



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 11400-11408

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Perlindungan Data Pribadi dalam Transfer Data Lintas Negara: Analisis Hukum Internasional dan Implementasinya di Indonesia

Muhammad Zibran AL Habsy, Andini Anjelina Karamoy, Nandang Kusnadi

Fakultas Hukum, Universitas Pakuan

zibrans31@gmail.com, andinianjelina8@gmail.com.

Abstrak

Perkembangan teknologi informasi dan komunikasi telah meningkatkan frekuensi pemindahan data pribadi antarnegara sebagai bagian dari transaksi digital, layanan cloud, perdagangan elektronik, serta kerja sama internasional. Namun, pengalihan data pribadi ke area hukum yang berbeda menimbulkan berbagai tantangan terkait perlindungan privasi, keamanan data, dan kepastian hukum bagi individu yang datanya dipindahkan. Penelitian ini bertujuan untuk mengevaluasi pengaturan perlindungan data pribadi dalam pemindahan data antarnegara dari sudut pandang hukum internasional dan meninjau implementasinya dalam sistem hukum di Indonesia. Metodologi yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan hukum. Sumber hukum yang digunakan meliputi instrumen hukum internasional, regulasi perlindungan data dari berbagai negara, serta peraturan perundang-undangan Indonesia yang relevan dengan perlindungan data pribadi. Hasil dari penelitian ini menunjukkan bahwa sejumlah instrumen hukum internasional telah mengembangkan prinsip-prinsip perlindungan data pribadi dengan penekanan pada aspek legalitas, transparansi, akuntabilitas, dan jaminan adanya tingkat perlindungan yang memadai dalam pemindahan data antarnegara. Di Indonesia, regulasi mengenai pemindahan data pribadi ke luar negeri telah diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun demikian, pelaksanaannya masih menghadapi beberapa tantangan, seperti belum optimalnya mekanisme pengawasan, perlunya penyelarasan regulasi di berbagai sektor, serta pentingnya penguatan kapasitas pengendali data dan pemroses data agar dapat memenuhi standar perlindungan data internasional. Penelitian ini menyimpulkan bahwa efektivitas perlindungan data pribadi dalam pemindahan data antarnegara membutuhkan penguatan regulasi turunan, kolaborasi internasional, dan peningkatan kepatuhan dari para pelaku pengolahan data untuk menjamin perlindungan hak-hak individu secara maksimal di era digital.

Kata kunci: Perlindungan Data Pribadi, Transfer Data Lintas Negara, Hukum Internasional, Privasi Data, Undang-Undang Perlindungan Data Pribadi

1. Latar Belakang

Perkembangan teknologi digital telah mendesak individu, korporasi, dan pemerintah untuk mengatur dan memanfaatkan informasi pribadi dengan cara yang berbeda. Saat ini, kegiatan ekonomi digital sangat tergantung pada pertukaran data yang cepat dan tidak terikat oleh batasan negara. Penggunaan layanan berbasis cloud, media sosial, perdagangan online, dan layanan keuangan digital membuat data pribadi sering kali diproses dan disimpan di berbagai negara secara bersamaan. Situasi ini menjadikan pemindahan data antarnegara sebagai salah satu aspek penting dalam lingkungan ekonomi digital di tingkat global. Meskipun terdapat banyak keuntungan, pemindahan data ternama juga menghadirkan berbagai risiko bagi keamanan dan privasi data pengguna.

Pemindahan data pribadi antarnegara menimbulkan tantangan legal karena setiap negara memiliki standar perlindungan data yang berbeda. Ketika informasi pribadi pindah ke negara lain, perlindungan hukum yang didapatkan oleh subjek data dapat berbeda mengikuti hukum yang berlaku di negara penerima. Variasi dalam regulasi ini bisa menciptakan ketidakpastian hukum, penyalahgunaan informasi, serta kesulitan dalam penegakan hak-hak pemilik data. Oleh karena itu, berbagai badan internasional dan negara-negara berusaha menciptakan mekanisme yang memastikan keseimbangan antara kelancaran aliran data global dan perlindungan hak privasi individu.

Dalam pandangan hukum internasional, perlindungan data pribadi semakin dianggap sebagai bagian dari hak asasi manusia yang berkaitan dengan hak atas privasi. Berbagai instrumen dan standar internasional telah merumuskan

prinsip-prinsip perlindungan data, termasuk transparansi, akuntabilitas, pembatasan tujuan pemrosesan, serta jaminan perlindungan yang cukup dalam pemindahan data antarnegara. Prinsip-prinsip ini menjadi acuan bagi negara-negara untuk menyusun regulasi nasional yang bisa mengatasi tantangan dari globalisasi data. Kehadiran standar internasional juga bertujuan untuk mendorong keselarasan kebijakan antara negara-negara demi menciptakan kepercayaan dalam pertukaran data secara internasional. Sebagai salah satu negara dengan pertumbuhan ekonomi digital tercepat di Asia Tenggara, Indonesia juga berhadapan dengan tantangan perlindungan data pribadi dalam konteks pemindahan data antarnegara. Sebelum adanya regulasi khusus, aturan terkait data pribadi tersebar dalam beberapa peraturan sektoral yang tidak memberikan kepastian hukum secara menyeluruh. Situasi ini memunculkan kebutuhan akan kerangka hukum nasional yang mampu memberikan perlindungan yang lebih baik terhadap data pribadi masyarakat serta mendukung perkembangan ekonomi digital di dalam negeri.

Usaha tersebut diwujudkan dengan dihasilkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini menjadi fondasi hukum utama yang mengatur hak-hak subjek data, kewajiban pengendali dan pemroses data, mekanisme pengolahan data pribadi, serta ketentuan tentang pemindahan data pribadi ke luar wilayah hukum Indonesia. Dalam hal pemindahan data antarnegara, undang-undang ini menetapkan bahwa perlindungan yang diberikan harus setara atau lebih baik di negara tujuan, atau harus ada jaminan perlindungan yang memadai dan mengikat jika standar tersebut belum dipenuhi. Ketentuan ini mencerminkan komitmen Indonesia untuk menyelaraskan regulasi nasional dengan kemajuan standar perlindungan data di tingkat global. Meskipun demikian, pelaksanaan aturan tentang transfer data antar negara di Indonesia masih mengalami banyak kendala, baik dari segi institusi, pengawasan, maupun keselarasan dengan praktik global. Perkembangan teknologi yang pesat memerlukan adanya kepastian hukum dan sistem perlindungan yang efisien agar hak-hak individu yang terlibat dalam data tetap dijaga. Berdasarkan hal ini, penelitian ini sangat penting dilakukan untuk menganalisis bagaimana pengaturan perlindungan data pribadi dalam transfer data antar negara sesuai dengan hukum internasional serta mengevaluasi pelaksanaan dan tantangan yang dihadapi dalam sistem hukum Indonesia.

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana Pengaturan Perlindungan Data Pribadi Dalam Transfer Data Lintas Negara Berdasarkan Perspektif Hukum Internasional?
2. Bagaimana Implementasi Ketentuan Transfer Data Pribadi Lintas Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia?
3. Apa Saja Tantangan Dan Upaya Yang Diperlukan Untuk Mewujudkan Perlindungan Data Pribadi Yang Efektif Dalam Transfer Data Lintas Negara Di Indonesia?

Meningkatnya pengalihan data pribadi antarnegara sebagai hasil dari kemajuan teknologi digital memunculkan sejumlah masalah hukum terkait perlindungan privasi, keamanan informasi, dan kepastian hukum. Ketidaksesuaian standar perlindungan data di berbagai negara pun berisiko terhadap hak-hak individu pemilik data. Dengan demikian, penelitian ini bertujuan untuk menginvestigasi pengaturan transfer data pribadi antara negara dalam konteks hukum internasional serta mengevaluasi pelaksanaannya dalam sistem hukum Indonesia untuk mengidentifikasi tantangan.

2. Metode Penelitian

Penelitian ini menerapkan pendekatan hukum normatif dengan metode yang meliputi pendekatan peraturan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan perbandingan (comparative approach) untuk mengeksplorasi perlindungan data pribadi dalam konteks pengalihan data antarnegara. Sumber hukum yang digunakan terdiri dari sumber hukum utama yang mencakup peraturan perundang-undangan dan instrumen hukum internasional, serta sumber hukum sekunder seperti buku, jurnal, dan studi yang memiliki kaitan, ditambah sumber hukum tersier yang merupakan kamus dan ensiklopedia hukum. Proses pengumpulan sumber hukum dilakukan melalui penelitian pustaka (library research), sedangkan analisis dilaksanakan secara kualitatif dengan pendekatan deskriptif-analitis untuk meneliti pengaturan hukum internasional tentang pengalihan data pribadi antarnegara serta penerapannya di dalam sistem hukum Indonesia, khususnya berdasarkan Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi.

3. Hasil dan Diskusi

Pengaturan Perlindungan Data Pribadi Dalam Transfer Data Lintas Negara Berdasarkan Perspektif Hukum Internasional

Perkembangan teknologi informasi dan proses globalisasi telah membuat pemindahan data pribadi antar negara menjadi elemen penting dalam kegiatan ekonomi, sosial, dan pemerintahan modern. Saat ini, data pribadi dapat diproses, disimpan, dan dikirim ke berbagai negara secara cepat melalui layanan cloud computing, platform digital, serta sistem informasi global. Di satu sisi, pemindahan data antar negara mendorong perkembangan ekonomi digital dan inovasi teknologi, namun di sisi lain juga menimbulkan ancaman terhadap privasi serta keamanan data pribadi jika negara penerima tidak memiliki standar perlindungan yang memadai. Oleh karena itu, hukum internasional mulai mengembangkan berbagai instrumen dan prinsip untuk menjamin perlindungan data pribadi dalam arus data global. Saat ini, perkembangan undang-undang mengenai perlindungan data di seluruh dunia banyak dipengaruhi oleh keberadaan Peraturan Perlindungan Data Umum (GDPR) dari Uni Eropa. GDPR tidak hanya diterapkan pada organisasi yang berada di dalam batas teritorial Uni Eropa, tetapi juga berdampak kepada perusahaan di luar wilayah tersebut yang menangani data milik warga Uni Eropa. Ketentuan ini menjadikan GDPR sebagai salah satu norma internasional yang paling signifikan dalam pengaturan alih data antar negara. Banyak negara kemudian menyesuaikan undang-undang domestiknya agar dapat dianggap setara dengan standar perlindungan yang ada di Uni Eropa. Fenomena ini menunjukkan bahwa pentingnya harmonisasi perlindungan data semakin mendesak dalam sistem hukum internasional. Pengaruh GDPR bahkan telah membentuk arah perkembangan regulasi perlindungan data di berbagai belahan dunia.

Salah satu instrumen internasional yang penting dalam mengatur pemindahan data antar negara adalah Pedoman OECD tentang Perlindungan Privasi dan Aliran Data Pribadi Lintas Batas. Pedoman ini menekankan bahwa perlindungan privasi dan kelancaran arus data internasional harus berjalan seimbang. OECD memperkenalkan prinsip-prinsip dasar seperti batasan pengumpulan data, kualitas data, spesifikasi tujuan, pembatasan penggunaan, keamanan data, keterbukaan, partisipasi individu, dan tanggung jawab. Prinsip-prinsip ini menjadi dasar bagi banyak negara dalam merumuskan regulasi perlindungan data pribadi dan pemindahan data antara negara. Dalam konteks hukum Uni Eropa, terdapat mekanisme yang dikenal sebagai keputusan kesesuaian, yaitu evaluasi yang dilakukan oleh Komisi Eropa terhadap tingkat perlindungan data di suatu negara. Jika suatu negara dinilai memiliki standar perlindungan yang cukup baik, maka transfer data dari Uni Eropa ke negara tersebut bisa dilakukan tanpa memerlukan syarat tambahan yang rumit. Sistem ini dirancang untuk memberikan kepastian hukum dan menjaga kelancaran pertukaran data internasional. Keberadaan mekanisme ini menjadikannya sebagai salah satu model yang banyak dirujuk oleh negara-negara lain dalam menyusun kebijakan transfer data antar negara. Pendekatan ini menunjukkan bahwa perlindungan data semakin dianggap sebagai indikator yang penting dalam tata kelola digital yang efektif. Selain itu, mekanisme ini memperkuat rasa saling percaya antar negara dalam pertukaran data di tingkat global.

Perkembangan hukum internasional yang berkaitan dengan transfer data juga dipengaruhi oleh sejumlah putusan pengadilan yang berdampak luas. Salah satu contoh signifikan adalah perkara Schrems II yang diputuskan oleh Pengadilan Eropa (CJEU) pada tahun 2020. Putusan tersebut membatalkan mekanisme EU-US Privacy Shield karena dianggap tidak cukup memberikan perlindungan yang setara bagi data warga Uni Eropa. Akibatnya, perusahaan-perusahaan multinasional perlu menilai kembali mekanisme transfer data yang mereka terapkan. Kasus ini menunjukkan bahwa perlindungan data tidak hanya bergantung pada regulasi yang tertulis, tetapi juga pada efektivitas pengawasan dan penegakan hukum.

Dengan demikian, putusan pengadilan dapat berfungsi sebagai alat yang penting dalam perkembangan hukum perlindungan data di tingkat internasional. Selain OECD, pengaturan perlindungan data pribadi dalam konteks hukum internasional juga berkembang lewat Konvensi 108 yang disusun oleh Dewan Eropa. Konvensi ini merupakan instrumen internasional pertama yang mengikat secara hukum dalam bidang perlindungan data pribadi. Konvensi 108 mewajibkan negara-negara yang terlibat untuk memastikan bahwa pemrosesan data pribadi berlangsung secara adil, sah, dan transparan, serta memberikan perlindungan terhadap hak-hak individu terkait data pribadinya. Modernisasi melalui Convention 108+ semakin memperkuat prinsip-prinsip tersebut untuk menghadapi tantangan teknologi digital dan pemindahan data lintas negara yang semakin kompleks.

Selain pendekatan yang berbasis pada negara, hukum internasional juga mengenal penggunaan Klausul Kontrak Standar (SCCs) sebagai instrumen untuk melindungi alih data. SCCs adalah klausul kontraktual yang disusun secara standar untuk memastikan bahwa pihak yang menerima data tetap mematuhi prinsip-prinsip perlindungan

data yang berlaku. Instrumen ini banyak digunakan ketika transfer data dilakukan ke negara yang belum diakui memiliki standar perlindungan yang memadai. Melalui mekanisme ini, hak-hak subjek data dapat tetap dijamin melalui kewajiban kontraktual yang mengikat semua pihak. Penggunaan SCCs menunjukkan betapa pentingnya pendekatan hukum privat dalam mendukung perlindungan data internasional. Maka dari itu, kontrak menjadi salah satu alat yang krusial dalam pengelolaan data global.

Seiring dengan perkembangannya, hukum internasional juga mengadopsi konsep tingkat perlindungan yang memadai sebagai syarat utama untuk pemindahan data pribadi ke negara lain. Konsep ini bertujuan untuk memastikan bahwa data pribadi tetap mendapatkan perlindungan yang setara meskipun telah berpindah ke yurisdiksi yang berbeda. Negara atau organisasi yang melakukan pemindahan data harus memastikan bahwa negara penerima memiliki sistem perlindungan data yang adekuat atau menyediakan mekanisme perlindungan hukum yang bisa menjamin hak-hak subjek data. Pendekatan ini kemudian menjadi model yang banyak diadopsi dalam berbagai rezim perlindungan data di seluruh dunia.

Di seluruh dunia, terdapat perdebatan yang berkembang terkait dengan ide tentang lokalisasi data dan aliran data bebas. Kebijakan lokalisasi data mewajibkan penyimpanan data tertentu di dalam batas negara asal, sedangkan aliran data bebas mendorong kebebasan untuk memindahkan data antar negara guna mendukung ekonomi digital. Kedua pendekatan ini masing-masing memiliki kelebihan dan kekurangan. Lokalisasi data dipandang bisa meningkatkan kedaulatan digital serta keamanan nasional, sementara aliran data bebas dianggap lebih mendukung inovasi dan perdagangan global. Diskusi ini mengindikasikan bahwa perlindungan data tidak hanya terkait dengan privasi pribadi, tetapi juga berkaitan dengan kepentingan ekonomi dan geopolitik. Oleh karena itu, banyak negara berusaha menemukan keseimbangan antara kedua pendekatan tersebut.

Untuk memastikan pemindahan data yang aman, berbagai instrumen internasional juga menciptakan mekanisme perlindungan tambahan, seperti perjanjian kontraktual standar, aturan korporasi yang mengikat, sertifikasi, serta kolaborasi antar otoritas perlindungan data. Mekanisme ini dirancang untuk memberikan jaminan hukum saat pemindahan data dilakukan ke negara yang belum memiliki tingkat perlindungan yang setara. Dengan adanya sistem ini, aktivitas bisnis internasional serta pertukaran data global dapat terus berlangsung tanpa mengabaikan hak privasi individu sebagai bagian dari hak asasi manusia.

Di wilayah Asia Tenggara, ASEAN telah merumuskan Kerangka Kerja Tata Kelola Data Digital ASEAN sebagai langkah untuk meningkatkan kesesuaian regulasi perlindungan data di antara negara-negara anggotanya. Tujuan dari kerangka ini adalah untuk memperkuat kepercayaan dalam transaksi digital sekaligus mendukung perkembangan ekonomi digital di kawasan ini. Melalui pendekatan ini, negara-negara ASEAN diharapkan dapat mengadopsi prinsip-prinsip perlindungan data yang sejalan tanpa mengesampingkan karakteristik hukum nasional masing-masing. Keberadaan kerangka regional ini menunjukkan bahwa kolaborasi internasional merupakan faktor penting dalam menghadapi tantangan transfer data antar negara. Dengan meningkatnya kegiatan ekonomi digital di kawasan ini, penyelarasan regulasi diperkirakan akan menjadi kebutuhan yang semakin mendesak di masa yang akan datang.

Berdasarkan sudut pandang hukum internasional, regulasi mengenai perlindungan data pribadi dalam pemindahan data antar negara pada dasarnya bertujuan untuk menciptakan keseimbangan antara kelancaran arus data secara global dan perlindungan hak privasi individu. Berbagai instrumen internasional mencerminkan kecenderungan untuk menyelaraskan standar perlindungan data melalui penerapan prinsip-prinsip universal seperti kepatuhan hukum, keterbukaan, tanggung jawab, keamanan data, serta perlindungan yang memadai di negara penerima. Oleh karena itu, pemindahan data antar negara tidak hanya dilihat sebagai masalah ekonomi dan teknologi, melainkan juga sebagai aspek penting dari perlindungan hak asasi manusia di era digital.

Implementasi Ketentuan Transfer Data Pribadi Lintas Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Di Indonesia

Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah langkah signifikan bagi Indonesia dalam menciptakan sistem perlindungan data yang lebih menyeluruh. Sebelum UU PDP diratifikasi, pengaturan mengenai data pribadi tersebar di berbagai regulasi di sektor-sektor tertentu, yang menyebabkan ketidakpastian hukum dan fragmentasi norma. Dengan adanya UU PDP, pemerintah memberikan dasar hukum yang lebih terperinci terkait hak-hak subjek data, kewajiban pengendali dan prosesor data, serta cara transfer data pribadi, termasuk yang dilakukan ke luar wilayah hukum Indonesia.

Penerapan ketentuan mengenai transfer data antarnegara dalam UU PDP harus dipahami sejalan dengan regulasi digital lainnya, terutama Peraturan Pemerintah Nomor 71 Tahun 2019 yang mengatur Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan ini menetapkan berbagai kewajiban bagi penyelenggara sistem elektronik terkait pengelolaan data dan keamanan informasi. Keterkaitan antara kedua regulasi ini menegaskan bahwa perlindungan data pribadi harus terintegrasi dengan tata kelola sistem elektronik secara keseluruhan. Dengan demikian, keberhasilan dalam transfer data antarnegara tidak hanya bergantung pada UU PDP, tetapi juga harus sinkron dengan regulasi digital lainnya. Harmonisasi hukum sangat penting untuk mencegah tumpang tindih norma. Selain itu, perlu adanya koordinasi antar lembaga untuk menjamin kepatuhan dari pelaku usaha digital.

Regulasi mengenai transfer data pribadi antarnegara secara khusus diatur dalam Bab VII UU PDP, khususnya Pasal 56. Ketentuan ini mengizinkan pengendali data pribadi untuk melakukan transfer kepada pengendali atau prosesor data di luar batas hukum Indonesia. Namun, transfer tersebut tidak dapat dilakukan sembarangan karena harus memenuhi syarat tertentu yang bertujuan untuk memastikan hak-hak subjek data tetap terlindungi setelah data berpindah ke negara lain.

Pelaksanaan Pasal 56 ayat (2) UU PDP menunjukkan bahwa Indonesia menerapkan prinsip tingkat perlindungan yang memadai, yang juga dikenal dalam berbagai sistem perlindungan data internasional. Aturan ini mewajibkan pengendali data untuk memastikan bahwa negara penerima mempunyai tingkat perlindungan data pribadi yang setara atau lebih tinggi dari standar yang ditetapkan dalam UU PDP. Dengan demikian, kesinambungan perlindungan terhadap data pribadi tetap terjaga meskipun data tersebut telah keluar dari yurisdiksi Indonesia dan mengikuti standar yang telah ditentukan oleh hukum nasional.

Apabila negara tujuan transfer tidak memenuhi tingkat perlindungan yang setara, Pasal 56 ayat (3) mewajibkan pengendali data untuk memberikan perlindungan yang cukup dan bersifat mengikat. Ketentuan ini memberikan keleluasaan bagi pelaku bisnis yang melakukan aktivitas global, sembari menjamin bahwa data pribadi tetap mendapatkan perlindungan hukum yang layak. Selain itu, jika perlindungan yang setara maupun yang memadai tidak dapat diwujudkan, Pasal 56 ayat (4) meminta agar ada persetujuan dari subjek data pribadi sebelum transfer dilakukan. Mekanisme ini menunjukkan bahwa persetujuan subjek data merupakan bentuk perlindungan terakhir dalam proses transfer data antarnegara.

Walaupun ada kerangka hukum untuk transfer data antarnegara, pelaksanaannya masih menghadapi sejumlah kendala. Salah satu tantangan utama adalah regulasi pelaksana yang belumm memadai dan tidak memberikan panduan teknis mengenai penilaian kesetaraan tingkat perlindungan data di negara tujuan. Di samping itu, koordinasi antara instansi dan mekanisme pengawasan terhadap transfer data antarnegara perlu diperkuat agar pelaksanaan Pasal 56 bisa berjalan dengan efektif. Beberapa penelitian juga mengindikasikan bahwa aspek kepastian hukum dalam penerapan transfer data antarnegara masih memerlukan pembahasan yang lebih terperinci melalui peraturan yang lebih konkret.

Di sisi lain, pelaksanaan UU PDP mencerminkan komitmen Indonesia untuk menyesuaikan diri dengan kemajuan standar perlindungan data internasional. Melalui penerapan prinsip perlindungan yang setara, perlindungan yang memadai, dan persetujuan subjek data, Indonesia berusaha menciptakan keseimbangan antara kebutuhan arus data global dan perlindungan privasi warga. Oleh karena itu, efektivitas pengimplementasian ketentuan transfer data pribadi antarnegara ke depan sangat tergantung pada pembentukan regulasi yang jelas dan terperinci.

Di tingkat internasional, keberadaan Data Protection Officer (DPO) menjadi salah satu komponen krusial dalam memastikan kepatuhan terhadap hukum perlindungan data. Walaupun UU PDP telah mengatur tentang penunjukan pejabat yang bertanggung jawab atas perlindungan data dalam situasi tertentu, penerapannya masih memerlukan penguatan lebih lanjut. DPO berperan dalam memantau kepatuhan dalam organisasi, memberikan rekomendasi mengenai risiko terkait perlindungan data, serta bertindak sebagai penghubung dengan otoritas pengawas. Kehadiran DPO dapat membantu organisasi dalam mengenali risiko sebelum proses transfer data dimulai. Selain itu, DPO juga penting dalam menciptakan budaya perlindungan data yang berkelanjutan di dalam organisasi. Dengan demikian, pengembangan kompetensi DPO adalah hal yang sangat penting dalam pelaksanaan UU PDP.

Saat ini, transfer data antarnegara banyak dilakukan oleh perusahaan teknologi internasional seperti penyedia layanan media sosial, komputasi awan, dan platform digital global. Aktivitas ini mengakibatkan data pengguna dari Indonesia dapat diproses melalui server yang berada di banyak negara. Situasi ini menuntut perusahaan untuk memastikan bahwa setiap proses pemindahan data sesuai dengan ketentuan dalam UU PDP. Di samping itu,

perusahaan juga wajib menjelaskan kepada pengguna mengenai lokasi pemrosesan data serta maksud penggunaannya. Transparansi menjadi hal yang sangat penting dalam membangun kepercayaan masyarakat terhadap layanan digital. Penerapan prinsip ini menjadi salah satu tantangan utama dalam ekosistem digital yang bersifat internasional.

Penggunaan teknologi cloud computing menawarkan keuntungan seperti penghematan biaya dan fleksibilitas operasional, tetapi juga menimbulkan tantangan hukum terkait dengan transfer data internasional. Infrastruktur cloud memungkinkan data berpindah secara otomatis ke berbagai server yang berada di berbagai negara. Dalam keadaan demikian, pengendali data harus memastikan bahwa semua proses pemrosesan tetap mematuhi ketentuan perlindungan data yang ada. Selain itu, organisasi perlu memahami di mana data disimpan dan mekanisme keamanan yang diterapkan oleh penyedia layanan cloud. Ketidakjelasan mengenai lokasi penyimpanan data dapat menimbulkan risiko hukum serta kesulitan dalam menegakkan hak subjek data. Oleh karena itu, manajemen risiko cloud menjadi bagian penting dalam pelaksanaan UU PDP.

Prinsip akuntabilitas adalah salah satu dasar penting dalam pelaksanaan transfer data antarnegara. Prinsip ini menuntut pengendali data untuk membuktikan bahwa semua proses pengolahan dan pemindahan data dilakukan sesuai dengan hukum yang ada. Akuntabilitas tidak hanya terlihat dari kepatuhan administratif, tetapi juga melalui dokumentasi kebijakan, penilaian risiko, dan penerapan langkah-langkah keamanan yang memadai. Dengan prinsip ini, organisasi diharuskan untuk lebih aktif dalam mengelola risiko terkait perlindungan data. Pendekatan ini mencerminkan pergeseran dari sekadar kepatuhan formal menuju pengelolaan data yang bertanggung jawab. Oleh karena itu, akuntabilitas menjadi indikator penting dalam menilai sejauh mana UU PDP dilaksanakan dengan efektif.

Salah satu langkah yang bisa memperkuat penerapan ketentuan transfer data lintas negara adalah melaksanakan audit perlindungan data secara rutin. Audit memberi kesempatan bagi organisasi untuk menilai sejauh mana kepatuhan terhadap kebijakan internal dan hukum yang berlaku. Dengan adanya audit, kelemahan yang mungkin ada dalam proses transfer data dapat ditemukan sejak awal, sehingga risiko pelanggaran bisa dikurangi. Audit juga berfungsi sebagai alat untuk meningkatkan transparansi dan akuntabilitas organisasi. Dalam konteks transfer data internasional, audit dapat membantu memastikan bahwa negara tujuan dan pihak yang menerima data masih memenuhi standar perlindungan yang ditetapkan. Dengan demikian, audit menjadi alat yang penting dalam memperkuat pengelolaan perlindungan data pribadi.

Tantangan Dan Upaya Yang Diperlukan Untuk Mewujudkan Perlindungan Data Pribadi Yang Efektif Dalam Transfer Data Lintas Negara Di Indonesia

Meskipun Indonesia telah mempunyai dasar hukum melalui Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi, pelaksanaan perlindungan data pribadi dalam pengiriman data ke luar negeri masih mengalami banyak kesulitan. Salah satu hambatan utama ialah belum adanya kepastian hukum yang memadai mengenai cara pelaksanaan pengiriman data internasional. Beberapa ketentuan dalam Undang-Undang tersebut masih membutuhkan regulasi tambahan yang lebih spesifik, terutama terkait dengan evaluasi tingkat perlindungan negara tujuan, prosedur pengiriman data, serta mekanisme pengawasan bagi pengendali data yang melakukan transfer tersebut. Situasi ini memungkinkan terjadinya variasi interpretasi dan ketidakjelasan dalam praktik pelaksanaannya.

Salah satu masalah yang masih dihadapi dalam penerapan perlindungan data pribadi di Indonesia adalah tidak adanya lembaga perlindungan data yang sepenuhnya mandiri seperti yang ada di negara lain. Lembaga independen memiliki fungsi krusial dalam mengawasi, menerima keluhan dari masyarakat, dan memberikan sanksi administratif atas pelanggaran perlindungan data. Adanya lembaga seperti ini dapat membantu meningkatkan kepercayaan masyarakat terhadap sistem perlindungan data nasional. Tanpa adanya mekanisme pengawasan yang efektif, pelaksanaan aturan transfer data antarnegara mungkin akan mengalami tantangan dalam hal efektivitas. Oleh karena itu, penguatan lembaga menjadi hal utama dalam pengembangan sistem perlindungan data di Indonesia. Hal ini juga akan memperkuat posisi Indonesia dalam kerjasama perlindungan data di tingkat internasional.

Hambatan selanjutnya berkaitan dengan aspek kelembagaan dan pengawasan. Keberhasilan dalam perlindungan data pribadi sangat bergantung pada adanya lembaga yang memiliki kekuasaan untuk melakukan pengawasan, pemeriksaan, serta penegakan hukum terhadap pelanggaran yang mungkin terjadi. Beberapa penelitian

menunjukkan bahwa penguatan lembaga merupakan elemen kunci untuk memastikan pelaksanaan Undang-Undang Perlindungan Data Pribadi berjalan dengan baik. Tanpa adanya sistem pengawasan yang kuat, pengendali data berisiko untuk tidak memenuhi kewajiban hukum yang ada, terutama saat melakukan pengiriman data ke daerah hukum asing yang memiliki peraturan berbeda.

Tantangan lain yang muncul berkaitan dengan penegakan hukum di berbagai yurisdiksi. Ketika pelanggaran melibatkan entitas dari negara lain, proses penyelesaian sengketa menjadi lebih rumit karena harus mempertimbangkan perbedaan sistem hukum yang ada. Di beberapa situasi, negara tempat pelanggaran terjadi mungkin memiliki standar perlindungan data yang berbeda dari yang ada di Indonesia. Keadaan ini dapat menghambat proses penyelidikan dan penerapan keputusan hukum. Oleh karena itu, kerjasama internasional dan mekanisme bantuan hukum timbal balik sangat penting. Memperkuat alat kerjasama antarnegara akan membantu meningkatkan efektivitas perlindungan data dalam konteks digital global.

Selain masalah hukum dan kelembagaan, tantangan juga timbul dari perkembangan teknologi yang sangat cepat. Pemanfaatan teknologi seperti cloud computing, kecerdasan buatan, big data, dan blockchain membuat aliran data internasional menjadi semakin rumit dan sulit untuk dikendalikan dengan regulasi tradisional. Data pribadi dapat berpindah secara otomatis melalui server yang berlokasi di berbagai negara tanpa sepengetahuan subjek data. Kondisi ini memerlukan sistem manajemen data yang fleksibel serta penerapan prinsip desain privasi dan keamanan dalam setiap tahap pengolahan data pribadi.

Meningkatnya ancaman kejahatan siber juga menjadi masalah serius dalam transfer data antarnegara. Serangan siber seperti peretasan, pencurian identitas, ransomware, dan kebocoran data bisa mengakibatkan kerugian besar bagi individu dan organisasi. Kondisi menjadi lebih rumit ketika data berpindah melalui berbagai sistem dan yurisdiksi yang berbeda. Oleh karena itu, perlindungan data harus terintegrasi dengan peningkatan keamanan siber di tingkat nasional. Investasi dalam teknologi keamanan informasi menjadi sangat penting dalam menghadapi perkembangan ancaman digital. Dengan sistem keamanan yang handal, risiko pelanggaran terhadap data pribadi dapat diminimalkan.

Tantangan lain yang dihadapi adalah rendahnya tingkat kepatuhan dan kesadaran beberapa pelaku bisnis mengenai pentingnya perlindungan data pribadi. Banyak organisasi masih melihat perlindungan data hanya sebagai sebuah kewajiban administratif, bukan sebagai bagian dari praktik tata kelola perusahaan yang baik. Sebagai akibatnya, masih ada praktik pengelolaan data yang tidak sesuai dengan prinsip akuntabilitas, transparansi, dan keamanan sebagaimana yang ditetapkan dalam Undang-Undang tersebut. Keadaan ini menjadi lebih berisiko ketika data pribadi dikirim ke luar negeri, karena kemungkinan kebocoran dan penyalahgunaan data dapat melibatkan banyak pihak dari berbagai yurisdiksi.

Untuk mengatasi berbagai tantangan ini, pemerintah perlu mempercepat penetapan dan penguatan regulasi pelaksana yang secara khusus mengatur pengiriman data pribadi internasional. Regulasi tersebut harus memberikan petunjuk yang jelas mengenai evaluasi tingkat perlindungan negara tujuan, standar kontrak yang patut digunakan, mekanisme persetujuan dari subjek data, serta prosedur untuk pengawasan dan pelaporan. Di samping itu, kerja sama internasional juga perlu diperkuat untuk menciptakan keselarasan dalam standar perlindungan data dan mempermudah penegakan hukum terhadap pelanggaran yang melibatkan lebih dari satu negara.

Upaya untuk harmonisasi regulasi dengan negara-negara ASEAN juga harus terus ditingkatkan. Pertumbuhan ekonomi digital di kawasan ini mengakibatkan transfer data antar negara anggota ASEAN semakin sering berlangsung. Perbedaan standar perlindungan data dapat menjadi penghalang bagi pelaku usaha dan regulator. Melalui harmonisasi regulasi, proses transfer data dapat dilakukan dengan lebih efisien tanpa menurunkan tingkat perlindungan terhadap hak individu. Selain itu, harmonisasi juga dapat meningkatkan daya saing kawasan dalam ekonomi digital global. Kerja sama regional menjadi salah satu strategi kunci dalam menghadapi tantangan perlindungan data antar negara.

Pendekatan privasi sejak tahap desain perlu didorong sebagai bagian dari strategi perlindungan data yang berkelanjutan. Konsep ini mewajibkan pengintegrasian aspek privasi sejak awal dalam perancangan sistem, produk, dan layanan digital. Dengan cara ini, perlindungan data tidak hanya dilakukan setelah sistem beroperasi, tetapi telah menjadi bagian integral dari proses pengembangan teknologi. Pendekatan ini dapat mengurangi risiko pelanggaran data dan meningkatkan kepercayaan pengguna. Selain itu, privasi sejak tahap desain dianggap lebih

efektif dibandingkan dengan pendekatan yang reaktif. Oleh karena itu, penerapan konsep ini harus menjadi komponen dalam tata kelola data modern di Indonesia.

Selain penguatan regulasi, peningkatan kapasitas sumber daya manusia dan pemahaman mengenai perlindungan data juga merupakan langkah penting yang tidak boleh diabaikan. Pengendali data, pemroses data, serta masyarakat perlu memahami hak dan kewajiban yang terkait dengan pengolahan data pribadi di lingkungan digital global. Dengan adanya regulasi yang jelas, sistem pengawasan yang efektif, teknologi yang aman, serta peningkatan kesadaran di kalangan semua pihak terkait, perlindungan data pribadi dalam pengiriman data lintas negara di Indonesia dapat dilaksanakan dengan lebih baik sehingga mampu menjamin keamanan data serta mendukung kemajuan ekonomi digital nasional.

Selain pengawasan dan regulasi, penerapan standar global seperti ISO/IEC 27701 bisa menjadi langkah strategis dalam memperkuat perlindungan informasi pribadi. Standar ini menyediakan panduan bagi lembaga untuk mengembangkan sistem manajemen informasi privasi yang terintegrasi dengan keamanan data. Penerapan standar internasional dapat membantu lembaga menunjukkan dedikasinya terhadap perlindungan data serta meningkatkan kepercayaan dari mitra internasional. Selain itu, sertifikasi berdasarkan standar global dapat memfasilitasi kerja sama bisnis antarnegara. Dengan meningkatnya kebutuhan akan perlindungan data, pemanfaatan standar internasional diprediksi akan menjadi semakin penting. Oleh sebab itu, penerapan standar tersebut dapat menjadi bagian dari upaya meningkatkan daya saing Indonesia di era ekonomi digital.

4. Kesimpulan

Perlindungan data pribadi dalam transfer data antarnegara menjadi isu hukum yang semakin relevan seiring dengan kemajuan pesat teknologi digital dan meningkatnya jumlah pertukaran data di seluruh dunia. Dalam konteks hukum internasional, beragam instrumen dan norma perlindungan data telah mengembangkan prinsip-prinsip mendasar, seperti kepatuhan hukum, keterbukaan, pertanggungjawaban, keamanan data, dan jaminan tingkat perlindungan yang cukup dalam mentransfer data antarnegara. Indonesia telah mengadopsi prinsip-prinsip ini melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya dalam hal transfer data pribadi ke luar negeri yang mengharuskan adanya perlindungan setara atau memadai di negara tempat data tersebut dikirimkan. Namun begitu, penerapan ketentuan ini masih menghadapi berbagai tantangan, termasuk kurang optimalnya regulasi pelaksana, penguatan lembaga pengawas, perkembangan teknologi yang semakin rumit, serta rendahnya kesadaran dan kepatuhan dari sebagian pelaku pengolahan data. Oleh karenanya, untuk mencapai efektivitas perlindungan data pribadi dalam transfer data antarnegara, diperlukan kolaborasi antara regulasi yang menyeluruh, pengawasan yang efisien, serta peningkatan kapasitas semua pihak terkait untuk memastikan perlindungan hak-hak subjek data di era digital saat ini. Pemerintah sebaiknya segera menyusun dan memperbaiki regulasi pelaksana yang memberikan pedoman teknis tentang mekanisme transfer data pribadi antarnegara, mencakup standar evaluasi tingkat perlindungan di negara tujuan, prosedur pengawasan, serta cara penegakan hukum terhadap pelanggaran yang mungkin terjadi. Selain itu, penguatan lembaga pengawas perlindungan data pribadi harus menjadi fokus utama agar pengawasan dan penegakan hukum dapat berlangsung dengan baik. Di sisi lain, sektor usaha dan penyelenggara sistem elektronik perlu meningkatkan kepatuhan terhadap prinsip-prinsip perlindungan data pribadi melalui penerapan tata kelola data yang baik, peningkatan sistem keamanan informasi, serta pengembangan kompetensi sumber daya manusia di bidang perlindungan data. Kerja sama internasional juga perlu diperluas untuk mendukung keselarasan standar perlindungan data dan menyederhanakan penyelesaian sengketa yang melibatkan transfer data antarnegara. Dengan langkah-langkah tersebut, diharapkan perlindungan data pribadi di Indonesia dapat dilaksanakan dengan lebih efektif dan dapat mengatasi tantangan perkembangan ekonomi digital global.

Referensi

1. Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
2. 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.
3. Council of Europe. (n.d.). Convention 108 and protocols. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>
4. Kuner, C. (2011). Regulation of transborder data flows under data protection and privacy law: Past, present, and future (OECD Digital Economy Papers No. 187). Organisation for Economic Co-operation and Development.
5. OECD. (2001). Guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Co-operation and Development.
6. OECD. (n.d.). Cross-border data flows. <https://www.oecd.org/en/topics/cross-border-data-flows.html>
7. Pasal.id. (n.d.). UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. <https://pasal.id/peraturan/uu/uu-no-27-tahun-2022>

DOI: <https://doi.org/10.31004/riggs.v5i2.10596>

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

8. Prastowo, A. A., Algamar, A. F., & Siahaan, G. Y. (2026). Kepastian hukum dalam transfer data lintas negara: Tinjauan terhadap Undang-Undang Perlindungan Data Pribadi di Indonesia. *Jurnal Ilmu Sosial dan Hukum*, 4(2), 7838–7851.
9. Rahman, F., & Mulyania, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. *International Review of Law*, 39(2), 281–300.
10. Rinjani, M. A., & Firmansyah, R. (2025). Hambatan implementasi UU 27/2022 dan strategi penguatan perlindungan data pribadi. *Jurnal Analisis Hukum*, 8(1), 70–83.
11. Wijaya, I. M. M. (2025). The application of blockchain technology in cross-border personal data transfer activities in Indonesia: Opportunities and challenges. *Jurnal Magister Hukum Udayana*, 14(1), 193–217.
12. ASEAN. (2018). ASEAN framework on digital data governance. Jakarta: ASEAN Secretariat.
13. Court of Justice of the European Union. (2020). Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18). Luxembourg: CJEU.
14. European Commission. (2024). Adequacy decisions. Brussels: European Commission.
15. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
16. Greenleaf, G. (2022). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 175, 10–13.
17. International Organization for Standardization. (2019). ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: ISO.
18. Kuner, C. (2023). *Transborder data flows and data privacy law* (2nd ed.). Oxford, England: Oxford University Press.
19. United Nations Conference on Trade and Development. (2024). *Data protection and privacy legislation worldwide*. Geneva: UNCTAD.
20. World Bank. (2021). *World development report 2021: Data for better lives*. Washington, DC: World Bank.
21. European Data Protection Board. (2023). Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR. Brussels: EDPB.