, H. (2021). Keamanan dan Akses Data Pribadi Penerima Pinjaman Dalam Peer-to-Peer Lending di Indonesia. *Kertha Bhayangkara*, *15*(1), 11–38.

Aulia, E. (2024). Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dari Perspektif Kepastian Hukum. *UNES Law Review*, *7*(1), 220–227.

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, *6*(3), 431–455.

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

Delia, D., Tan, D., & Agustini, S. (2026). Regulasi Hukum Ekonomi Digital: Implikasi Undang-Undang Nomor 1 Tahun 2024 Terhadap E-Commerce dan Start-Up di Indonesia. *Unes Journal of Swara Justisia*, *10*(1), 42.

Fahriawan, H., Hasibuan, I. H., & Rahmawati, A. (2025). Global Digital Trade Regulation: An International Law Perspective on Cross-Border Data Flows and Privacy Standards. *Jurnal Ilmu Hukum Dan Sosial (HAKIM)*, *3*(3), 1291.

Fitriyanti, F., Fadhlurrahman, M. Z., Akbar, I. M. A., & Noviantoro, J. (2025). The Role of Legal Frameworks in Ensuring Certainty and Compliance in International Business Transactions. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *24*(1), 2956–2972.

Liat, K. E., & Wahyuningtyas, S. Y. (2025). PERSONAL DATA PROTECTION IN CLOUD COMPUTING BUSINESSES IN INDONESIA: CROSS-BORDER DATA TRANSFERS AND ACCESS BY PUBLIC AUTHORITIES. *Refleksi Hukum: Jurnal Ilmu Hukum*, *9*(2), 195–214. https://doi.org/https://doi.org/10.24246/jrh.2025.v9.i2.p195-214

Mahdi, M. P. S. Al, & Triadi, I. (2025). Dari Rectsvaccum Menuju Kepastian Hukum: Pembentukan Lembaga Perlindungan Data Pribadi Sebagai Penemuan Hukum Di Era Digital. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *12*(11), 4417.

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *JUSTISI*, *10*(1), 20–35. https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Mertokusumo, S. (1993). *Bab-Bab Tentang Penemuan Hukum*. Citra Aditya Bakti.

Ramli, A. M. (2004). *Cyber Law and HAKI Dalam Sistem Hukum Indonesia*. Refika Aditama.

Soekanto, S., & Mamudji, S. (2014). *Penelitian Hukum Normatif : Suatu Tinjauan Singkat* (16th ed.). Rajawali Pers.

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457.

Van Donge, W., Bharosa, N., & Janssen, M. F. W. H. A. (2022). Data-Driven Government: Cross-Case Comparison of Data Stewardship in Data Ecosystems. *Government Information Quarterly*, *39*(2), 101642. https://doi.org/https://doi.org/10.1016/j.giq.2021.101642

Voigt, P., & Bussche, A. von dem. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Pringer.

 