

PREVENTIVE CONSTITUTIONAL HARM DAN DIGITAL SOVEREIGNTY SEBAGAI KONSTRUKSI BARU PERLINDUNGAN DATA PRIBADI DALAM KERJA SAMA INTERNASIONAL

Melki T. Tunggati^{*1}, Sri Wahyuni S. Moha², Mohamad Batu³,
Irwan Polidu⁴, Arif Mahfudin Ibrahim⁵

^{1,2,3,4,5} Universitas Bina Taruna Gorontalo, Kota Gorontalo, Indonesia

*Corresponding Author: melkitunggati@gmail.com

Info Article	Abstract: <i>This study aims to construct the concepts of “preventive constitutional harm” and “digital sovereignty” as a new paradigm for personal data protection in international cooperation, analyze the normative gap between Article 62(2) (2) of the Personal Data Protection Law (PDP Law) against the constitutional standards of Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, and to formulate a comprehensive constitutional protection model to fill this normative gap. This study employs a normative legal research method using a legislative approach, a case-based approach, a conceptual approach, and a comparative law approach to the EU’s GDPR, Brazil’s LGPD, and Indonesia’s Personal Data Protection Act. The findings indicate that Article 62(2) of the PDP Law contains a multidimensional normative gap encompassing substantive, institutional, procedural-democratic, and remedial dimensions; thus, this study formulates the CDPFIC as an integrative model that positions digital sovereignty as an operational constitutional constraint on executive discretion in international cooperation regarding the transfer of personal data of Indonesian citizens.</i>
Received :	
01 April 2026	
Revised :	
04 May 2026	
Accepted :	
02 June 2026	
Publication :	
30 June 2026	
Keywords:	
Preventive	
Constitutional	
Harm, Digital	
Sovereignty,	
Personal Data	
Protection,	
International	
Cooperation.	
Kata Kunci:	
Preventive	
Constitutional	
Harm, Digital	
Sovereignty,	
Perlindungan Data	
Pribadi, Kerja Sama	
Internasional.	
Licensed Under a	
Creative Commons	
Attribution 4.0	
International	
License	

INTRODUCTION

Perkembangan teknologi digital yang eksponensial telah mengubah data pribadi menjadi komoditas strategis yang melampaui batas-batas yurisdiksi negara (Geofani Milthre Saragih & Mirza Nasution, 2026). Dalam konteks ini, perlindungan data pribadi tidak lagi sekadar persoalan teknis administratif, melainkan telah berkembang menjadi isu fundamental yang menyentuh dimensi hak asasi manusia dan kedaulatan negara (Nethan & Tundjung Herning Situbuana, 2025). Sebagaimana ditegaskan oleh Bygrave, "*Undang-undang perlindungan data telah berkembang dari sekadar masalah administratif menjadi bidang yang kompleks yang bersinggungan dengan hak-hak dasar, perdagangan internasional, dan kedaulatan negara*" (Bygrave, 2014). Indonesia melalui UU PDP membangun perlindungan data komprehensif, namun menandatangani RTA dengan AS ber klausul adequacy tanpa pengawasan parlemen, menciptakan paradoks konstitusional. Putusan MK Nomor 133/PUU-XXIV/2026 menunjukkan persoalan ini telah diuji, mempersoalkan Pasal 62 ayat (2) UU PDP terhadap Pasal 28G ayat (1) UUD NRI 1945 (Putusan | Mahkamah Konstitusi RI, t.t.), sebuah fenomena yang mengindikasikan betapa mendesaknya kebutuhan akan konstruksi hukum baru dalam mengatur transfer data pribadi lintas negara dalam bingkai kerja sama internasional.

Realitas lapangan menunjukkan betapa rentannya data pribadi warga negara Indonesia dalam ekosistem digital global. Sejumlah insiden kebocoran data yang melibatkan institusi negara dan badan publik telah mengonfirmasi kerentanan sistemik dimaksud. Data Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2023 terdapat lebih dari 403 juta serangan siber yang menasar infrastruktur digital Indonesia, dengan sektor keuangan dan layanan publik sebagai target utama (EduCSIRT, t.t.). Insiden serangan siber pada Bank Syariah Indonesia pada Mei 2023 yang melumpuhkan layanan perbankan nasional, dugaan kebocoran data 370 ribu nasabah Bank Tabungan Negara, serta kebocoran data peserta BPJS Kesehatan yang ditengarai melibatkan ratusan juta data penduduk merupakan manifestasi nyata dari lemahnya ekosistem perlindungan data di Indonesia (Putri & Yusuf, 2025). Dalam perspektif komparatif global, fenomena serupa mendorong pengadilan konstitusional Kenya pada Desember 2025 untuk mengeluarkan putusan sela yang menangguhkan pelaksanaan *Kerangka Kerja Sama antara Pemerintah Republik Kenya dan Pemerintah Amerika Serikat di Bidang Kesehatan*, dengan pertimbangan bahwa perjanjian tersebut berpotensi melanggar hak privasi warga negara atas data kesehatan mereka (Okoiti v

Cabinet Secretary, National Treasury & 5 Others (Petition 337 of 2019) [2025] KEHC 4444 (KLR) (Constitutional and Human Rights) (4 April 2025) (Judgment), 2025). Uni Eropa menunjukkan sikap tegas melalui pembatalan EU-US Privacy Shield dalam *Schrems II* (C-311/18), menegaskan akses luas pemerintah terhadap komunikasi elektronik merusak esensi hak privasi (“Data Protection Commissioner v Facebook and Max Schrems (Standard Contractual Clauses),” t.t.). Rangkaian fakta ini secara kolektif mempertegas bahwa persoalan transfer data pribadi dalam kerja sama internasional bukan sekadar isu teknis perdagangan, melainkan persoalan hak konstitusional yang memerlukan konstruksi hukum baru dan responsif.

Kajian perlindungan data dalam hukum internasional-konstitusional berkembang pesat namun menyisakan celah konseptual. Westin dalam *Privacy and Freedom* meletakkan fondasi doktrin privasi sebagai hak individu menentukan pengungkapan informasi dirinya (Westin & Solove, 2015). Lebih lanjut, Barak dalam *Proportionality: Constitutional Rights and Their Limitations* mengembangkan prinsip proporsionalitas sebagai alat uji konstitusional atas pembatasan hak asasi manusia, termasuk dalam konteks transfer data lintas negara (Barak, 2012). Pada tataran hukum positif komparatif, Voigt dan von dem Bussche menganalisis secara mendalam mekanisme *adequacy decision* dalam GDPR sebagai instrumen perlindungan data lintas batas (Voigt & von dem Bussche, 2024), sementara Greenleaf dalam kajian komparatifnya terhadap 120 negara menemukan bahwa “Negara-negara di kawasan Asia-Pasifik semakin banyak yang memberlakukan undang-undang perlindungan data, namun terdapat perbedaan yang signifikan dalam hal ketegasan mekanisme penegakan hukum dan tingkat kemandirian otoritas pengawas” (Greenleaf, 2019). Sinta Dewi Rosadi mencatat kerangka hukum perlindungan data Indonesia masih sektoral tanpa otoritas pengawas independen, kondisi yang sebagian dijawab UU PDP 2022 namun menyisakan problem kelembagaan fundamental (Rosadi, 2015). Literatur belum menjelajahi preventive constitutional harm dan digital sovereignty sebagai pembatas diskresi kerja sama internasional data. Penelitian ini mengisi celah tersebut menggunakan Putusan MK Nomor 133/PUU-XXIV/2026 sebagai laboratorium konstitusional.

Kesenjangan (gap) yang paling mendasar dalam literatur yang ada terletak pada ketidakmampuan kerangka konseptual yang ada untuk menjelaskan secara memadai hubungan antara kerja sama internasional di bidang perdagangan digital dengan kewajiban konstitusional negara dalam melindungi data pribadi warganya. Di satu sisi,

literatur hukum perdagangan internasional cenderung memandang transfer data sebagai komponen dari arus perdagangan bebas yang harus difasilitasi (Meltzer, 2019), sementara di sisi lain literatur hukum konstitusional dan hak asasi manusia menekankan bahwa data pribadi adalah ekstensi dari hak privasi yang tidak dapat diperdagangkan secara bebas tanpa jaminan perlindungan yang setara (Floridi, 2016). Kontradiksi ini tampak nyata dalam konteks RTA Indonesia–Amerika Serikat, di mana ketentuan Article 3.3 yang mewajibkan Indonesia untuk berkonsultasi dengan Amerika Serikat sebelum memasuki perjanjian perdagangan digital dengan negara lain yang dapat merugikan kepentingan Amerika Serikat, secara substantif berpotensi melemahkan kedaulatan regulasi (*regulatory sovereignty*) Indonesia atas data pribadi warganya (Anitasari & Sampurna, 2025). Inkonsistensi MK: mengakui legal standing pemohon namun menolak permohonan berdasarkan Pasal 56 UU PDP, mengungkap kekosongan normatif standar perlindungan data dalam kerja sama internasional yang tak terjawab hukum privat (*Solove & Schwartz, 2019*).

Berdasarkan urgensi, data lapangan, telaah literatur, dan gap analysis di atas, penelitian ini merumuskan tiga rumusan masalah. Pertama, bagaimana konstruksi konsep preventive constitutional harm sebagai kategori baru kerugian konstitusional dalam pengujian undang-undang perlindungan data pribadi, serta relevansinya terhadap Putusan MK Nomor 133/PUU-XXIV/2026? Kedua, bagaimana konsep digital sovereignty dapat dikonstruksikan sebagai pembatas konstitusional atas diskresi pemerintah dalam kerja sama internasional yang melibatkan transfer data pribadi, dengan merujuk perbandingan GDPR Uni Eropa, LGPD Brazil, dan UU PDP Indonesia? Ketiga, model perlindungan konstitusional apa yang tepat untuk mengisi kekosongan normatif tersebut guna menjamin hak konstitusional warga negara sesuai Pasal 28G ayat (1) UUD NRI 1945?

METHOD

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*), yakni penelitian yang mengkaji hukum sebagai norma, asas, doktrin, dan sistem yang bersumber dari bahan-bahan kepustakaan hukum. Sebagaimana ditegaskan oleh Marzuki, "*penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai preskripsi dalam menyelesaikan masalah yang dihadapi*" (Marzuki, 2017), sehingga penelitian ini tidak semata-mata mendeskripsikan hukum yang berlaku, melainkan juga membangun konstruksi konseptual baru berupa

preventive constitutional harm dan *digital sovereignty* sebagai paradigma perlindungan data pribadi dalam kerja sama internasional.

Penelitian ini menggunakan empat pendekatan yang saling melengkapi: (1) pendekatan perundang-undangan, mengkaji UUD NRI 1945, UU PDP, UU Perjanjian Internasional, GDPR, dan LGPD; (2) pendekatan kasus, menganalisis Putusan MK Nomor 133/PUU-XXIV/2026 beserta putusan terkait (151/PUU-XXII/2024, 137/PUU-XXIII/2025), putusan sela High Court Kenya, dan Schrems II CJEU; (3) pendekatan konseptual, mengembangkan teori proporsionalitas Barak, doktrin privasi Westin, konsep data sovereignty Floridi, dan open legal policy MK; serta (4) pendekatan perbandingan, membandingkan kerangka perlindungan data Uni Eropa, Brazil, dan Kenya untuk menemukan best practice, sejalan dengan pandangan Zweigert dan Kötz mengenai fungsi hukum perbandingan dalam mencari solusi lintas sistem hukum (Zweigert & Kötz, 1998).

Bahan hukum penelitian diklasifikasikan tiga kategori: primer (UUD NRI 1945, undang-undang, peraturan, putusan pengadilan, perjanjian internasional); sekunder (buku, jurnal, penelitian terdahulu, pendapat ahli); dan tersier (kamus hukum, ensiklopedia, referensi penjelas bahan primer-sekunder) (Soekanto, 1986). Pengumpulan bahan hukum melalui studi kepustakaan sistematis, menelusuri portal MK RI, EUR-Lex, HeinOnline, Google Scholar, dan repositori hukum lain, diklasifikasikan berdasarkan relevansi.

Analisis bahan hukum dilakukan dengan menggunakan metode *preskriptif-analitis*, yakni tidak hanya menganalisis norma-norma hukum yang berlaku secara *lex lata*, tetapi juga merumuskan argumentasi normatif tentang bagaimana seharusnya hukum dibangun secara *lex ferenda* guna mengisi kekosongan dan menutup kesenjangan normatif yang teridentifikasi (Disemadi, 2022). Dalam proses analisis tersebut, digunakan teknik interpretasi hukum yang meliputi interpretasi gramatikal, sistematis, historis, dan teleologis (Mertokusumo, 2014), serta teknik konstruksi hukum untuk membangun konsep *preventive constitutional harm* dan *digital sovereignty* secara koheren dan konsisten dalam sistem hukum konstitusional Indonesia, sehingga pada akhirnya penelitian ini mampu menghasilkan rekomendasi normatif yang dapat menjadi acuan bagi pembaruan regulasi perlindungan data pribadi di Indonesia, khususnya dalam konteks kerja sama internasional yang melibatkan transfer data pribadi warga negara.

RESULTS AND DISCUSSION

Results

Konstruksi Konsep *Preventive Constitutional Harm* Sebagai Kategori Baru Kerugian Konstitusional Dalam Pengujian Undang-Undang Di Bidang Pelindungan Data Pribadi Dan Relevansinya terhadap putusan MK Nomor 133/PUU-XXIV/2026

Doktrin kerugian konstitusional dalam sistem pengujian undang-undang di Indonesia telah mengalami perkembangan yang signifikan sejak Mahkamah Konstitusi pertama kali menetapkan lima syarat kumulatif kerugian konstitusional melalui Putusan MK Nomor 006/PUU-III/2005 dan Putusan MK Nomor 11/PUU-V/2007 (Sulaiman dkk., 2019). Kelima syarat tersebut mencakup: (a) adanya hak konstitusional pemohon yang diberikan UUD 1945; (b) hak tersebut dianggap dirugikan oleh berlakunya undang-undang yang diuji; (c) kerugian bersifat spesifik dan aktual, atau setidaknya potensial yang menurut penalaran wajar dapat dipastikan terjadi; (d) adanya hubungan sebab-akibat (*causal verband*) antara kerugian dan norma yang diuji; serta (e) adanya kemungkinan bahwa dengan dikabulkannya permohonan, kerugian tidak akan terjadi (Hernando Santoso dkk., 2025). Syarat ketiga adalah titik kritis paling dinamis, terutama pada data pribadi. Mahfud MD menyatakan MK memperluas "kerugian konstitusional" mencakup potensi kerugian, mencerminkan komitmen perlindungan efektif (Mahfud MD, 2019). Ekspansi doktrin belum mengakomodasi kerugian antisipatif-struktural timbul dari norma yang membuka ruang pelanggaran sulit dipulihkan. Karakteristik ini membedakan preventive constitutional harm, diakui implisit dalam Putusan MK Nomor 133/PUU-XXIV/2026, di mana pemohon menegaskan kerugian preventif-konstitusional akibat transfer data lintas negara tanpa perlindungan HAM tegas (Putusan | Mahkamah Konstitusi RI, t.t.). Argumentasi ini secara normatif membuka pintu bagi rekonstruksi doktrin *legal standing* dalam konteks perlindungan data pribadi yang melampaui batas-batas konseptual doktrin kerugian konstitusional yang selama ini berlaku.

Preventive constitutional harm memerlukan tiga lapisan teoretis. Pertama, teori privasi Westin menegaskan privasi sebagai hak individu menentukan sendiri pengungkapan informasi pribadinya kepada pihak lain (Westin & Solove, 2015). Lebih lanjut, Solove mengembangkan taksonomi kerugian privasi (*privacy harm taxonomy*) yang mengidentifikasi bahwa kerugian privasi tidak selalu berwujud kerugian material

yang langsung terukur, melainkan dapat berupa *“hilangnya kendali atas informasi pribadi seseorang”, “kecemasan mengenai bagaimana data akan digunakan”, dan “kerentanan struktural yang disebabkan oleh kerangka hukum yang tidak memadai”* (Solove & Schwartz, 2019). Taksonomi ini menjelaskan mengapa kerugian data pribadi berbeda dari konvensional. Barak menegaskan prinsip proporsionalitas: norma pembatas hak fundamental harus memenuhi uji legitimate aim, necessity, dan proportionality stricto sensu (Barak, 2012) seperti Pasal 62 ayat (2) UU PDP, secara *prima facie* bermasalah dari perspektif konstitusional. Lapisan ketiga bersumber dari prinsip *lex certa* dalam negara hukum (*rechtstaat*). Asshiddiqie menegaskan bahwa *“prinsip negara hukum menuntut agar setiap norma dirumuskan secara tegas, jelas, dan dapat diprediksi (predictable), sehingga mampu memberikan perlindungan yang efektif terhadap hak-hak warga negara”* (Asshiddiqie, 2021). Norma kabur melanggar *lex certa*, menimbulkan kerugian struktural-antisipatif karena ketidakpastian hukum yang membuka ruang pelanggaran tak terpulihkan. Ketiga lapisan analisis membangun fondasi preventive constitutional harm: kerugian dari norma yang membuka ruang pelanggaran irreversible, sehingga perlindungan konstitusional tak boleh menunggu kerugian factual.

Analisis terhadap Putusan MK Nomor 133/PUU-XXIV/2026 mengungkap paradoks konstitusional signifikan: Mahkamah mengakui legal standing pemohon berdasarkan kerugian konstitusional potensial atas data pribadi, namun menolak permohonan dengan alasan perlindungan telah tersedia dalam Pasal 56 UU PDP. Dalam pertimbangan [3.5], Mahkamah menyatakan pemohon telah membuktikan hubungan sebab-akibat atas potensi kerugian akibat berlakunya Pasal 62 ayat (2) UU PDP—pengakuan yang secara implisit mengonfirmasi diterimanya argumentasi preventive constitutional harm pada tataran legal standing, meski tak dijadikan dasar mengabulkan pokok perkara. Pada pertimbangan [3.11]-[3.12], Mahkamah berpandangan Pasal 56 ayat (1)-(4) UU PDP telah menjawab kekhawatiran pemohon soal transfer data lintas negara (Putusan | Mahkamah Konstitusi RI, t.t.).

Argumentasi tersebut mengandung tiga kelemahan konseptual. Pertama, Pasal 56 UU PDP mengatur pengendali data sebagai subjek hukum privat, sementara Pasal 62 ayat (2) berkaitan dengan kerja sama internasional oleh negara sebagai subjek hukum internasional—dua kategori berbeda secara fundamental. Kedua, mekanisme Pasal 56 bersifat reaktif berbasis sanksi administratif, yang tak dapat diterapkan pada kerja sama antarnegara. Ketiga, perjanjian seperti RTA Indonesia-AS beroperasi pada level hukum

internasional publik yang hierarkis berbeda dari hukum privat UU PDP. Karenanya, argumentasi Mahkamah bahwa Pasal 56 telah menjawab kekhawatiran pemohon kurang tepat, justru menegaskan perlunya preventive constitutional harm untuk menjembatani kesenjangan perlindungan konstitusional tersebut (Alamri, 2025).

Tabel 01. Perbandingan Doktrin Kerugian Konstitusional Konvensional dengan Konsep *Preventive Constitutional Harm* dalam Konteks Pelindungan Data Pribadi

Dimensi Analisis	Kerugian Konstitusional Aktual	Kerugian Konstitusional Potensial (Konvensional)	Preventive Constitutional Harm (Konsep Baru)
Definisi	Kerugian yang telah terwujud secara nyata akibat berlakunya norma	Kerugian yang belum terjadi namun menurut penalaran wajar dapat dipastikan akan terjadi	Kerugian struktural-antisipatif yang timbul dari keberadaan norma yang membuka ruang bagi pelanggaran <i>irreversible</i>
Basis Normatif	Pasal 51 ayat (1) UU MK; Putusan MK No. 006/PUU-III/2005	Pasal 51 ayat (1) UU MK; Putusan MK No. 11/PUU-V/2007	Pasal 28G ayat (1) UUD 1945; Prinsip <i>lex certa</i> ; Doktrin <i>irreversibility</i>
Karakteristik Kerugian	Konkret, terukur, telah terjadi	Spesifik, dapat diperkirakan secara wajar	Struktural, antisipatif, berbasis ketidakpastian normatif
Sifat Pemulihan	Dapat dipulihkan melalui putusan	Dapat dicegah melalui putusan	Tidak dapat dipulihkan secara sempurna apabila sudah terwujud
Relevansi dalam Data Pribadi	Kebocoran data yang telah terjadi	Risiko transfer data yang dapat diprediksi	Keberadaan norma kabur yang membuka ruang transfer tanpa pagar konstitusional
Contoh dalam Putusan MK	—	Putusan MK No. 151/PUU-XXII/2024	Putusan MK No. 133/PUU-XXIV/2026 (diakui pada <i>legal standing</i> , belum pada pokok perkara)
Landasan Teoretis	Teori kerugian hukum tradisional	Teori risiko hukum (<i>legal risk theory</i>)	Teori privasi Westin (1967); Proporsionalitas Barak (2012); <i>Lex certa</i> Asshiddiqie (2010)
Implikasi terhadap Uji Norma	Uji norma <i>ex post facto</i>	Uji norma berbasis prediksi kerugian	Uji norma berbasis karakter struktural norma (<i>vague norm doctrine</i>)

Seluruh pemohon memenuhi lima syarat kerugian konstitusional sebagaimana digunakan Mahkamah Konstitusi untuk menilai legal standing dalam Putusan MK Nomor 133/PUU-XXIV/2026. Hak konstitusional yang diklaim berlandaskan Pasal 28G ayat (1) UUD 1945, meliputi perlindungan data finansial, keimigrasian, dan kesehatan. Kerugian yang diajukan bersumber dari potensi transfer data pribadi tanpa pengawasan memadai akibat Pasal 62 ayat (2), didukung oleh kasus kebocoran data dan risiko akses lintas yurisdiksi. Mahkamah menilai kerugian tersebut bersifat spesifik, aktual atau setidaknya potensial, serta memiliki hubungan sebab-akibat yang jelas dengan norma yang diuji. Selain itu, apabila permohonan dikabulkan, potensi kerugian dinilai dapat dicegah melalui penguatan perlindungan hak asasi manusia dan standar

perlindungan data. Atas dasar itu, Mahkamah menyatakan seluruh pemohon memiliki kedudukan hukum (*legal standing*).

Pengakuan konsep *preventive constitutional harm* sebagai kategori otonom dalam doktrin kerugian konstitusional Indonesia memiliki implikasi normatif yang berlapis dan jauh jangkauannya. Pada tataran doktrin pengujian undang-undang, konsep ini mengharuskan reorientasi metodologi analisis *legal standing* dalam perkara-perkara yang berkaitan dengan hak-hak fundamental yang bersifat *irreversible*, di mana kriteria "kerugian potensial yang menurut penalaran wajar dapat dipastikan terjadi" harus ditafsirkan secara luas untuk mencakup kerugian struktural yang timbul dari karakter norma itu sendiri, bukan hanya dari probabilitas terjadinya tindakan pelanggaran di masa mendatang (Ibáñez Colomo, 2023). Kerugian konstitusional struktural tidak timbul dari penerapan suatu norma, melainkan dari keberadaan norma itu sendiri, karena hal tersebut menciptakan kerentanan sistemik yang merongrong perlindungan hak-hak dasar secara efektif (Alamri, 2025). Pada tataran pengujian pokok perkara, konsep *preventive constitutional harm* menghendaki agar MK tidak hanya menguji apakah norma yang dipersoalkan secara langsung melanggar hak konstitusional, tetapi juga apakah norma tersebut memenuhi standar *lex certa* yang memadai untuk menjamin bahwa implementasinya tidak akan membuka ruang bagi pelanggaran hak konstitusional yang *irreversible* (Efendi & Disantara, 2022). Dalam konteks Putusan MK Nomor 133/PUU-XXIV/2026, penerapan standar ini seharusnya mendorong MK untuk memerintahkan pembentuk undang-undang melengkapi Pasal 62 ayat (2) UU PDP dengan parameter-parameter normatif yang tegas mengenai standar perlindungan data dalam kerja sama internasional, bukan sekadar merujuk pada mekanisme Pasal 56 yang dirancang untuk konteks yang berbeda secara fundamental.

Pada tataran reformasi legislasi, konsep *preventive constitutional harm* menuntut bahwa setiap norma yang mengatur kerja sama internasional di bidang data pribadi harus secara eksplisit memuat (Setyagraha dkk., 2026) : (a) standar kesetaraan perlindungan (*adequacy standard*) yang terukur dan diverifikasi oleh otoritas independen; (b) mekanisme notifikasi dan persetujuan subjek data dalam konteks transfer massal; (c) mekanisme pengawasan parlemen (*parliamentary oversight*) atas perjanjian internasional yang memuat klausul data; dan (d) mekanisme pemulihan (*effective remedy*) yang dapat diakses oleh warga negara apabila data pribadinya disalahgunakan dalam konteks kerja sama internasional. Sebagaimana diperingatkan oleh Solove dan Schwartz, "*Hukum privasi tidak dapat disederhanakan menjadi*

sekadar daftar persyaratan kepatuhan; hukum tersebut harus didasarkan pada teori yang koheren mengenai kepentingan privasi apa saja yang dipertaruhkan dan bagaimana kepentingan tersebut harus dilindungi dalam berbagai konteks" (Solove & Schwartz, 2019). Keseluruhan implikasi normatif ini mengonfirmasi bahwa konstruksi konsep *preventive constitutional harm* bukan sekadar inovasi akademis, melainkan kebutuhan hukum yang mendesak dalam konteks Indonesia yang tengah berhadapan dengan tantangan perlindungan data pribadi di era globalisasi digital, dan bahwa Putusan MK Nomor 133/PUU-XXIV/2026, meskipun pada akhirnya menolak permohonan para pemohon, telah membuka pintu bagi perkembangan doktrin ini melalui pengakuannya atas *legal standing* berbasis kerugian konstitusional yang bersifat antisipatif-struktural.

***Digital Sovereignty* sebagai Pembatas Konstitusional Diskresi Pemerintah dalam Kerja Sama Internasional Transfer Data Pribadi: Analisis Komparatif GDPR Uni Eropa, LGPD Brazil, dan UU PDP Indonesia**

Konsep *digital sovereignty* merupakan perkembangan kontemporer dari doktrin kedaulatan negara (*state sovereignty*) yang telah mengalami transformasi fundamental akibat digitalisasi masif dalam seluruh aspek kehidupan bernegara (Yokotani dkk., 2025). Secara tradisional, kedaulatan negara dipahami sebagai kekuasaan tertinggi negara atas wilayah, penduduk, dan sumber daya dalam batas-batas teritorialnya sebagaimana dikonseptualisasikan oleh Bodin dan kemudian dikembangkan lebih lanjut dalam teori Westphalian (Pohle & Thiel, 2020). Namun dalam era digital, batas-batas teritorial menjadi semakin kabur ketika data pribadi warga negara dapat mengalir melampaui yurisdiksi secara instan dan masif melalui infrastruktur digital yang beroperasi tanpa mengenal batas geografis (Revista & GEOGRAPHY, 2025). Pohle dan Thiel mendefinisikan *digital sovereignty* sebagai "*kemampuan suatu negara untuk melakukan pengendalian yang efektif atas infrastruktur digital, aliran data, dan ekonomi digital di wilayahnya yang berdampak pada warganya*" (Pohle & Thiel, 2020), sementara Couture dan Toupin (2019) memperluas definisi tersebut dengan menegaskan bahwa "*digital sovereignty mencakup hak masyarakat dan negara untuk menentukan masa depan digital mereka sendiri, termasuk kendali atas data yang dihasilkan oleh warga negaranya*" (Couture & Toupin, 2019). Dalam kerangka hukum konstitusional Indonesia, *digital sovereignty* dapat dikonstruksikan sebagai derivasi normatif dari tiga sumber konstitusional yang saling menopang (Kusuma Jatri dkk.,

2025): Pertama, prinsip kedaulatan rakyat (Pasal 1 ayat (2) UUD NRI 1945) yang mensyaratkan data rakyat berada dalam kontrol rakyat dan negara yang mewakilinya. Kedua, hak atas perlindungan diri pribadi (Pasal 28G ayat (1)) yang memberikan dimensi individual, yakni kendali warga negara atas data identitas pribadinya. Ketiga, kewajiban negara melindungi bangsa (Pembukaan UUD NRI 1945 alinea keempat) yang memberikan positive obligation membangun digital sovereignty. Dengan demikian, digital sovereignty memiliki substansi konstitusional konkret sebagai pembatas diskresi eksekutif, sejalan dengan pandangan Floridi bahwa data pribadi merupakan perpanjangan digital kepribadian yang layak dilindungi setara integritas fisik (Floridi, 2016), sehingga setiap kebijakan negara yang membuka ruang bagi mengalirnya data warga negara ke luar yurisdiksi tanpa standar perlindungan yang memadai secara konstitusional dapat dipandang sebagai pelanggaran atas dimensi *digital sovereignty* dari hak konstitusional warga negara.

GDPR Uni Eropa mewujudkan digital sovereignty melalui mekanisme adequacy decision (Article 45), mensyaratkan negara ketiga memiliki perlindungan data setara sebelum transfer (Wolford, 2018). Voigt dan von dem Bussche menjelaskan bahwa dalam melakukan *adequacy assessment*, Komisi Eropa harus mempertimbangkan serangkaian faktor yang komprehensif, meliputi: "*penegakan hukum, penghormatan terhadap hak asasi manusia dan kebebasan dasar, peraturan perundang-undangan yang berlaku di negara ketiga, keberadaan dan fungsi yang efektif dari lembaga pengawas independen, serta komitmen internasional yang telah diikat oleh negara ketiga*" (Voigt & von dem Bussche, 2024). Mekanisme ini mencerminkan tiga dimensi digital sovereignty: sovereignty as control, di mana Uni Eropa mengendalikan aliran data melalui penilaian kesetaraan yang mengikat; sovereignty as protection, melindungi warga dari rezim hukum asing yang tak setara; dan sovereignty as accountability, mensyaratkan negara penerima bertanggung jawab atas standar perlindungannya, dengan konsekuensi pencabutan adequacy decision. Rangkaian keputusan Schrems menjadi bukti operasionalisasi dan preseden hukum internasional monumentalnya (Voigt & von dem Bussche, 2024). Schrems I: CJEU membatalkan Safe Harbor Uni Eropa-AS karena akses pemerintah luas terhadap komunikasi elektronik merusak esensi hak privasi. (Court of Justice of the European Union | European Union, t.t.). Selanjutnya dalam Schrems II (C-311/18), CJEU kembali membatalkan EU-US Privacy Shield dengan pertimbangan serupa, mempertegas bahwa kedaulatan digital Uni Eropa tidak dapat dikesampingkan bahkan oleh kepentingan kerja sama dengan mitra dagang

terbesar sekalipun (*Court of Justice of the European Union | European Union, t.t.*). Kedua putusan ini secara persuasif mendemonstrasikan bahwa *digital sovereignty* yang dikodifikasikan dalam GDPR berfungsi sebagai pembatas konstitusional yang efektif atas diskresi eksekutif dalam menjalin kerja sama internasional di bidang data.

Brazil melalui *Lei Geral de Proteção de Dados* (LGPD) yang mulai berlaku penuh pada September 2020 menawarkan model *digital sovereignty* yang secara kontekstual lebih relevan bagi Indonesia, mengingat kesamaan posisi keduanya sebagai negara berkembang dengan kompleksitas hubungan internasional yang tinggi, khususnya dalam konteks tekanan dari negara-negara maju untuk membuka akses atas data (LGPD, t.t.-a). LGPD mengejawantahkan *digital sovereignty* melalui dua pilar utama yang saling melengkapi (LGPD, t.t.-a). Pilar pertama LGPD Brazil adalah mekanisme adequacy (Article 33), yang mengizinkan transfer data internasional hanya kepada negara atau organisasi yang memiliki tingkat perlindungan data setara. Perbedaan dengan model Uni Eropa terletak pada penekanan proporsionalitas dalam konteks keamanan nasional. Article 4 Paragraf (1) LGPD menegaskan bahwa pemrosesan data untuk kepentingan keamanan publik, pertahanan, dan keamanan negara harus diatur perundang-undangan khusus yang memuat langkah-langkah proporsional dan diperlukan guna melindungi kepentingan publik serta hak dan kebebasan dasar (LGPD, t.t.-b). Ketentuan ini berbeda dari UU PDP Indonesia yang tidak mensyaratkan undang-undang khusus bagi pemrosesan atau transfer data untuk keamanan nasional, sehingga membuka ruang diskresi eksekutif tak terkendali. Pilar kedua LGPD adalah ANPD (Article 55-A), otoritas pengawas dengan otonomi teknis dan administratif serta yurisdiksi nasional. Otonomi ANPD merupakan manifestasi kelembagaan *digital sovereignty*: kendali atas data warga negara harus berada di tangan lembaga independen, bebas dari distorsi kepentingan diplomatik atau ekonomi eksekutif (LGPD, t.t.-b). Mendes dan Doneda menegaskan independensi otoritas perlindungan data adalah keharusan konstitusional demi perlindungan hak, bukan kepentingan politik sesaat (Mendes, 2018a). Model Brazil mengajarkan Indonesia: *digital sovereignty* memerlukan norma substantif tegas dan infrastruktur kelembagaan independen dalam kerja sama internasional.

Tabel 03. Analisis Komparatif Model *Digital Sovereignty* dalam GDPR Uni Eropa, LGPD Brazil, dan UU PDP Indonesia

Dimensi Analisis	GDPR Uni Eropa	LGPD Brazil	UU PDP Indonesia	Penilaian Komparatif
Basis Konstitusional	Charter of Fundamental	Constituição Federal Brasil,	UUD NRI 1945, Pasal 28G ayat (1)	Indonesia memiliki basis konstitusional,

Digital Sovereignty	Rights EU, Article 8 (hak perlindungan data); Article 16 TFEU	Article 5 (X dan XII) — hak privasi dan kerahasiaan	— hak perlindungan diri pribadi	namun belum dikonstruksikan secara eksplisit sebagai <i>digital sovereignty</i>
Mekanisme Adequacy Assessment	<i>Adequacy decision</i> oleh Komisi Eropa (Article 45 GDPR) — otoritatif, mengikat, dan dapat dicabut	<i>Adequacy assessment</i> oleh ANPD (Article 33 LGPD) — berbasis kesetaraan perlindungan	Penilaian kesetaraan oleh pengendali data pribadi (Pasal 56 ayat (2) UU PDP) — berbasis swasertifikasi	Kelemahan kritis UU PDP: meletakkan penilaian <i>adequacy</i> pada entitas privat, bukan otoritas publik
Otoritas Pengawas Data	Data Protection Authorities (DPA) independen di setiap negara anggota EU; European Data Protection Board (EDPB) di level supranasional	ANPD — otonomi teknis dan administratif, independen dari eksekutif (Article 55-A LGPD)	Lembaga Pelindungan Data Pribadi (LPDP) — di bawah koordinasi Presiden (Pasal 59 UU PDP)	Kelemahan kritis UU PDP: LPDP tidak independen dari eksekutif, menimbulkan konflik kepentingan
Standar Transfer Data Internasional	Tingkat perlindungan setara atau mekanisme pengamanan yang tepat (SCCs, BCRs)	Tingkat perlindungan identik atau persetujuan subjek data	Tingkat perlindungan setara; jika tidak, perlindungan memadai; jika tidak, persetujuan subjek data	Mekanisme cascading UU PDP mirip LGPD, namun tanpa otoritas independen yang memverifikasi
Perlindungan Data dalam Konteks Keamanan Nasional	Article 23 GDPR — pembatasan harus proporsional, berdasarkan undang-undang, menghormati esensi hak fundamental	Article 4(1) LGPD — wajib diatur oleh undang-undang khusus dengan langkah proporsional	Pasal 2 huruf b UU PDP — pengecualian untuk kepentingan pertahanan dan keamanan nasional tanpa mandat UU khusus	Kelemahan kritis UU PDP: tidak mensyaratkan UU khusus untuk pengecualian keamanan nasional
Mekanisme Parliamentary Oversight	Parlemen Eropa memiliki hak pengawasan atas <i>adequacy decisions</i> Komisi Eropa	Kongres Brazil terlibat dalam pembentukan LGPD dan pengawasan ANPD	DPR RI tidak dilibatkan dalam proses <i>adequacy decision</i> atau kerja sama internasional data (kasus RTA)	Kelemahan kritis: absennya mekanisme <i>parliamentary oversight</i> dalam kerja sama internasional data
Mekanisme Pemulihan (Effective Remedy)	Article 77-82 GDPR — hak mengajukan pengaduan ke DPA, hak ganti rugi, hak gugat perdata	Articles 42-45 LGPD — tanggung jawab bersama pengendali data, pemulihan kerugian	Pasal 57 UU PDP — sanksi administratif oleh LPDP; belum ada mekanisme khusus untuk konteks kerja sama internasional	Kelemahan kritis: tidak ada mekanisme pemulihan khusus untuk pelanggaran data dalam konteks kerja sama internasional
Preseden Pembatalan Kerja Sama	<i>Schrems I</i> (2015) — batalkan <i>Safe Harbor</i> ; <i>Schrems</i>	Proses evaluasi kerja sama data dengan AS	Belum ada preseden pembatalan; RTA	Indonesia tertinggal dalam membangun mekanisme evaluasi

Internasional	<i>II (2020) — batalkan Privacy Shield</i>	sedang berlangsung	Indonesia-AS ditandatangani tanpa tinjauan memadai	konstitusional atas kerja sama internasional data
----------------------	--	--------------------	--	---

Tabel 04.Matriks *Digital Sovereignty* — Perbandingan Empat Variabel Kunci

Variabel	Indikator	GDPR (EU)	LGPD (Brazil)	UU PDP (Indonesia)
Kontrol Negara atas Aliran Data	Mekanisme <i>adequacy</i> oleh otoritas publik	✅ Sangat kuat (Komisi Eropa)	✅ Kuat (ANPD)	❌ Lemah (swasertifikasi)
Independensi Kelembagaan	Otoritas pengawas bebas dari intervensi eksekutif	✅ Sangat independen	✅ Independen secara teknis	❌ Di bawah koordinasi Presiden
Proporsionalitas Pembatasan Hak	Mensyaratkan UU khusus untuk pengecualian keamanan	✅ Ada (Article 23 GDPR)	✅ Ada (Article 4(1) LGPD)	❌ Tidak ada mandat UU khusus
Pengawasan Demokratis	Keterlibatan parlemen dalam kerja sama internasional data	✅ Ada mekanisme pengawasan	✅ Terlibat dalam pembentukan regulasi	❌ Absen dalam kasus RTA

Analisis UU PDP mengungkap kesenjangan konstitusional, diperparah RTA Indonesia-AS. Pertama, Pasal 62 ayat (2) yang menyatakan kerja sama "sesuai peraturan dan prinsip hukum internasional" terlalu umum, berbeda dari GDPR (*adequacy*) dan LGPD (*identikalitas standar*), tak menetapkan standar minimum negara mitra, sehingga bertentangan dengan *lex certa* (Asshiddiqie, 2021). Kedua, secara kelembagaan, LPDP berada di bawah koordinasi Presiden (Pasal 59 UU PDP), berbeda dari ANPD Brazil atau DPA Uni Eropa yang independen, menciptakan konflik kepentingan struktural. Ketiga, dan paling kritis, RTA Indonesia-AS yang memuat klausul *adequacy* bagi AS serta Article 3.3 yang mewajibkan konsultasi sebelum perjanjian digital dengan negara lain, menunjukkan absennya *digital sovereignty*—Indonesia mengakui perlindungan data AS memadai, padahal Uni Eropa dua kali membatalkan mekanisme transfer data dengan AS akibat *mass surveillance* yang diungkap Snowden (Nugraha, 2018). Giegerich memperingatkan bahwa "*Perjanjian internasional mengenai aliran data yang didorong oleh pihak eksekutif, apabila disepakati tanpa pengawasan parlemen yang berarti dan tinjauan regulasi yang independen, merupakan ancaman struktural terhadap kedaulatan digital, terlepas dari keabsahan hukum formalnya*" (Giegerich, 2026). Ketiadaan *parliamentary oversight*

atas perjanjian data internasional membuktikan digital sovereignty Indonesia rentan terhadap diskresi eksekutif tak terkendali.

Penelitian ini merekonstruksi digital sovereignty melalui dua pilar utama: substantif-konstitusional, mengakui digital sovereignty sebagai bagian Pasal 28G ayat (1) UUD NRI 1945 yang mencakup digital self, mensyaratkan proporsionalitas ketat; dan kelembagaan-independen, mereformasi LPDP setara Komisi Yudisial/KPU, berwenang eksklusif melakukan adequacy assessment, sejalan Rosenfeld dan Sajó (Rosenfeld & Sajó, 2012). Pilar ketiga, prosedural-demokratis: perjanjian bermuatan transfer data/adequacy wajib ratifikasi undang-undang (Pasal 10 huruf d UU Nomor 24/2000). Ketiganya membentuk digital sovereignty operasional, sejalan Greenleaf bahwa efektivitas bergantung kekuatan kelembagaan, bukan kerumitan aturan (Greenleaf, 2019). Indonesia, untuk dapat sejajar dengan standar *digital sovereignty* global sebagaimana dicontohkan oleh Uni Eropa dan Brazil, memerlukan rekonstruksi holistik atas kerangka normatif dan kelembagaan perlindungan datanya, dengan menempatkan *digital sovereignty* sebagai landasan konstitusional yang tidak dapat dikesampingkan oleh kepentingan diplomatik maupun ekonomi jangka pendek.

Model Normatif dan Kelembagaan Perlindungan Data Pribadi dalam Kerja Sama Internasional: Menuju Reformasi Konstitusional Pengaturan Transfer Data Pribadi di Indonesia

Kekosongan normatif dalam pengaturan kerja sama internasional bidang data pribadi merupakan persoalan multidimensional yang memerlukan rekonstruksi konseptual sistematis. Analisis Putusan MK Nomor 133/PUU-XXIV/2026 mengidentifikasi empat lapis kekosongan normatif yang secara kolektif menciptakan constitutional vacuum. Lapis pertama, kekosongan norma substantif: Pasal 62 ayat (2) UU PDP tidak memuat parameter konstitusional minimum, mencakup standar kesetaraan perlindungan negara mitra, kategori data yang dapat ditransfer, mekanisme notifikasi subjek data, dan pemulihan pelanggaran lintas yurisdiksi. Pertimbangan [3.7] menegaskan norma tersebut terlalu umum, hanya merujuk peraturan perundang-undangan dan prinsip hukum internasional tanpa batasan jelas mengenai ruang lingkup, jenis data, standar kesetaraan, persetujuan subjek, pengawasan, akuntabilitas, dan pemulihan (Putusan | Mahkamah Konstitusi RI, t.t.).

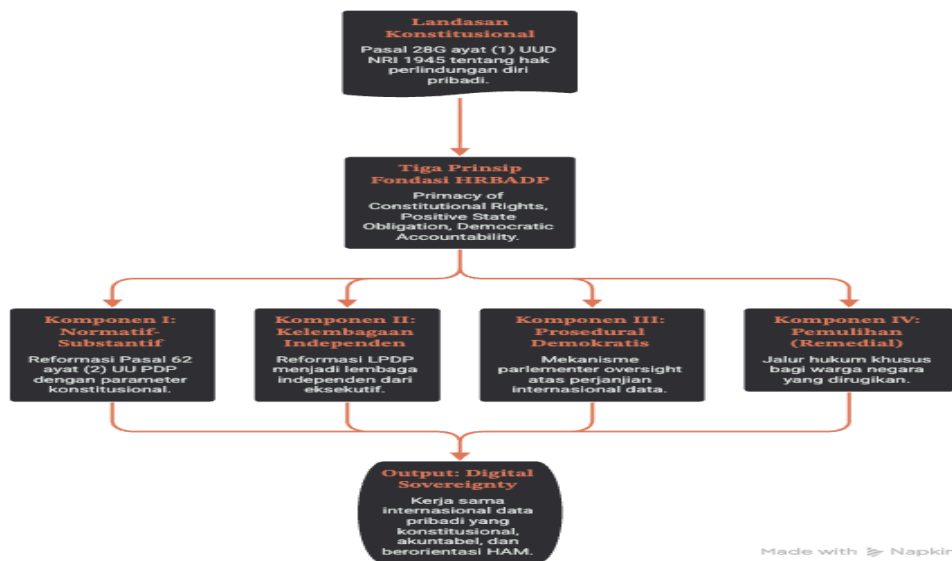
Lapis kedua, kekosongan kelembagaan: tiada pemisahan fungsi evaluasi adequacy dari kepentingan politik eksekutif. Lapis ketiga, kekosongan prosedural-

demokratis: tiada mekanisme persetujuan DPR atas perjanjian bermuatan transfer data, sehingga RTA Indonesia-AS diratifikasi via Keppres tanpa pengawasan parlemen bermakna. Lapis keempat, remedial gap: warga yang dirugikan tak memiliki jalur hukum efektif, karena sanksi Pasal 57 UU PDP dirancang bagi pengendali swasta, bukan kerja sama antarnegara. Bjørnskov dan Berggren menegaskan kekosongan konstitusional hak dasar memerlukan tindakan legislatif tegas berlandaskan konstitusi, bukan sekadar perluasan penafsiran (Bjørnskov & Berggren, 2026). Identifikasi keempat lapis kekosongan normatif ini menjadi titik berangkat bagi konstruksi model perlindungan konstitusional yang komprehensif sebagaimana diuraikan dalam paragraf-paragraf selanjutnya.

Model perlindungan konstitusional yang tepat mengisi kekosongan normatif adalah Human Rights-Based Approach to Data Protection (HRBADP), kerangka normatif yang menempatkan hak perlindungan diri pribadi (Pasal 28G ayat (1) UUD NRI 1945) sebagai nilai suprematif yang tak dapat dikesampingkan pertimbangan ekonomi, diplomatik, atau keamanan nasional tanpa proporsionalitas konstitusional ketat. Pendekatan ini berbeda fundamental dari compliance-based approach yang mendominasi praktik regulasi data Indonesia, yang memperlakukan perlindungan data sekadar kewajiban administratif-prosedural. Human Rights Committee PBB dalam General Comment No. 16 atas Pasal 17 ICCPR menegaskan hak privasi merupakan hak asasi fundamental yang mewajibkan negara melindungi individu dari campur tangan sewenang-wenang, termasuk melalui perjanjian pertukaran data internasional (*International Covenant on Civil and Political Rights*, t.t.).

Fondasi filosofis HRBADP berpijak pada prinsip pertama yaitu primacy of constitutional rights: hak konstitusional atas perlindungan data pribadi bersifat suprematif, tak dapat dikorbankan open legal policy pemerintah. Prinsip ini diakui MK dalam Putusan Nomor 151/PUU-XXII/2024 yang menegaskan perlindungan data pribadi sebagai hak asasi manusia yang wajib dilindungi maksimal oleh negara (*Tracking Perkara - MKRI*, t.t.-a). Prinsip kedua, positive state obligation: negara wajib aktif membangun kerangka normatif-kelembagaan mencegah pelanggaran data oleh pihak ketiga. Prinsip ketiga, democratic accountability: kebijakan berpotensi memengaruhi hak data warga negara harus tunduk pengawasan demokratis bermakna, tidak diserahkan sepenuhnya pada diskresi eksekutif. Ketiganya membentuk fondasi model perlindungan konstitusional yang ditawarkan.

Diagram 01. Arsitektur Model Perlindungan Konstitusional *Human Rights-Based Approach to Data Protection* (HRBADP) dalam Kerja Sama Internasional Data Pribadi di Indonesia



Komponen pertama HRBADP adalah reformasi normatif Pasal 62 ayat (2) UU PDP dengan lima elemen substantif. Pertama, standar kesetaraan perlindungan (adequacy standard): kerja sama internasional hanya dilakukan jika negara mitra ditetapkan otoritas independen memiliki perlindungan setara atau lebih tinggi. Kedua, klausul kategorisasi data: membedakan data biasa dan sensitif (kesehatan, biometrik, keuangan, keimigrasian) dengan standar lebih ketat untuk kategori sensitif. Ketiga, mekanisme notifikasi dan persetujuan subjek data sebelum data menjadi bagian kerja sama internasional. Keempat, klausul pengawasan-akuntabilitas: pelaporan berkala kepada DPR dan publik. Kelima, mekanisme pemulihan efektif: menjamin jalur hukum konkret dan dapat diakses bagi warga yang dirugikan. Komponen kedua HRBADP adalah reformasi kelembagaan LPDP menuju independensi konstitusional sejati.

Dalam Putusan MK Nomor 137/PUU-XXIII/2025, Mahkamah telah menegaskan peran sentral LPDP sebagai otoritas yang memiliki "*kewenangan final, otoritatif, dan mengikat untuk menentukan daftar negara yang dianggap setara*" dalam konteks transfer data pribadi (*Tracking Perkara - MKRI*, t.t.-b). Kewenangan tersebut tak bermakna tanpa independensi struktural LPDP dari eksekutif. Penelitian merekomendasikan reformasi LPDP menjadi lembaga negara independen setara Komisi Yudisial/OJK, dengan anggota dipilih transparan oleh DPR, masa jabatan terlindungi dari intervensi eksekutif, dan kewenangan ex ante review atas perjanjian internasional bermuatan transfer data sebelum diratifikasi—sejalan dengan Mendes dan Doneda bahwa independensi otoritas data adalah keharusan konstitusional (*Mendes, 2018b*). Tanpa reformasi kelembagaan ini, reformasi normatif-substantif apapun akan

kehilangan kekuatan implementatifnya, mengingat norma yang paling canggih sekalipun tidak akan efektif tanpa lembaga yang independen dan berkompeten untuk menegakkannya.

Tabel 05.

Matriks Komponen Model HRBADP — Parameter Reformasi Normatif dan Kelembagaan

Komponen Model	Kondisi Saat Ini (UU PDP)	Kekosongan Normatif	Rekomendasi Reformasi	Basis Konstitusional/Hukum
I. Normatif-Substantif	Pasal 62 ayat (2): norma terlalu umum, tidak memuat parameter minimum	Tidak ada standar <i>adequacy</i> , kategorisasi data, mekanisme notifikasi, dan pemulihan khusus untuk konteks kerja sama internasional	Reformulasi Pasal 62 ayat (2) dengan lima elemen substantif: <i>adequacy standard</i> , kategori sasi data, notifikasi subjek, pengawasan, dan pemulihan	Pasal 28G ayat (1) UUD 1945; Prinsip <i>lex certa</i> ; Article 45 GDPR; Article 33 LGPD
II. Kelembagaan Independen	LPDP di bawah koordinasi Presiden (Pasal 59 UU PDP) — tidak independen dari eksekutif	Konflik kepentingan antara LPDP sebagai pengawas dan eksekutif sebagai negosiator perjanjian internasional	Reformasi LPDP menjadi lembaga negara independen dengan kewenangan <i>ex ante review</i> atas perjanjian internasional data	Pasal 24C UUD 1945 (analog lembaga negara independen); Article 55-A LGPD Brazil
III. Prosedural-Demokratis	Tidak ada mekanisme <i>parliamentary oversight</i> khusus atas perjanjian internasional data	RTA Indonesia-AS diratifikasi melalui Keppres tanpa persetujuan DPR	Mandatori ratifikasi melalui UU untuk perjanjian internasional yang memuat klausul <i>adequacy</i> atau transfer data masif	Pasal 11 UUD 1945; Pasal 10 UU No. 24/2000 tentang Perjanjian Internasional
IV. Pemulihan (Remedial)	Sanksi administratif Pasal 57 UU PDP — hanya untuk pengendali data swasta	Tidak ada jalur pemulihan bagi warga negara atas pelanggaran data dalam konteks kerja sama internasional antar-negara	Pembentukan mekanisme pengaduan khusus kepada LPDP independen dan jalur gugatan perdata lintas yurisdiksi	Pasal 28D ayat (1) UUD 1945 (hak atas kepastian hukum); Article 77-82 GDPR; Articles 42-45 LGPD

Komponen ketiga HRBADP menyentuh dimensi prosedural-demokratis: transfer data warga negara harus lahir dari proses demokratis bermakna, bukan diskresi eksekutif semata. Dalam Putusan MK Nomor 133/PUU-XXIV/2026, RTA Indonesia-AS yang memuat klausul *adequacy* diratifikasi tanpa persetujuan DPR, meski menyentuh HAM yang menurut Pasal 10 huruf d UU Nomor 24/2000 mensyaratkan pengesahan undang-undang. Ketiadaan *parliamentary oversight* ini merupakan defisit konstitusional fundamental: pengakuan AS sebagai negara berperlindungan memadai, saat Uni Eropa dua kali menolaknya, berdampak konstitusional jangka panjang. Parlemen Eropa memiliki mekanisme pengawasan ketat atas *adequacy decisions*,

terbukti dalam perdebatan EU-US Data Privacy Framework pasca Schrems II (*Velasco Puffleau, 2024*). Penelitian merekomendasikan amandemen UU Nomor 24/2000 agar perjanjian internasional bermuatan transfer data masif atau pengakuan adequacy dikategorikan perjanjian HAM (Pasal 10 huruf d), sehingga wajib diratifikasi melalui undang-undang dengan persetujuan DPR.

Instrumen kedua adalah mekanisme konsultasi publik wajib sebelum LPDP mengeluarkan adequacy decision, melibatkan masyarakat sipil, akademisi, dan komunitas terdampak, sejalan prinsip meaningful public participation dalam yurisprudensi MK. Komponen keempat HRBADP adalah mekanisme pemulihan efektif—dimensi paling kritis, karena tanpa ini warga tetap tak terlindungi meski komponen I-III terimplementasi. Penelitian merekomendasikan tiga jalur pemulihan: (a) administratif melalui LPDP independen dengan kewenangan investigasi dan penghentian sementara kerja sama yang melanggar; (b) yudisial melalui pengadilan negeri berkewenangan khusus sengketa data lintas yurisdiksi; dan (c) diplomatik melalui kewajiban negara mitra menyediakan pemulihan setara bagi warga Indonesia, sebagai syarat minimum perjanjian transfer data. Solove dan Schwartz menegaskan sistem perlindungan data efektif harus mencakup hak substantif, jaminan kelembagaan, dan upaya hukum yang mudah diakses warga biasa (*Solove & Schwartz, 2019*).

Tabel 06. Perbandingan Mekanisme Pemulihan (*Effective Remedy*) dalam Tiga Sistem Hukum dan Rekomendasi untuk Indonesia

Dimensi Pemulihan	GDPR Uni Eropa	LGPD Brazil	UU PDP Indonesia (Saat Ini)	Rekomendasi Model HRBADP
Jalur Administratif	Pengaduan ke DPA nasional (Article 77 GDPR); investigasi wajib dilakukan	Pengaduan ke ANPD; kewenangan investigasi dan sanksi	Pengaduan ke LPDP (belum operasional penuh); kewenangan terbatas	LPDP independen dengan kewenangan investigasi, mediasi, dan penghentian sementara kerja sama
Jalur Yudisial	Gugatan perdata ke pengadilan nasional (Article 79 GDPR); class action dimungkinkan	Gugatan perdata (Articles 42-45 LGPD); tanggung jawab bersama	Gugatan perdata umum; tidak ada mekanisme khusus untuk konteks kerja sama internasional	Pengadilan khusus sengketa data atau kamar khusus di Pengadilan Negeri dengan kompetensi lintas yurisdiksi
Ganti Rugi (<i>Compensation</i>)	Hak atas kompensasi materil dan immateriil (Article 82 GDPR)	Tanggung jawab penuh pengendali data (Article 42 LGPD)	Sanksi administratif; ganti rugi melalui gugatan perdata umum yang terbatas	Ketentuan khusus ganti rugi yang proporsional dengan jenis dan dampak pelanggaran, termasuk ganti rugi immateriil
Konteks Kerja Sama	Mekanisme <i>Privacy Shield</i>	ANPD dapat menanggukuhkan	Tidak ada mekanisme khusus	Klausul wajib dalam setiap

Internasional	Ombudsman (meskipun telah dibatalkan); DPA dapat menanggihkan transfer	transfer yang tidak memenuhi standar	untuk konteks kerja sama internasional antar-negara	perjanjian internasional data: mekanisme pemulihan bagi warga negara di yurisdiksi mitra
Akses Kolektif (Class Action)	Dimungkinkan melalui organisasi nirlaba (Article 80 GDPR)	Dimungkinkan melalui mekanisme gugatan kolektif	Tidak ada mekanisme <i>class action</i> khusus untuk pelanggaran data	Pengakuan <i>class action</i> dalam sengketa perlindungan data dan <i>amicus curiae</i> dalam pengujian perjanjian internasional

Sintesis komponen HRBADP menghasilkan Constitutional Data Protection Framework for International Cooperation (CDPFIC), kerangka terintegrasi yang mengatur dimensi substantif, kelembagaan, prosedural, dan remedial dalam kerja sama internasional transfer data. CDPFIC berpijak pada pemahaman bahwa kekosongan Pasal 62 ayat (2) UU PDP merupakan constitutional deficit yang memerlukan intervensi konstitusional-legislatif, bukan sekadar persoalan teknis regulasi. Meski MK menolak permohonan dalam Putusan Nomor 133/PUU-XXIV/2026, pengakuan legal standing berbasis kerugian konstitusional potensial dan penghubungan Pasal 62 ayat (2) dengan Pasal 56 mengandung pesan implisit: arsitektur perlindungan data Indonesia masih memiliki celah struktural dalam kerja sama internasional antarnegara. Pesan ini sejalan dengan Putusan Nomor 151/PUU-XXII/2024 bahwa perlindungan data mencakup tertib hukum sebagai perwujudan HAM. Implementasi CDPFIC memerlukan langkah legislatif berurutan: pertama, amandemen Pasal 62 ayat (2) UU PDP memuat lima elemen substantif komponen I HRBADP, serta reformasi kelembagaan LPDP (Pasal 59) menjamin independensi strukturalnya dari eksekutif.

Langkah kedua, amandemen UU Nomor 24/2000 mengkategorikan perjanjian bermuatan transfer data masif/adequacy decision sebagai perjanjian HAM yang wajib ratifikasi undang-undang. Langkah ketiga, pembentukan undang-undang khusus kerja sama internasional data pribadi memuat adequacy assessment, standar perlindungan minimum, konsultasi publik, dan pemulihan lintas yurisdiksi. Ketiganya, jika konsisten diimplementasikan, mewujudkan digital sovereignty operasional dan mencegah Pasal 28G ayat (1) UUD NRI 1945 menjadi mere paper rights, sejalan Rosenfeld dan Sajó bahwa uji komitmen konstitusional terletak pada efektivitas kelembagaan, bukan keindahan redaksi teks.

Diagram 02. Peta Jalan Implementasi *Constitutional Data Protection Framework for International Cooperation* (CDPFIC)



Diagram tersebut memvisualisasikan empat tahap implementasi CDPFIC secara berurutan. Tahap pertama, amandemen Pasal 62 ayat (2) dan Pasal 59 UU PDP serta reformasi LPDP menjadi lembaga independen. Tahap kedua, amandemen UU Nomor 24/2000 memastikan parliamentary oversight atas perjanjian bermuatan transfer data. Tahap ketiga, pembentukan undang-undang khusus menjamin jalur pemulihan dan kewenangan LPDP menerbitkan daftar negara adequacy terverifikasi. Tahap keempat, evaluasi berkala dengan indikator keberhasilan berupa pengakuan timbal balik Uni Eropa dan Brazil atas standar perlindungan data Indonesia.

CONCLUSION

Penelitian ini menghasilkan tiga temuan utama. Pertama, preventive constitutional harm dikonstruksikan sebagai kategori otonom kerugian konstitusional—timbul dari norma yang membuka ruang pelanggaran hak bersifat irreversible—terkonfirmasi implisit dalam pengakuan legal standing Putusan MK Nomor 133/PUU-XXIV/2026. Kedua, digital sovereignty dikonstruksikan sebagai pembatas konstitusional operasional atas diskresi eksekutif, dengan Indonesia tertinggal dari standar GDPR (adequacy decision) dan LGPD (ANPD independen), khususnya dalam independensi LPDP dan parliamentary oversight. Ketiga, penelitian merumuskan Constitutional Data Protection Framework for International Cooperation (CDPFIC) dalam empat komponen-normatif-substantif, kelembagaan independen, prosedural-demokratis, remedial-yang mengisi kekosongan Pasal 62 ayat (2) UU PDP dan menjamin Pasal 28G ayat (1) UUD NRI 1945 tidak tereduksi paper rights.

REFERENSI

Alamri, M. (2025). CONSTITUTIONAL COURTS AND THE PROTECTION OF CONSTITUTIONAL RIGHTS: A COMPARATIVE ANALYSIS OF

- INSTITUTIONAL AUTHORITY IN INDONESIA AND MOROCCO. *International Journal of Constitutional and Administrative Law*, 116–130. <https://doi.org/10.66502/0wcva437>
- Anitasari, Y., & Sampurna, A. F. (2025). POLICY CAPACITY OF THE INDONESIAN GOVERNMENT IN IMPLEMENTING CROSS-BORDER DATA TRANSFER WITHIN TRADE AGREEMENTS WITH THE UNITED STATES. *Asian Journal of Social and Humanities*, 3(12), 2139–2149. <https://doi.org/10.59888/ajosh.v3i12.618>
- Asshiddiqie, J. (2021). KONSTITUSI DAN KONSTITUSIONALISME INDONESIA. Sinar Grafika.
- Barak, A. (2012). PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS. Cambridge University Press. <https://books.google.co.id/books?id=hHRNIIlMljUC>
- Bjørnskov, C., & Berggren, N. (2026). LEGISLATIVE POPULISM, IDEOLOGICAL ALIGNMENT, AND HUMAN FREEDOM. *European Journal of Political Economy*, 93, 102846. <https://doi.org/10.1016/j.ejpoleco.2026.102846>
- Bygrave, L. A. (2014). DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199675555.001.0001>
- Couture, S., & Toupin, S. (2019). WHAT DOES THE NOTION OF “SOVEREIGNTY” MEAN WHEN REFERRING TO THE DIGITAL? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Disemadi, H. S. (2022). LENSES OF LEGAL RESEARCH: A DESCRIPTIVE ESSAY ON LEGAL RESEARCH METHODOLOGIES. *Journal of Judicial Review*, 24(2), 289–304. <https://doi.org/10.37253/jjr.v24i2.7280>
- EduCSIRT. (n.d.). EDUCSIRT. Retrieved June 9, 2026, from <https://educsirt.kemendikdasmen.go.id/portal/berita/197>
- Efendi, A., & Disantara, F. P. (2022). POST CONDITIONALLY UNCONSTITUTIONAL OF JOB CREATION LAW: QUO VADIS LEGAL CERTAINTY? *Yuridika*, 37(2), 345–382. <https://doi.org/10.20473/ydk.v37i2.33364>

- Floridi, L. (2016). ON HUMAN DIGNITY AS A FOUNDATION FOR THE RIGHT TO PRIVACY. *Philosophy & Technology*, 29(4), 307–312. <https://doi.org/10.1007/s13347-016-0220-8>
- Geofani Milthree Saragih, G., & Nasution, M. (2026). KECERDASAN BUATAN, BIG DATA DAN KONSTITUSIONALISME DIGITAL: PERBANDINGAN UNI EROPA, KOREA SELATAN DAN INDONESIA. *Konferensi Nasional Asosiasi Pengajar Hukum Tata Negara dan Hukum Administrasi Negara*, 3(1), 147–164. <https://doi.org/10.55292/7vb8n428>
- Giegerich, T. (2026). THE HUMAN RIGHT TO DEMOCRACY IN MULTILEVEL SYSTEMS AT A TIME OF DEMOCRATIC BACKSLIDING: GLOBAL, REGIONAL AND EUROPEAN UNION PERSPECTIVES (Vol. 24). Springer Nature Switzerland. <https://doi.org/10.1007/978-3-032-01689-8>
- Greenleaf, G. (2019). GLOBAL DATA PRIVACY LAWS 2019: 132 NATIONAL LAWS & MANY BILLS (SSRN Scholarly Paper No. 3381593). Social Science Research Network. <https://papers.ssrn.com/abstract=3381593>
- Hernando Santoso, S. M. S., Divia Nur Alan Nur, D. N. A., Raddine Nur Halizah Rihhadatul Aisy, R. N. H. A., Nafisatul Aini, N. A., & Faisal Alfarizi, F. A. (2025). KONSEP CONSTITUTIONAL INJURY SEBAGAI SYARAT PENGAJUAN PERMOHONAN PENGUJIAN UNDANG-UNDANG TERHADAP UNDANG-UNDANG DASAR. *Veteran Society Journal*, 5(1), 33–52. <https://doi.org/10.33005/vsj.v5i1.182>
- Ibáñez Colomo, P. (2023). THE (SECOND) MODERNISATION OF ARTICLE 102 TFEU: RECONCILING EFFECTIVE ENFORCEMENT, LEGAL CERTAINTY AND MEANINGFUL JUDICIAL REVIEW. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4598161>
- International Covenant on Civil and Political Rights. (n.d.). INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS. OHCHR. Retrieved June 10, 2026, from <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Kusuma Jatri, L., Wisnaeni, F., & Faculty of Law, Diponegoro University. (2025). THE URGENCY OF REGULATING CYBER SOVEREIGNTY WITHIN THE CONSTITUTIONAL LAW SYSTEM TO ENSURE DIGITAL SOVEREIGNTY. *International Journal of Social Science and Human Research*, 8(12). <https://doi.org/10.47191/ijsshr/v8-i12-24>

- Mahfud MD. (2019). KONSTITUSI DAN HUKUM DALAM KONTROVERSI ISU. Rajawali Pers.
- Marzuki, P. M. (2017). PENELITIAN HUKUM: EDISI REVISI. Prenada Media.
- Meltzer, J. P. (2019). GOVERNING DIGITAL TRADE. *World Trade Review*, 18(S1), S23–S48. <https://doi.org/10.1017/S1474745618000502>
- Mertokusumo, S. (2014). PENEMUAN HUKUM: SEBUAH PENGANTAR. Cahaya Atma Pustaka.
- Nethan, & Situbuana, T. H. (2025). IMPLEMENTASI FUNGSI PERLINDUNGAN KEMENTERIAN KOMUNIKASI DAN DIGITAL DALAM MENJAMIN PERLINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA. *Kertha Semaya: Journal Ilmu Hukum*, 13(10), 2339–2349. <https://doi.org/10.24843/KS.2025.v13.i10.p14>
- Nugraha, R. A. (2018). PERLINDUNGAN DATA PRIBADI DAN PRIVASI PENUMPANG MASKAPAI PENERBANGAN PADA ERA BIG DATA. *Mimbar Hukum*, 30(2), 262. <https://doi.org/10.22146/jmh.30855>
- Okoiti v Cabinet Secretary, National Treasury & 5 Others (Petition 337 of 2019) [2025] KEHC 4444 (KLR). (2025). JUDGMENT. <https://new.kenyalaw.org/akn/ke/judgment/kehc/2025/4444/eng@2025-04-04>
- Pohle, J., & Thiel, T. (2020). DIGITAL SOVEREIGNTY. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Putri, A. A., & Yusuf, H. (2025). RANSOMWARE DI SEKTOR KEUANGAN: STUDI KASUS SERANGAN TERHADAP BSI PADA TAHUN 2023. *Jurnal Intelek Insan Cendikia*, 2(8), 15649–15656.
- Revista, Z., & Geography, 10. (2025). ALGORITHMIC GEOPOLITICS: THE DATAFICATION OF BOUNDARIES AND THE FUTURE OF THE STATE. <https://doi.org/10.5281/ZENODO.17728334>
- Rosadi, S. D. (2015). CYBER LAW: ASPEK DATA PRIVASI MENURUT HUKUM INTERNASIONAL, REGIONAL, DAN NASIONAL. Refika Aditama.
- Rosenfeld, M., & Sajó, A. (2012). THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW. Oxford University Press.
- Setyagraha, J. A., Kuntalasari, I., & Sholikhah, D. I. (2026). IMPLIKASI HUKUM INTERNASIONAL TERHADAP SENGKETA KEPEMILIKAN DATA DIGITAL ANTARA NEGARA DAN KORPORASI GLOBAL. *Cerdika:*

Jurnal Ilmiah Indonesia, 6(2), 545–557.

<https://doi.org/10.59141/cerdika.v6i2.2961>

- Soekanto, S. (1986). *PENELITIAN HUKUM NORMATIF: SUATU TINJAUAN SINGKAT*. CV Rajawali.
- Solove, D. J., & Schwartz, P. M. (2019). *PRIVACY LAW FUNDAMENTALS*. International Association of Privacy Professionals.
- Sulaiman, S., Adli, M., & Mansur, T. M. (2019). KETIDAKTERATURAN HUKUM PENGAKUAN DAN PERLINDUNGAN MASYARAKAT HUKUM ADAT DI INDONESIA. *Law Reform*, 15(1), 12. <https://doi.org/10.14710/lr.v15i1.23352>
- Tracking Perkara MKRI. (n.d.-a). TRACKING PERKARA NOMOR 151/PUU-XXII/2024. Retrieved June 10, 2026, from <https://tracking.mkri.id/index.php?page=web.TrackPerkara&id=151/PUU-XXII/2024>
- Tracking Perkara MKRI. (n.d.-b). TRACKING PERKARA NOMOR 137/PUU-XXIII/2025. Retrieved June 10, 2026, from <https://tracking.mkri.id/index.php?page=web.TrackPerkara&id=137/PUU-XXIII/2025>
- Velasco Pufleau, M. (2024, June 10). THE EUROPEAN PARLIAMENT AND THE PROTECTION OF PRIVACY AND PERSONAL DATA: AN INSTITUTIONAL ANALYSIS OF ITS RESPONSE TO THE SCHREMS JUDGEMENTS. *Global Conference on Parliamentary Studies*. <https://orbilu.uni.lu/handle/10993/61376>
- Voigt, P., & von dem Bussche, A. (2024). *THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE*. Springer Nature Switzerland.
- Westin, A. F., & Solove, D. J. (2015). *PRIVACY AND FREEDOM*. IG Publishing.
- Wolford, B. (2018, November 7). WHAT IS GDPR, THE EU'S NEW DATA PROTECTION LAW? *GDPR.eu*. <https://gdpr.eu/what-is-gdpr/>
- Yokotani, Y., Kurnia, A. C., Wirazilmustaan, W., & Salfutra, R. D. (2025). PENGENDALIAN DATA PRIBADI DAN RUANG SIBER OLEH PLATFORM DIGITAL BIG DATA GLOBAL TERKAIT KEDAULATAN DIGITAL INDONESIA. *Progresif: Jurnal Hukum*, 19(1), 70–80. <https://doi.org/10.33019/cdt5p455>
- Zweigert, K., & Kötz, H. (1998). *INTRODUCTION TO COMPARATIVE LAW* (3rd rev. ed.). Clarendon Press; Oxford University Press.