Locus Journal of Academic Literature Review
Volume 5 Issue 1, January 2026.
P-ISSN: 2829-4262, E-ISSN: 2829-3827

Kajian Komparatif Perlindungan Data Pribadi Warga Negara Antara Indonesia dengan Malaysia

Muhammad Nur Aziz[1], M. Abdim Munib[2],-Mochamad Mansur[3].

[1.2.3.] *Fakultas Hukum, Universitas Bojonegoro.*
E-mail: Azizn2569@gmail.com (CA)

Abstrak: Penelitian ini menganalisis dan membandingkan pengaturan perlindungan hak subjek data pribadi di Indonesia dan Malaysia guna mengidentifikasi kelebihan serta kekurangan dari masing-masing regulasi dalam melindungi kedaulatan data individu. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perbandingan hukum (comparative approach) dan pendekatan perundang-undangan (statute approach), dengan merujuk pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia dan Personal Data Protection Act 2010 (Akta 709) di Malaysia. Hasil penelitian menunjukkan bahwa pengaturan di Indonesia memiliki keunggulan pada cakupan sektor yang komprehensif (publik dan privat) serta pengakuan hak portabilitas data dan perlindungan dari profilasi otomatis yang lebih modern. Sementara itu, pengaturan di Malaysia unggul dalam hal kemandirian finansial otoritas pengawas melalui Personal Data Protection Fund serta adanya kepastian hukum dalam penyelesaian sengketa melalui lembaga spesialis Appeal Tribunal. Perbedaan substansial ditemukan pada status kelembagaan pengawas dan teknis penegakan hukum, di mana Malaysia memiliki prosedur investigasi yang lebih independen dan spesifik, sedangkan Indonesia masih mengandalkan struktur birokrasi pemerintahan pusat dan penegakan hukum umum. Secara keseluruhan, perbandingan ini memberikan gambaran objektif mengenai model perlindungan data yang dapat memberikan jaminan keamanan lebih kuat bagi subjek data di era digital.

Kata Kunci: Kajian Komparatif, Perlindungan Data Pribadi, Indonesia, Malaysia.

Sitasi: Nur Aziz, M., Munib, M. A., & Mansur, M. (2026). Kajian Komparatif Perlindungan Data Pribadi Warga Negara Antara Indonesia dengan Malaysia. *Locus Journal of Academic Literature Review*, *5*(1), 110–123. https://doi.org/10.56128/ljoalr.v5i1.811

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan masif dalam pengumpulan, pemrosesan, dan pemanfaatan data pribadi di berbagai sektor, mulai dari layanan publik, perbankan, hingga media sosial. Data pribadi tidak lagi hanya digunakan sebagai sarana administratif, tetapi telah menjadi komoditas strategis yang bernilai ekonomi tinggi (Bagenda et al., 2025). Kondisi ini menimbulkan risiko serius terhadap hak privasi individu, terutama ketika data pribadi diproses tanpa persetujuan yang sah, disalahgunakan, atau mengalami kebocoran (Nasution, 2025). Seiring dengan akselerasi transformasi digital di ASEAN di mana nilai ekonomi digital

diperkirakan mencapai US$1 triliun pada tahun 2025, potensi kolaborasi regional seperti ASEAN *Digital Economy Framework Agreement* (DEFA) berpotensi terhambat, sehingga membahayakan hak privasi warga negara di tengah kemajuan teknologi inovatif seperti kecerdasan buatan atau AI dan big data ((IDC), 2023).

Di Indonesia, perkembangan perlindungan data pribadi telah menunjukkan kemajuan yang nyata melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur prinsip-prinsip esensial seperti persetujuan, keterbukaan, serta sanksi pidana maksimal enam tahun penjara atau denda hingga Rp 6 miliar bagi pelanggaran (Indonesia, 2022). Namun, pelaksanaannya masih dihadapkan pada berbagai kendala, di antaranya kekurangan lembaga pengawas independen yang efektif dan maraknya kasus kebocoran data. Data dari Badan Siber dan Sandi Negara (BSSN) mengindikasikan bahwa pada tahun 2023, lebih dari 1,2 miliar catatan data pribadi Indonesia mengalami kebocoran, termasuk insiden signifikan seperti pengungkapan 35 juta data pemilih Komisi Pemilihan Umum (KPU) pada Januari 2024 ((Kominfo), 2024). Fenomena ini menggarisbawahi bahwa penegakan hukum tetap lemah dengan hanya 15% kasus yang ditangani secara efektif.

Sebaliknya, di Malaysia, *Personal Data Protection* Act 2010 (PDPA) telah menjadi landasan utama, yang menitikberatkan pada pengumpulan data yang sah serta hak subjek data untuk mengakses dan mengoreksi informasi. Lembaga pengawas seperti Personal *Data Protection Commissioner* (PDPC) telah memproses ribuan keluhan, dengan sanksi administratif hingga RM500.000 (setara dengan sekitar Rp.1,8 miliar). Meskipun begitu, kondisi terkini menunjukkan keterbatasan, khususnya dalam menangani data lintas batas dan sektor digital yang baru muncul. Laporan PDPC Malaysia mencatat bahwa pada tahun 2022, terdapat 1.248 pengaduan terkait pelanggaran data, termasuk kasus mencolok seperti kebocoran data 22 juta pengguna aplikasi MySejahtera selama pandemi COVID-19 (PDPC Malaysia, 2023).Kedua negara ini masih bergantung pada kerangka ASEAN yang belum sepenuhnya terintegrasi sehingga rentan terhadap disparitas dalam penegakan hukum.

Kolaborasi regional melalui inisiatif ASEAN, khususnya ASEAN *Framework on Digital Data Governance* (2021) menempati posisi sentral dalam mengatasi fragmentasi regulasi yang masih menghambat koherensi kebijakan di Indonesia dan Malaysia. Meskipun kedua negara telah menunjukkan upaya penyesuaian kebijakan nasional dengan kerangka regional, perbedaan pendekatan dalam implementasi seperti dominasi sanksi pidana dalam sistem Indonesia dibandingkan pendekatan administratif di Malaysia mengindikasikan perlunya pendekatan analitis yang mendalam. Tanpa komitmen kerja sama yang lebih kuat, pemain global seperti perusahaan teknologi multinasional kerap memanfaatkan celah regulasi untuk mengumpulkan data tanpa izin yang sah. Oleh karenanya, kajian ini memberikan basis

penting bagi penguatan kerja sama regional guna membangun ekosistem data yang terkoordinasi dan resilien.

Kajian komparatif ini esensial untuk mengisi kekosongan penelitian yang ada, di mana mayoritas studi sebelumnya lebih menitikberatkan pada perbandingan dengan standar global seperti GDPR ketimbang antarnegara ASEAN. Justifikasi utamanya terletak pada dukungan terhadap harmonisasi kebijakan regional guna melindungi data pribadi lintas batas yang saat ini masih terfragmentasi. Penelitian ini berpotensi menyediakan rekomendasi praktis, misalnya dengan mengadopsi kerangka pengawasan mandiri ala Malaysia ke dalam konteks Indonesia atau memperkuat mekanisme sanksi pidana bergaya Indonesia di Malaysia. Dengan populasi digital Indonesia yang mencapai 215 juta pengguna internet dan Malaysia 29 juta, ketidakmerataan implementasi dapat memicu eksploitasi data oleh aktor eksternal. Kajian ini juga memiliki relevansi akademis dalam memperkaya wacana hukum internasional di ASEAN (Greenleaf, 2018).

Pada tingkat global, kerugian ekonomi akibat kejahatan siber yang diproyeksikan mencapai US$10,5 triliun per tahun pada 2025 menunjukkan besarnya risiko yang dihadapi, terutama karena ketergantungan tinggi pada layanan digital asing (prnewswire.com, tanpa tahun). Kajian komparatif mengenai UU PDP Indonesia dan PDPA Malaysia menjadi penting untuk melihat bagaimana kedua regulasi dapat diselaraskan dengan standar internasional guna mencegah eksploitasi lintas batas. Implementasi hasil kajian ini berpotensi mendukung stabilitas kawasan di tengah tantangan fragmentasi hukum dan ketergantungan pada teknologi asing (Antaranews.com, tanpa tahun). Berdasarkan uraian tersebut peneliti tertarik untuk melakukan penelitian dalam bentuk skripsi yang berjudul "Kajian Komparatif Perlindungan Data Pribadi Warga Negara Antara Indonesia Dengan Malaysia".

2. Metode Penelitian

Jenis penelitian ini adalah penelitian hukum normatif (*normative law*). Sebagaimana dikemukakan oleh Peter Mahmud Marzuki bahwa penelitian hukum normatif merupakan pendekatan utama dalam ilmu hukum karena hukum bersifat normatif secara inheren. Ia bertujuan untuk menganalisis norma hukum yang berlaku (*positive law*) secara sistematis, dengan fokus pada interpretasi, sistematisasi, dan evaluasi norma untuk mencapai pemahaman yang koheren tentang 'apa yang seharusnya' (*sollen*) dalam tatanan hukum. Dalam era digital saat ini, metode ini tetap relevan untuk mengkritik norma-norma baru seperti regulasi data pribadi, di mana norma harus diuji terhadap prinsip konstitusional (Marzuki, 2023).

Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menganalisis secara mendalam semua regulasi dan undang-undang yang relevan dengan isu hukum yang sedang dibahas. Selain itu, digunakan pendekatan konseptual (*conceptual approach*) yang bertujuan menggali ide-ide yang melahirkan pengertian dan prinsip hukum guna membangun argumentasi hukum yang efektif dalam memecahkan permasalahan hukum kontemporer. Sebagai inti dari kajian ini, digunakan pendekatan komparatif (*comparative approach*) dengan membandingkan pengaturan hukum di Indonesia dan Malaysia untuk memperoleh persamaan dan perbedaan di antara peraturan hukum tersebut.

Sumber bahan hukum dalam skripsi ini mencakup bahan hukum primer yang terdiri dari UUD NRI Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan *Personal Data Protection Act* (PDPA) Tahun 2010 Malaysia. Selain itu, digunakan bahan hukum sekunder berupa publikasi tentang hukum yang bukan merupakan dokumen resmi, seperti buku dan jurnal. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan mengklasifikasikan data yang relevan baik secara *offline* maupun *online*. Analisis dilakukan secara kualitatif dengan interpretasi mendalam terhadap aturan hukum yang berlaku untuk mengungkapkan tingkat keefektifan perlindungan hukum serta mengajukan rekomendasi regulasi di Indonesia.

3. Hasil & Pembahasan

3.1. Pengaturan Perlindungan Data Pribadi di Indonesia dan Malaysia

Pengaturan perlindungan data pribadi di Indonesia telah mengalami evolusi yang sangat signifikan dari yang semula bersifat sektoral dan tersebar di berbagai peraturan perundang-undangan menjadi sebuah regulasi yang komprehensif melalui pengundangan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Wibowo et al., 2025). Secara fundamental, landasan filosofis perlindungan data pribadi di Indonesia berakar pada konstitusi, yaitu Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya (Ikrom & Tamam, 2024).

Hak konstitusional ini menjadi ruh utama yang melatarbelakangi perlunya negara hadir untuk memberikan kepastian hukum di tengah masifnya digitalisasi dan ancaman penyalahgunaan data dalam ruang siber yang tanpa batas. Sebelum adanya UU PDP, masyarakat Indonesia seringkali mengalami kekosongan hukum ketika terjadi kebocoran data,(Lustarini, 2023) mengingat aturan yang ada seperti dalam UU ITE atau UU Administrasi Kependudukan belum mampu menjangkau aspek perlindungan data secara holistik dari sisi hak subjek data maupun kewajiban pengendali data.

Dalam tatanan normatif UU PDP, perlindungan data pribadi diposisikan sebagai bagian dari hak asasi manusia yang harus dijunjung tinggi dalam setiap proses pengolahan data, baik oleh instansi publik maupun privat (Jdih.komdigi.go.id, tanpa tahun.). UU PDP memberikan definisi yang jelas mengenai data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lain baik secara langsung maupun tidak langsung melalui elektronik atau nonelektronik (Jdih.komdigi.go.id, tanpa tahun).

Pembagian kategori data pribadi di Indonesia menunjukkan bahwa negara menerapkan pendekatan berbasis risiko (*risk-based approach*) dalam memberikan perlindungan. Data pribadi spesifik mencakup informasi yang memiliki risiko tinggi bagi pemiliknya jika bocor, seperti data kesehatan, biometrik, genetika, catatan kejahatan, data anak, dan data keuangan pribadi. Pembagian ini memastikan bahwa data yang lebih sensitif mendapatkan standar pengamanan dan perlakuan hukum yang lebih ketat dibandingkan dengan data pribadi yang bersifat umum.

Pilar utama dalam pengaturan perlindungan data di Indonesia adalah penempatan Subjek Data sebagai pemegang hak tertinggi atas informasi miliknya, yang secara eksplisit diatur dalam Bab IV UU PDP. Hak-hak tersebut mencakup hak untuk mendapatkan informasi tentang kejelasan identitas pengendali data, hak untuk melengkapi, memperbarui, dan memperbaiki kesalahan data. Indonesia juga mengakui hak untuk menarik kembali persetujuan pemrosesan data sebagai bentuk kedaulatan warga negara terhadap informasi pribadinya.

Selain itu, Indonesia mengakui hak yang sangat krusial dalam dunia digital, yaitu hak untuk mengakhiri pemrosesan, menghapus, dan memusnahkan data pribadi (*right to be forgotten*) (Hukum.uma, 2025). Penegasan hak-hak ini memberikan perlindungan bagi warga negara Indonesia terhadap data mereka sendiri, yang sebelumnya seringkali dieksploitasi oleh perusahaan teknologi atau pihak ketiga tanpa adanya transparansi dan mekanisme kontrol yang memadai dari sisi pemilik data atau subjek data.

Kewajiban Pengendali Data Pribadi menjadi fokus utama dalam implementasi UU PDP untuk menjamin bahwa setiap proses dilakukan secara akuntabel (Hutapea, 2021). Dalam Pasal 20 ayat (1) dan (2) menetapkan, pengendali data wajib memiliki dasar hukum yang kuat sebelum melakukan pemrosesan, baik itu berupa persetujuan eksplisit dari subjek data, pemenuhan kewajiban kontrak, kewajiban hukum, atau untuk kepentingan publik yang sah.[9] Hal ini menuntut tanggung jawab penuh dari pihak yang mengelola data masyarakat.

Prinsip-prinsip pelindungan data pribadi, termasuk pengumpulan terbatas dan penjaminan akurasi data, ditegaskan dalam Pasal 16 ayat (2) UU PDP. Sementara itu,

kewajiban hukum bagi pengendali data untuk menyampaikan pemberitahuan tertulis kepada subjek data dan lembaga pengawas dalam waktu paling lama 3 kali 24 jam apabila terjadi kegagalan pelindungan data diatur secara tegas dalam Pasal 46 ayat (1) UU PDP. Langkah ini bertujuan untuk memitigasi dampak kerugian yang lebih luas bagi warga negara.

Peran Pejabat Pelindungan Data atau *Data Protection Officer* (DPO) sangat strategis sebagai jembatan antara organisasi, subjek data, dan lembaga pengawas guna memastikan kepatuhan internal terhadap regulasi. Keberadaan DPO diharapkan dapat mengubah budaya organisasi di Indonesia agar lebih peduli terhadap privasi sebagai sebuah standar operasional. Hal ini berkaitan erat dengan latar belakang perlunya perlindungan data sebagai syarat mutlak dalam membangun kepercayaan ekonomi digital dan integritas tata kelola pemerintahan berbasis elektronik (SPBE) (Hukumonline, 2022).

Aspek penegakan hukum dalam UU PDP Indonesia mencakup sanksi administratif dan sanksi pidana yang cukup progresif guna memberikan efek jera terhadap para pelanggar. Denda administratif yang nilainya dapat mencapai paling tinggi 2 persen dari pendapatan tahunan terhadap variabel pelanggaran tersebut ditegaskan dalam Pasal 57 ayat (3) UU PDP, yang menunjukkan keseriusan pemerintah Indonesia dalam menyelaraskan standarnya dengan regulasi global seperti GDPR di Eropa (Simanjuntak, 2024). Indonesia telah meletakkan fondasi yang kokoh untuk melindungi privasi warganya di abad digital (Suleiman et al., 2020).

Pengaturan perlindungan data pribadi di Malaysia secara komprehensif diatur dalam Personal Data *Protection Act* 2010 (Akta 709), yang menjadi tonggak sejarah sebagai salah satu regulasi perlindungan data pertama di wilayah Asia Tenggara. Melalui Akta 709, Malaysia menegaskan bahwa perlindungan data bukan hanya sekadar isu teknis, melainkan kewajiban hukum yang memiliki konsekuensi serius bagi siapa pun yang bertindak sebagai pengguna data (data user) (Negoro & Purwanto, 2024). Inti dari pengaturan di Malaysia terletak pada tujuh Prinsip Perlindungan Data Pribadi yang wajib dipatuhi, mulai dari prinsip umum, pemberitahuan dan pilihan, hingga prinsip akses. Persetujuan dari subjek data menjadi fondasi utama sebelum pemrosesan dilakukan sebagaimana ditegaskan dalam Pasal 6 (1), yang memastikan kedaulatan individu atas informasinya dihormati sejak tahap awal pengumpulan data (Citra et al., 2023).

Malaysia memberikan perhatian khusus pada transparansi melalui Prinsip Notis dan Pilihan di mana berdasarkan Pasal 7 (1), pengguna data wajib memberikan pemberitahuan tertulis mengenai jenis data dan tujuan pemrosesan. Ketentuan dalam Pasal 7 ayat (2) mewajibkan pemberitahuan tersebut disampaikan dalam Bahasa

Malaysia dan Bahasa Inggris untuk memastikan pemahaman luas bagi subjek data.Secara kelembagaan, Akta 709 menonjolkan peran Komisioner Perlindungan Data Pribadi sebagai badan hukum tunggal (*corporation sole*) yang diangkat oleh Menteri dengan kekuasaan luas untuk mengawasi implementasi undang-undang. Pengawasan preventif juga diterapkan melalui sistem pendaftaran wajib bagi kelas pengguna data tertentu dalam sektor strategis seperti perbankan dan kesehatan guna memastikan standar perlindungan yang memadai sebelum beroperasi.

Hak subjek data dijamin secara eksplisit dalam Pasal 30 (1) yang memberikan wewenang bagi individu untuk mengakses dan memperoleh salinan data miliknya agar akurasi informasi tetap terjaga. Selain itu, Pasal 43 (1) memberikan kontrol kepada individu untuk menghentikan pemrosesan data untuk tujuan pemasaran langsung yang sering mengganggu privasi (Pratiwi, 2024). Dalam hal penegakan hukum, Komisioner memiliki kekuatan investigasi setara aparat kepolisian, termasuk wewenang penggeledahan dan penyitaan alat elektronik. Untuk menjamin keadilan bagi pihak yang merasa dirugikan oleh keputusan Komisioner, dibentuk pula Tribunal Banding (*Appeal Tribunal*) sebagai jalur formal peninjauan kembali sebagaimana diatur dalam Pasal 83.

Mengenai transfer data ke luar wilayah, Pasal 129 (1) melarang pemindahan data pribadi ke luar Malaysia kecuali ke negara yang masuk dalam daftar putih (whitelist) pilihan Menteri (Pitchan & Omar, 2019).Penegakan hukum dalam Akta 709 juga menyentuh tanggung jawab kolektif pengurus korporasi, di mana direktur atau kepala eksekutif dapat dianggap melakukan pelanggaran jika badan hukum tersebut terbukti melanggar aturan. Meskipun memiliki sanksi pidana yang berat, Malaysia tetap mengenal mekanisme kompensasi atau damai administratif untuk efisiensi penegakan hukum pada pelanggaran teknis. Melalui struktur yang detail dan perlindungan terhadap informan (*whistleblower*), Akta 709 tidak hanya melindungi privasi individu tetapi juga memperkuat posisi Malaysia sebagai destinasi investasi digital yang aman dan terpercaya di kancah global.

3.2. Kelebihan dan Kekurangan Pengaturan Perlindungan Hak Subjek Data Pribadi di Indonesia dan Malaysia

Terdapat beberapa perbedaan yang dapat dianalisis sebagai kajian komparatif. Pertama, dalam hal sektor pengawasannya, Indonesia menganut model perlindungan yang lebih komprehensif sebagaimana diatur dalam Pasal 2 UU PDP, yang menjangkau subjek hukum baik di sektor publik maupun sektor privat tanpa pengecualian. Hal ini berbeda secara fundamental dengan Malaysia yang dalam Pasal 3 PDPA 2010 secara tegas mengecualikan sektor pemerintahan dan hanya membatasi keberlakuan undang-undang pada transaksi komersial.

Perbedaan ini menunjukkan bahwa subjek data di Indonesia memiliki perlindungan hukum yang sama kuatnya saat berhadapan dengan instansi negara maupun perusahaan swasta, sementara di Malaysia, perlindungan terhadap penyalahgunaan data oleh otoritas publik harus dicari melalui instrumen hukum administratif atau konstitusional lainnya di luar Akta 709. Dari sisi status kelembagaan, Indonesia memilih struktur lembaga yang berada di bawah wewenang Presiden berdasarkan Pasal 58 UU PDP, yang menunjukkan adanya sentralisasi kebijakan di tingkat eksekutif (Mahameru et al., 2023). Di sisi lain, Malaysia menonjolkan independensi administratif melalui pembentukan Komisioner sebagai badan hukum tunggal (*corporation sole*) menurut Pasal 47 PDPA 2010. Perbedaan status ini berimplikasi pada fleksibilitas operasional, lembaga di Malaysia memiliki kewenangan hukum untuk memiliki aset, menandatangani kontrak, dan menuntut secara mandiri di pengadilan, sedangkan lembaga di Indonesia sangat bergantung pada struktur organisasi pemerintah dan regulasi birokrasi yang ditetapkan melalui Keputusan Presiden.

Mengenai hak portabilitas data, Indonesia jauh lebih maju dengan mengadopsi standar global modern dalam Pasal 13 UU PDP yang memberikan hak kepada subjek data untuk memindahkan data pribadinya antar pengendali data dalam format yang umum digunakan. Hak ini sangat krusial dalam ekonomi digital untuk mencegah penguncian data (*data lock-in*) oleh platform besar, sehingga persaingan usaha menjadi lebih sehat (Chushair et al., 2025). Sebaliknya, Malaysia tidak mengatur hak portabilitas ini dalam PDPA 2010, yang mencerminkan bahwa regulasi tersebut lahir pada era di mana interoperabilitas data belum menjadi isu utama dalam transaksi komersial dibandingkan pada saat UU PDP Indonesia disusun.

Dalam hal mekanisme keberatan hukum, Malaysia memiliki sistem efektif melalui pembentukan *Appeal* Tribunal (Tribunal Banding) berdasarkan Pasal 83 PDPA 2010. Lembaga semi yudisial ini memungkinkan subjek data atau pengguna data untuk menyanggah keputusan Komisioner secara cepat tanpa harus melalui kerumitan prosedur pengadilan umum. Indonesia, meskipun mengakui hak keberatan dalam Pasal 12 UU PDP, belum memiliki lembaga spesialis serupa, sehingga sengketa data pribadi kemungkinan besar akan bermuara pada mediasi Lembaga Pengawas atau gugatan perdata di Pengadilan Negeri, yang secara praktis memakan waktu dan biaya lebih besar bagi subjek data.

Sistem transfer data luar negeri juga menunjukkan perbedaan yang, di mana Malaysia menggunakan pendekatan *whitelist* (daftar putih) berdasarkan Pasal 129 PDPA 2010. Dalam sistem ini, transfer data hanya diperbolehkan ke negara-negara yang secara eksplisit disetujui oleh Menteri. Sementara itu, Pasal 56 UU PDP Indonesia memberikan fleksibilitas lebih melalui beberapa lapisan syarat, mulai dari tingkat perlindungan setara, adanya kontrak standar yang mengikat, hingga persetujuan langsung dari

subjek data. Pendekatan Indonesia ini lebih memudahkan arus data global bagi pelaku usaha multinasional dibandingkan pendekatan Malaysia yang sangat bergantung pada pembaruan daftar negara oleh otoritas pemerintah.

Terkait perlindungan terhadap teknologi otomatis, Pasal 10 UU PDP Indonesia secara eksplisit memberikan hak kepada subjek data untuk tidak tunduk pada keputusan yang didasarkan hanya pada pemrosesan otomatis atau profilasi yang menimbulkan efek hukum (Lexology.com, 2024). Ketentuan ini merespons kemajuan teknologi kecerdasan buatan (AI) dan algoritma yang dapat merugikan hak-hak individu secara tidak terlihat. Dalam PDPA 2010 Malaysia, perlindungan terhadap pengambilan keputusan otomatis ini tidak diatur secara detail, sehingga subjek data di Malaysia memiliki perlindungan yang lebih lemah dalam menghadapi penggunaan algoritma profilasi oleh perusahaan komersial (Afifah, 2023).

Terakhir, mengenai batas waktu pengaduan, Malaysia memberikan kepastian hukum melalui Pasal 106 PDPA 2010 yang menetapkan daluwarsa selama 2 tahun sejak subjek data mengetahui adanya pelanggaran. Ketentuan ini bertujuan untuk mencegah adanya tuntutan hukum yang sudah kedaluwarsa dan mendorong subjek data untuk aktif menjaga haknya. Di sisi lain, Dalam Pasal 15 ayat (1) huruf a dan Pasal 64 UU PDP, subjek data diberikan hak untuk mengajukan keberatan dan menyelesaikan sengketa. Namun, sepanjang isi Pasal 64 hingga Pasal 66 yang mengatur tentang Penyelesaian Sengketa dan Hukum Acara, UU PDP tidak mencantumkan batas waktu bagi subjek data untuk melaporkan pelanggaran administratif kepada Lembaga Pengawas. Oleh sebab itu, di satu sisi menguntungkan subjek data karena memberikan waktu lebih luas, namun di sisi lain dapat menimbulkan ketidakpastian bagi pengendali data terkait potensi tuntutan di masa depan.

Salah satu kelebihan utama UU No. 27 Tahun 2022 (UU PDP) Indonesia terletak pada jangkauan hukumnya yang komprehensif sebagaimana diatur dalam Pasal 2, yang mencakup sektor publik dan privat secara setara. Hal ini menjamin bahwa hak subjek data tetap terlindungi meskipun data tersebut dikelola oleh instansi pemerintah. Sementara di dalam PDPA 2010 Malaysia yang dalam Pasal 3 justru mengecualikan kekuasaan pemerintah dari kewajiban perlindungan data. Dengan demikian, Indonesia memiliki standar keadilan yang lebih merata bagi warga negara dalam menuntut akuntabilitas dari pemegang data mana pun, baik perusahaan komersial maupun birokrasi negara.

Namun, kekurangan signifikan dari regulasi Indonesia adalah ketergantungan finansial lembaga pengawas pada APBN, yang berbeda jauh dengan kemandirian PDPA 2010 Malaysia melalui personal data protection fund yang termaktub dalam Pasal 61. Malaysia memiliki kelebihan dalam keberlanjutan operasional karena dana tersebut

dikelola secara mandiri dari biaya pendaftaran pengguna data sebagaimana ketentuannya dalam Pasal 61 "(1) For the purposes of this Act, a fund to be known as the "Personal Data Protection Fund" is established. (2) The Fund shall be controlled and administered by the Commissioner."yang artinya, (1) Untuk tujuan Akta ini, sebuah dana yang dikenal sebagai "Dana Perlindungan Data Pribadi" dibentuk. (2) Dana tersebut harus dikendalikan dan dikelola oleh Komisioner. Tanpa kemandirian dana, lembaga pengawas di Indonesia berisiko mengalami hambatan kinerja apabila terjadi efisiensi anggaran di tingkat pusat, yang pada akhirnya dapat melemahkan pengawasan terhadap hak-hak subjek data (Pratiwi, 2024).

Kelebihan lain dari pengaturan di Malaysia adalah adanya mekanisme Appeal Tribunal yang termaktub dalam Pasal 83, yang memberikan kepastian hukum bagi subjek data melalui jalur semi-yudisial yang cepat dan spesialis. Hal ini merupakan kekurangan pada sistem Indonesia yang belum memiliki lembaga banding khusus, sehingga sengketa data di Indonesia cenderung berlarut-larut karena harus melalui mediasi lembaga pengawas atau pengadilan umum yang padat perkara. Keberadaan tribunal di Malaysia memastikan bahwa setiap keberatan terhadap keputusan Komisioner dapat diselesaikan oleh para ahli hukum yang memahami seluk-beluk privasi digital secara mendalam.

Dari sisi teknologi masa depan, Indonesia unggul dengan adanya perlindungan terhadap pemrosesan otomatis dan profilasi dalam Pasal 10 UU PDP. Kelebihan ini menjawab tantangan era kecerdasan buatan (AI) di mana data sering kali diolah algoritma untuk mengambil keputusan yang merugikan individu tanpa keterlibatan manusia. Sebaliknya, kekurangan PDPA 2010 Malaysia adalah belum adanya pasal yang secara eksplisit mengatur hak subjek data untuk keberatan terhadap pengambilan keputusan otomatis, sehingga warga Malaysia memiliki kerentanan lebih tinggi terhadap diskriminasi algoritma di sektor komersial.

Dalam hal penegakan hukum administratif, Malaysia memiliki keunggulan melalui Pasal 106 yang mengatur daluwarsa pengaduan selama 2 tahun sejak subjek data mengetahui pelanggaran. Hal ini memberikan kejelasan durasi tanggung jawab bagi pengendali data. Di sisi lain, Indonesia memiliki kekurangan karena tidak mengatur batas waktu pengetahuan (*actual knowledge*) secara tegas dalam UU PDP, yang meskipun tampak menguntungkan subjek data, namun secara hukum administratif dapat menciptakan ketidakpastian bagi pelaku usaha terkait masa berlaku ancaman sanksi atas data yang pernah mereka olah di masa lampau.

Kelebihan instrumen investigasi di Malaysia juga terlihat pada kewenangan pejabat berwenang yang memiliki kekuatan setara polisi dalam hal penyitaan dan penggeledahan, termasuk akses ke data terenkripsi berdasarkan Pasal 115 PDPA 2010.

Hal ini merupakan kekuatan represif yang sangat efektif untuk mengamankan bukti digital sebelum sempat dimusnahkan. Di Indonesia, meskipun UU PDP mengatur sanksi berat, teknis penggeledahan paksa masih sangat bergantung pada koordinasi dengan penyidik Polri sesuai KUHAP, yang dalam praktiknya bisa memakan waktu koordinasi lebih lama dibandingkan otoritas Malaysia yang memiliki wewenang tersebut secara inheren.

Selanjutnya, kekurangan dari sistem Malaysia adalah ketidakhadiran hak portabilitas data yang merupakan standar emas perlindungan data modern. Indonesia melalui Pasal 13 UU PDP memberikan kelebihan berupa hak bagi subjek data untuk memindahkan datanya antar platform, yang mendorong kompetisi usaha dan mencegah monopoli data. Tanpa hak ini, pengguna jasa digital di Malaysia cenderung terkunci pada satu penyedia layanan karena kesulitan teknis untuk memindahkan data mereka secara mandiri, yang secara tidak langsung melemahkan kedaulatan subjek data atas informasinya sendiri.

Terakhir, regulasi Malaysia memiliki kelebihan dalam perlindungan saksi dan informan yang sangat detail melalui Pasal 140, yang bahkan mewajibkan pengadilan untuk menutupi identitas pelapor dalam dokumen bukti. Indonesia, meskipun memiliki UU Perlindungan Saksi dan Korban secara umum, tidak mengatur proteksi khusus bagi *whistleblower* data dalam teks utama UU PDP-nya. Hal ini menjadi catatan kekurangan bagi Indonesia, karena tanpa jaminan kerahasiaan identitas yang kuat di dalam regulasi privasi itu sendiri, masyarakat mungkin merasa enggan untuk melaporkan pelanggaran data pribadi yang melibatkan entitas besar atau pengaruh kekuasaan.

4. Penutup

Pengaturan perlindungan data pribadi di Indonesia melalui UU No. 27 Tahun 2022 (UU PDP) memiliki karakter yang komprehensif karena menjangkau sektor publik dan privat, serta mengadopsi hak-hak modern seperti portabilitas data dan perlindungan dari profilasi otomatis sesuai standar global. Sebaliknya, PDPA 2010 Malaysia (Akta 709) memiliki karakter yang lebih spesifik pada sektor komersial dengan struktur otoritas yang sangat mapan, di mana kekuasaan eksekutif Malaysia memfokuskan perlindungan pada integritas pasar digital melalui sistem pendaftaran pengguna data dan pengawasan ketat oleh Komisioner yang didukung oleh institusi spesialis seperti Tribunal Banding. Perbandingan antara kedua regulasi tersebut menunjukkan bahwa masing-masing negara memiliki keunggulan kompetitif. Indonesia unggul dalam hal pengakuan hak subjek data yang progresif dan cakupan hukum yang luas, namun masih memiliki kelemahan pada aspek kemandirian anggaran dan ketiadaan lembaga banding khusus. Di sisi lain, Malaysia memiliki keunggulan dalam kemandirian finansial melalui Personal Data Protection Fund (Pasal 61) dan kepastian hukum dalam

penyelesaian sengketa melalui Appeal Tribunal (Pasal 83), meskipun memiliki kekurangan fundamental pada pengecualian sektor publik dari jangkauan undang-undang serta belum diaturnya hak portabilitas data bagi warganya.

Referensi

(IDC), I. D. C. (2023). *Asia Pacific Cybersecurity Report 2022*.

(Kominfo), K. K. dan I. (2024). *Laporan Kebocoran Data Nasional 2023*. Kominfo.

Afifah, Y. (2023). *Pakar Hukum Siber UNAIR Jelaskan Prinsip Perlindungan Data Pribadi*. fh.unair. https://fh.unair.ac.id/pakar-hukum-siber-unair-jelaskan-prinsip-perlindungan-data-pribadi/

Antaranews.com. (n.d.). *CIPS: Kesenjangan peraturan data hambat ekonomi digital ASEAN*. antaranews.com.

Bagenda, C., Harimurti, D. A., Djou, A. M. G., Rustam, Bosco, Y. D., & Watu. (2025). Legalitas Monetisasi Data Pengguna Oleh Perusahaan Teknologi: Analisis Perlindungan Konsumen Dan Hukum Perekonomian Nasional. *Jurnal Kolaboratif Sains2*, *Vol. 8*(2), 8708–8716.

Chushair, S. M., Fithry, A., & Rusfandi. (2025). Perlindungan Hukum Bagi Korban Atas Kebocoran Pusat Data Nasional Sementara (PDNS) Perspektif Perlindungan Data Pribadi. *Jurnal Jendela Hukum*, *Vol. 12*(2), 89–122.

Citra, M. E. A., Munir, A. B., Lanang, K. S., P.Perbawa, Julianti, L., Aryamisra, I. D. G. A., Dita, N. W., & Maharani. (2023). Perlindungan Hukum Terhadap Data Diri Pribadi Di Era Ekonomi Digital: Peluang Dan Tantangan (Studi Komparasi Indonesia Dan Malaysia). *Jurnal Hukum Saraswati (JHS)*, *Vol. 5*(2), 519–534. https://doi.org/10.36733/jhshs.v5i2 %0D

Greenleaf, G. (2018). *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press. https://doi.org/10.1093/oso/9780198753673.001.0001

Hukum.uma. (2025). *Perlindungan Data Pribadi: Pilar Hak Digital di Era Informasi*. https://hukum.uma.ac.id/perlindungan-data-pribadi-pilar-hak-digital-di-era-informasi/

Hukumonline. (2022). *Bedah UU PDP: Perbedaan Pengendali vs Prosesor Data Pribadi*. https://www.hukumonline.com/berita/a/bedah-uu-pdp--perbedaan-pengendali-vs-prosesor-data-pribadi-lt63460658550b0/

Hutapea, S. A. (2021). Right To Be Forgotten Sebagai Bentuk Rehabilitasi Bagi Korban Pelanggaran Data Pribadi. *Jurnal Jurisprudentia*, *Vol. 1*(1), 1–10. https://jurisprudentia.bunghatta.ac.id/

Ikrom, M. B. F. D., & Tamam, B. (2024). Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia. *Constitution Journal*, *Vol. 3*(2), 140–154.

Indonesia, R. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Sekretariat Negara.

Jdih.komdigi.go.id. (n.d.). *Perlindungan Data Pribadi*. https://jdih.komdigi.go.id/infografis/view/19

Lexology.com. (2024). *Overview of Amendments to the Malaysian Personal Data Protection Act 2010*. https://www.lexology.com/library/detail.aspx?g=69c66cb8-6720-4758-aeba-72a0ca22729d

Lustarini, M. (2023). Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022. *Jurnal Hukum*. https://jdih.komdigi.go.id/artikel_hukum/artikel-hukum/t/jurnal-hukum/83

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., Badjeber, Haikal, M., & Rahmadia. (2023). Implementasi Uu Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia. *Jurnal Esensi Hukum*, *Voo. 5*(2), 115–131.

Malaysia, P. D. P. C. (PDPC). (2023). *Annual Report on Data Protection Complaints 2023*. PDPC.

Marzuki, P. M. (2023). *Penelitian Hukum : Edisi Revisi*. K E N C A N A.

Nasution, S. H. (2025). *Tata Kelola Data dan Perlindungan Data Pribadi melalui ASEAN Digital Masterplan 2025*. cips.indonesia.org. https://www.cips-indonesia.org/publications/tata-kelola-data-dan-perlindungan-data-pribadi-melalui-asean-digital-masterplan-2025?lang=id#:~:text=Ekonomi digital di ASEAN bertumbuh,ekosistem digital yang aman dan

Negoro, D. G., & Purwanto, G. H. (2024). Customer Data Protection by Bank Rakyat Indonesia is Reviewed by Law Number 27 of 2022 Concerning Personal Data. *Legal Brief*, *Vol. 13*(2), 246–254.

Pitchan, M. A., & Omar, S. Z. (2019). Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang. *Jurnal Komunikasi: Malaysia Journal of comunication*, *1*. https://www.academia.edu/download/74414424/9178.pdf

Pratiwi, N. R. N. (2024). Desain Formulasi Pengaturan Social Commercedi Indonesia Perspektif Maslahah Mursalah (Studi Perbadingan Hukum Malaysia Dan Indonesia). *Skripsi*.

prnewswire.com. (n.d.). *Kejahatan Siber Akan Merugikan Dunia $10,5 Triliun Setiap Tahunnya pada Tahun 2025*. prnewswire.com.

Simanjuntak, P. H. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). *Jurnal Esensi Hukum*, *Vol. 6*(2), 105–124.

Suleiman, A., Audrin, P., & Dewaranu, T. (2020). Pengaturan Bersama dalam Perlindungan Data Pribadi: Potensi Peran Asosiasi Industri sebagai Organisasi Regulator Mandiri. *Makalah Kebijakan No. 50*. https://repository.cips-indonesia.org/media/publications/555906-pengaturan-bersama-dalam-perlindungan-da-4a68a0d2.pdf

Wibowo, Y., DPW, I. A., & Ismiyanto. (2025). Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi. *Jurnal Serambi Hukum*, *Vol. 18*(1), 1–6.

****