BAB III

PEMBAHASAN

A. Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Malaysia

1. Pengaturan Perlindungan Data Pribadi Di Indonesia dalam Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi

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).[21] 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.[22]

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

---

[21] Yulianto Wibowo, Ida Aryati DPW, dan Ismiyanto, 2025, *Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi*, Jurnal Serambi Hukum, Vol. 18 No. 1, hal. 2.

[22] Moh Bagas Fadhli Dzil Ikrom dan Badrut Tamam, 2024, *Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia*, Constitution Journal, Vol. 3 No. 2, hal. 140.

yang tanpa batas. Sebelum adanya UU PDP, masyarakat Indonesia seringkali mengalami kekosongan hukum ketika terjadi kebocoran data,[23] 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.[24] 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 normatif UU PDPelektronik atau nonelektronik.[25]

UU PDP juga secara khusus membagi data pribadi ke dalam dua kategori. Di dalam Pasal 4 dijabarkan:

> " (1) Data Pribadi yang bersifat spesifik sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf a meliputi: a. data dan informasi kesehatan; b. data biometrik; c. data genetika; d. catatan kejahatan; e. data anak; f. data keuangan pribadi; dan/atau g. data lainnya sesuai dengan ketentuan peraturan perundang-undangan. (2) Data Pribadi yang bersifat umum sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf b meliputi: a. nama lengkap; b. jenis kelamin; c. kewarganegaraan; d. agama; e. status perkawinan; dan/atau f. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang."

---

[23] Mediodecci Lustarini, 2023, *Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022*, Jurnal Hukum, Kementerian Komunikasi dan Digital, hal. 2, https://jdih.komdigi.go.id/artikel_hukum/artikel-hukum/t/jurnal-hukum/83.

[24] Jdih.komdigi.go.id, "Perlindungan Data Pribadi," jdih.komdigi.go.id, tanpa tahun, https://jdih.komdigi.go.id/infografis/view/19.

[25] Penjelasan Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

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

Pilar utama dalam pengaturan perlindungan data di Indonesia adalah penempatan Subjek Data sebagai pemegang hak tertinggi atas informasi miliknya,[26] yang secara eksplisit diatur dalam Bab IV UU PDP. Hak-hak tersebut mencakup hak untuk mendapatkan informasi tentang kejelasan identitas dan dasar kepentingan hukum pengendali data, hak untuk melengkapi, memperbarui, dan memperbaiki kesalahan data, serta hak untuk mengakses dan mendapatkan salinan data pribadi miliknya.

Selain itu, Indonesia juga mengakui hak yang sangat krusial dalam dunia digital, yaitu hak untuk mengakhiri pemrosesan, menghapus, dan memusnahkan data pribadi (*right to be forgotten*), serta hak untuk menarik kembali persetujuan pemrosesan data. [27] Penegasan hak-hak ini

[26] Hukum.uma, "Perlindungan Data Pribadi: Pilar Hak Digital Di Era Informasi," hukum.uma.ac.id, 2025, https://hukum.uma.ac.id/perlindungan-data-pribadi-pilar-hak-digital-di-era-informasi/.

[27] Sintong Arion Hutapea, 2021, *Right To Be Forgotten Sebagai Bentuk Rehabilitasi Bagi Korban Pelanggaran Data Pribadi*, Jurnal Jurisprudentia, Universitas Bung Hatta, Vol. 1 No. 1, hal. 6.

memberikan kedaulatan 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.

Kewajiban Pengendali Data Pribadi menjadi fokus utama dalam implementasi UU PDP untuk menjamin bahwa setiap proses dilakukan secara akuntabel. [28] 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.[29]

Prinsip-prinsip pelindungan data pribadi di Indonesia, yang mencakup pengumpulan secara terbatas dan spesifik, pemrosesan yang transparan, serta penjaminan akurasi dan keamanan data, secara eksplisit ditegaskan dalam Pasal 16 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sedangkan kewajiban hukum bagi pengendali data untuk menyampaikan pemberitahuan tertulis kepada subjek data dan lembaga pengawas dalam waktu paling lama 3 kali

[28] Hukumonline, "Bedah UU PDP: Perbedaan Pengendali vs Prosesor Data Pribadi," hukumonline.com, 2022, https://www.hukumonline.com/berita/a/bedah-uu-pdp--perbedaan-pengendali-vs-prosesor-data-pribadi-lt63460658550b0/

[29] PPredderics Hockop Simanjuntak, 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, Universitas Pembangunan Nasional Veteran Jakarta, Vol. 6 No. 2, hal. 106.

24 jam apabila terjadi kegagalan pelindungan data diatur secara tegas dalam Pasal 46 ayat (1) UU PDP.

Lebih lanjut, pengaturan di Indonesia juga mewajibkan penunjukan Pejabat Pelindungan Data atau *Data Protection Officer* (DPO) bagi pengendali data yang melakukan pemrosesan untuk kepentingan pelayanan publik, kegiatan utama yang memerlukan pemantauan sistematis berskala besar, atau pemrosesan data pribadi spesifik berskala besar. Peran DPO di Indonesia sangat strategis sebagai jembatan antara organisasi, subjek data, dan lembaga pengawas guna memastikan kepatuhan internal terhadap regulasi yang berlaku. Keberadaan DPO diharapkan dapat mengubah budaya organisasi di Indonesia, baik di sektor pemerintahan maupun bisnis, agar lebih peduli terhadap privasi sebagai sebuah standar operasional, bukan sekadar pelengkap administratif. 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).[30]

Aspek penegakan hukum dalam UU PDP Indonesia mencakup sanksi administratif dan sanksi pidana yang cukup progresif guna memberikan efek jera terhadap para pelanggar, di mana ketentuan mengenai ragam sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan atau

[30] Ajisatria Suleiman, Pingkan Audrin, dan Thomas Dewaranu, 2020, *Pengaturan Bersama Dalam Perlindungan Data Pribadi: Potensi Peran Asosiasi Industri Sebagai Organisasi Regulator Mandiri*, Makalah Kebijakan Center for Indonesian Policy Studies (CIPS), No. 50.

pemusnahan data pribadi, hingga denda administratif diatur dalam Pasal 57 ayat (1) dan ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Lebih spesifik, denda administratif yang nilainya dapat mencapai paling tinggi 2 persen dari pendapatan tahunan atau penerimaan 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.[31]

Sementara itu, ketentuan pidana diatur secara tegas dalam Bab XIV, khususnya pada Pasal 67 ayat (1), ayat (2), dan ayat (3) serta Pasal 68 UU PDP, yang memberikan ancaman penjara dan denda miliaran rupiah bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri atau orang lain yang mengakibatkan kerugian bagi subjek data.

Indonesia juga mengatur mengenai mekanisme transfer data pribadi ke luar wilayah hukum Indonesia yang mensyaratkan adanya tingkat perlindungan data yang setara di negara penerima sebagaimana diatur dalam Pasal 56 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Jika tingkat perlindungan tersebut tidak setara, pengendali data wajib memastikan adanya kontrak standar

[31] Csirt.teknokrat.ac.id, "GDPR vs UU PDP: Perbandingan Regulasi Perlindungan Data," csirt.teknokrat.ac.id, 2025, https://csirt.teknokrat.ac.id/gdpr-vs-uu-pdp-perbandingan-regulasi-perlindungan-data/

perlindungan data yang mengikat berdasarkan Pasal 56 ayat (3), atau mendapatkan persetujuan dari subjek data sesuai dengan Pasal 56 ayat (4) UU PDP.[32] Langkah ini diambil untuk melindungi data warga negara Indonesia agar tetap aman meskipun berada di server atau yurisdiksi asing, yang sangat relevan dengan latar belakang banyaknya perusahaan multinasional yang beroperasi di Indonesia. Pengaturan ini memastikan bahwa kedaulatan data nasional tetap terjaga di tengah arus lalu lintas data global yang semakin cair, sekaligus mendorong adanya kerja sama internasional dalam penegakan standar privasi.

Lembaga penyelenggara pelindungan data pribadi di Indonesia memegang peranan kunci dalam mengawasi pelaksanaan UU PDP, meskipun detail strukturnya ditentukan oleh Presiden. Lembaga ini memiliki wewenang untuk merumuskan kebijakan, mengawasi kepatuhan pengendali data, menerima pengaduan, hingga menjatuhkan sanksi administratif. Kehadiran lembaga ini menjadi jawaban atas kebutuhan akan otoritas pengawas yang mampu bertindak secara cepat dan tegas terhadap pelanggaran privasi di sektor publik maupun swasta.[33] Dengan adanya otoritas tunggal ini, diharapkan tidak lagi terjadi tumpang tindih kewenangan antar kementerian dalam menangani masalah kebocoran data, sehingga perlindungan hukum bagi masyarakat Indonesia menjadi lebih

[32] Hukumonline, "Aturan Dan Risiko Transfer Data Pribadi Antarnegara," hukumonline.com, 2025, https://www.hukumonline.com/klinik/a/aturan-dan-risiko-transfer-data-pribadi-antarnegara-lt690aac9c5fd49/.

[33] Erlyns Yolanda dan Rugun Romaida Hutabarat, 2023, *Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif*, Syntax Literate: Jurnal Ilmiah Indonesia, Vol. 8 No. 6, hal. 4167–82..

terintegrasi dan responsif terhadap dinamika teknologi yang terus berkembang.

Secara prosedural, UU PDP Indonesia juga mengakui penyelesaian sengketa melalui lembaga arbitrase atau pengadilan jika mediasi tidak membuahkan hasil sebagaimana diatur dalam Pasal 64 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan jalan bagi subjek data untuk menuntut ganti rugi atas pelanggaran data pribadi miliknya sesuai dengan hak yang dijamin dalam Pasal 12 UU PDP.

Hak atas ganti rugi ini merupakan manifestasi dari tanggung jawab perdata pengendali data terhadap kerugian materiil maupun immateriil yang dialami oleh warga negara. Hal ini sangat krusial karena selama ini subjek data di Indonesia seringkali berada pada posisi tawar yang lemah di hadapan korporasi besar. Dengan adanya landasan hukum ganti rugi yang jelas, masyarakat memiliki insentif hukum untuk lebih aktif dalam memperjuangkan hak privasi mereka yang tercederai.

Keberadaan sanksi pidana khusus bagi tindak pidana yang dilakukan oleh korporasi di Indonesia menambah lapisan perlindungan yang kuat sebagaimana diatur dalam Pasal 70 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), di mana pidana denda dapat dijatuhkan kepada korporasi itu sendiri serta pengurus yang bertanggung jawab berdasarkan Pasal 70 ayat (1) UU PDP.

Selain denda pokok, pidana tambahan berupa perampasan keuntungan haram, penutupan seluruh atau sebagian tempat usaha, hingga pembubaran korporasi secara eksplisit diatur dalam Pasal 70 ayat (3) UU PDP dan dapat dikenakan dalam kasus pelanggaran berat. Hal ini sangat relevan mengingat banyak insiden kebocoran data di Indonesia melibatkan entitas bisnis berskala besar yang memiliki kontrol luas atas data jutaan orang. Dengan ancaman hukuman terhadap korporasi tersebut, diharapkan entitas bisnis akan mengalokasikan investasi yang lebih besar pada sistem keamanan data dan kepatuhan hukum demi menghindari risiko reputasi serta finansial yang fatal.

Penyusunan UU PDP ini pada dasarnya juga merupakan respon terhadap tekanan internasional dan kebutuhan harmonisasi hukum agar Indonesia dapat bersaing dalam pasar ekonomi digital global. Dengan memiliki standar perlindungan data yang setara dengan standar global, Indonesia dapat memfasilitasi aliran data lintas batas yang aman, yang pada gilirannya akan menarik investasi teknologi dan meningkatkan daya saing *startup* lokal di kancah internasional. Latar belakang ekonomi inilah yang memperkuat posisi UU PDP sebagai instrumen hukum yang tidak hanya bersifat protektif bagi warga negara, tetapi juga strategis bagi pertumbuhan ekonomi nasional yang berbasis pada inovasi dan teknologi informasi.

Sebagai penutup dalam konteks pengaturan di Indonesia, UU No. 27 Tahun 2022 menjadi tonggak sejarah yang mengakhiri era ketidakpastian

hukum dalam perlindungan data pribadi. [34] Melalui integrasi hak konstitusional, kewajiban pengendali data yang ketat, dan mekanisme penegakan hukum yang komprehensif, Indonesia telah meletakkan fondasi yang kokoh untuk melindungi privasi warganya di abad digital. Pengaturan ini menyeimbangkan antara hak individu untuk dilindungi dan kepentingan nasional untuk mengembangkan ekosistem digital yang sehat, aman, dan berintegritas. Implementasi yang konsisten dari seluruh pasal dalam UU PDP akan menentukan sejauh mana Indonesia dapat bertransformasi menjadi bangsa yang berdaulat secara data dan dihormati dalam tata kelola data di tingkat global.

2. Pengaturan Perlindungan Data Pribadi Di Malaysia dalam *Personal Data Protection* ACT 2010

Penyebaran informasi yang terus-menerus ini berbahaya jika dilakukan secara ilegal dan tidak adil jika pengolahan data pribadi dilakukan secara sewenang-wenang dan melanggar hukum yang berlaku. Hal yang perlu diperhatikan adalah bahwa saat menggunakan perangkat internet, semua tindakan yang dilakukan atau tujuan yang dikunjungi akan direkam dan menjadi jejak digital yang dapat digunakan untuk kegiatan ilegal. Oleh karena itu, perdebatan mengenai penyalahgunaan perlindungan data pribadi terhadap pihak ketiga bersifat sensitif dan sulit. Masalah ini pada akhirnya mendorong beberapa negara dan lembaga

[34] Yulianto Wibowo, Ida Aryati DPW, dan Ismiyanto, *Loc.,Cit.*

internasional untuk mengembangkan dan menyelesaikan masalah ini dengan menetapkan kerangka hukum mengenai pengolahan data pribadi,[35] termasuk di negara Malaysia.

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*).[36]

Inti dari pengaturan di Malaysia terletak pada tujuh Prinsip Perlindungan Data Pribadi yang wajib dipatuhi, yakni:[37]

a. Prinsip Am.
b. Prinsip Notis dan Pilihan.
c. Prinsip Penzahiran.
d. Prinsip Keselamatan.
e. Prinsip Penyimpanan.
f. Prinsip Integriti Data.
g. Prinsip Akses.

Prinsip pertama adalah Prinsip Am atau Prinsip Umum, memuat uraian:

> "(1) Seseorang pengguna data tidak boleh: a) dalam hal data peribadi selain data peribadi sensitif, memproses data peribadi mengenai seorang subjek data melainkan jika subjek data itu telah memberikan

[35] Della Gatiko Negoro dan Gunawan Hadi Purwanto, 2024, *Customer Data Protection by Bank Rakyat Indonesia is Reviewed by Law Number 27 of 2022 Concerning Personal Data*, Legal Brief, Vol. 13 No. 2, hal. 251.

[36] Penjelasan dalam Seksyen 5 Bahagian II, Undang-Undang Malaysia, Akta 709, Akta Perlindungan Data Pribadi 2010.

[37] Seksyen 5. Prinsip Perlindungan Data Peribadi, Undang-Undang Malaysia, Akta 709, Akta Perlindungan Data Pribadi 2010.

persetujuannya bagi pemprosesan data peribadi itu; atau (b) dalam hal data peribadi sensitif, memproses data peribadi sensitif mengenai seorang subjek data kecuali mengikut peruntukan seksyen 40. (2) Walau apa pun perenggan (1)(a), seseorang pengguna data boleh memproses data peribadi mengenai seorang subjek data jika pemprosesan itu perlu: (a) bagi melaksanakan sesuatu kontrak yang subjek data itu ialah suatu pihak kepadanya; (b) bagi mengambil langkah atas permintaan subjek data itu dengan tujuan untuk membuat sesuatu kontrak; (c) bagi mematuhi apa-apa obligasi undang-undang yang pengguna data itu merupakan subjek baginya, selain suatu obligasi yang dikenakan oleh sesuatu kontrak; (d) bagi melindungi kepentingan vital subjek data itu; (e) bagi mentadbirkan keadilan; atau (f) bagi menjalankan apa-apa fungsi yang diberikan kepada mana-mana orang oleh atau di bawah mana-mana undang-undang. (3) Data peribadi tidak boleh diproses melainkan jika: (a) data peribadi itu diproses bagi maksud yang sah yang berhubungan secara langsung dengan aktiviti pengguna data itu; (b) pemprosesan data peribadi itu perlu bagi atau berhubungan secara langsung dengan maksud itu; dan (c) data peribadi itu adalah mencukupi tetapi tidak berlebihan berhubung dengan maksud itu."

Dalam prinsip Am di atas, persetujuan dari subjek data menjadi fondasi utama sebelum pemrosesan dilakukan, kecuali untuk kondisi-kondisi tertentu yang dikecualikan oleh undang-undang. Hal ini ditegaskan dalam Seksyen 6 (1) yang berbunyi: "

(1) Seseorang pengguna data tidak boleh: (a) dalam hal data peribadi selain data peribadi sensitif, memproses data peribadi mengenai seorang subjek data melainkan jika subjek data itu telah memberikan persetujuannya bagi pemprosesan data peribadi itu; atau (b) dalam hal data peribadi sensitif, memproses data peribadi sensitif mengenai seorang subjek data kecuali mengikut peruntukan seksyen 40."

Pengaturan tersebut di atas memastikan bahwa kedaulatan individu atas informasinya dihormati sejak tahap awal pengumpulan data. Malaysia juga memberikan perhatian khusus pada transparansi melalui Prinsip Notis dan Pilihan (*Notice and Choice Principle*). Berdasarkan Seksyen 7 (1) yang berbunyi:

"(1) Seseorang pengguna data hendaklah melalui notis bertulis memaklumkan seorang subjek data: (a) bahawa data peribadi subjek data itu sedang diproses oleh atau bagi pihak pengguna data itu, dan hendaklah memberikan perihalan data peribadi itu kepada subjek data itu; (b) maksud yang baginya data peribadi itu sedang atau akan dikumpulkan dan diproses selanjutnya; (c) apa-apa maklumat yang ada pada pengguna data itu tentang sumber data peribadi itu; (d) hak subjek data itu untuk meminta akses kepada dan untuk meminta pembetulan terhadap data peribadi itu dan bagaimana untuk menghubungi pengguna data itu tentang apa-apa pertanyaan atau aduan berkenaan dengan data peribadi itu; (e) golongan pihak ketiga yang kepadanya pengguna data menzahirkan atau boleh menzahirkan data peribadi itu; (f) pilihan dan cara yang ditawarkan oleh pengguna data itu kepada subjek data bagi mengehadkan pemprosesan data peribadi, termasuklah data peribadi yang berhubungan dengan orang lain yang boleh dikenal pasti daripada data peribadi itu; (g) sama ada wajib atau sukarela bagi subjek data untuk memberikan data peribadi itu; dan (h) jika wajib bagi subjek data itu untuk memberikan data peribadi itu, akibat kepadanya jika dia tidak memberikan data peribadi itu."

Seksyen 7 (1) di atas pada pokoknya, pengguna data wajib memberikan pemberitahuan tertulis yang jelas kepada subjek data mengenai jenis data yang dikumpulkan, tujuan pemrosesan, serta hak subjek data untuk mengakses dan meminta koreksi. Serta dalam ketentuan dalam Seksen 7 (2) dan (3) *Personal Data Protection Act 2010,* yang berbunyi:

"(2) Notis di bawah subseksyen (1) hendaklah diberikan dengan secepat yang dapat dilaksanakan oleh pengguna data itu: (a) apabila subjek data itu pertama kalinya diminta oleh pengguna data itu untuk memberikan data peribadinya; (b) apabila pengguna data itu pertama kalinya mengumpul data peribadi subjek data itu; atau (c) dalam mana-mana hal lain, sebelum pengguna data itu (i) menggunakan data peribadi subjek data itu bagi maksud selain maksud yang baginya data peribadi itu dikumpulkan; atau (ii) menzahirkan data peribadi itu kepada pihak ketiga. (3) Suatu notis di bawah subseksyen (1) hendaklah dalam bahasa kebangsaan dan bahasa Inggeris, dan individu itu hendaklah diberi cara yang jelas dan mudah diakses untuk membuat pilihannya, jika perlu, dalam bahasa kebangsaan dan bahasa Inggeris."

Pemberitahuan ini harus disampaikan dalam bahasa nasional (Bahasa Malaysia) dan bahasa Inggris untuk memastikan pemahaman yang luas.[38] Dengan adanya kewajiban ini, individu di Malaysia tidak lagi berada dalam ketidaktahuan saat data mereka dikelola oleh korporasi, sehingga tercipta ekosistem digital yang berbasis pada keterbukaan dan akuntabilitas informasi.

Aspek kelembagaan dalam Akta 709 menonjolkan peran sentral seorang Komisioner Perlindungan Data Pribadi yang disebut dengan Pesuruh Jaya, yang diangkat langsung oleh Menteri. Komisioner ini bukan sekadar jabatan administratif, melainkan sebuah badan hukum tunggal (*corporation sole*) dengan kekuasaan yang sangat luas untuk mengatur dan mengawasi implementasi undang-undang. Hal ini sebagaimana diatur dalam Seksyen 47 tentang Pelantikan Pesuruhjaya:

> "(1) Menteri hendaklah melantik mana-mana orang sebagai "Pesuruhjaya Perlindungan Data Peribadi" bagi maksud menjalankan fungsi dan kuasa yang diberikan kepada Pesuruhjaya di bawah Akta ini atas apa-apa terma dan syarat yang difikirkannya wajar. (2) Pelantikan Pesuruhjaya hendaklah disiarkan dalam Warta. (3) Pesuruhjaya yang dilantik di bawah subseksyen (1) ialah suatu pertubuhan perbadanan yang kekal turun-temurun dan mempunyai suatu meterai perbadanan. (4) Pesuruhjaya boleh membawa guaman dan dibawa guaman terhadapnya atas nama perbadanannya"

Pesuruhjaya ini memiliki wewenang mulai dari mendaftarkan pengguna data, mengeluarkan kode praktik, hingga melakukan investigasi

[38] Ketentuan dalam Seksyen 7 (1) dan (2) Undang-Undang Malaysia, Akta 709, Akta Perlindungan Data Pribadi 2010.

mendalam terhadap dugaan pelanggaran yang dilakukan oleh entitas komersial di Malaysia.[39]

Salah satu pengaturan di Malaysia adalah adanya sistem pendaftaran wajib bagi kelas pengguna data tertentu. Uraiannya termuat dalam Seksyen 14, 15 dan 16 yang berbunyi: "

Seksyen 14. Pendaftaran pengguna data:

"(1) Menteri boleh, atas syor Pesuruhjaya, melalui perintah yang disiarkan dalam Warta, menyatakan golongan pengguna data yang dikehendaki untuk didaftarkan sebagai pengguna data di bawah Akta ini. (2) Pesuruhjaya hendaklah, sebelum membuat syornya di bawah subseksyen (1), berunding dengan: (a) mana-mana badan yang mewakili pengguna data yang berada dalam golongan itu; atau (b) mana-mana orang berkepentingan yang lain"

Seksyen 15:

"Permohonan untuk pendaftaran (1) Seseorang yang berada dalam golongan pengguna data yang dinyatakan dalam perintah yang dibuat di bawah subseksyen 14 (1) hendaklah mengemukakan suatu permohonan untuk pendaftaran kepada Pesuruhjaya mengikut cara dan dalam bentuk yang ditentukan oleh Pesuruhjaya. (2) Tiap-tiap permohonan untuk pendaftaran hendaklah disertai dengan fi pendaftaran yang ditetapkan dan apa-apa dokumen sebagaimana yang dikehendaki oleh Pesuruhjaya. (3) Pesuruhjaya boleh secara bertulis pada bila-bila masa selepas menerima permohonan dan sebelum permohonan itu diputuskan, menghendaki pemohon untuk memberikan apa-apa dokumen atau maklumat tambahan dalam tempoh masa yang dinyatakan oleh Pesuruhjaya. (4) Jika kehendak di bawah subseksyen (3) tidak dipatuhi, permohonan untuk pendaftaran hendaklah disifatkan telah ditarik balik oleh pemohon dan tidak boleh diteruskan oleh Pesuruhjaya, tetapi tanpa menjejaskan suatu permohonan baru dibuat oleh pemohon."

Seksyen 16:

"Perakuan pendaftaran (1) Selepas pertimbangan yang sewajarnya diberikan kepada suatu permohonan di bawah subseksyen 15(1), Pesuruhjaya boleh (a) mendaftarkan pemohon dan mengeluarkan suatu perakuan pendaftaran kepada pemohon itu dalam apa-apa bentuk yang

[39] Ketentuan dalam Pasal 48 *Personal Data Protection Act 2010* Malaysia

ditentukan oleh Pesuruhjaya; atau (b) menolak permohonan itu. (2) Perakuan pendaftaran boleh dikeluarkan tertakluk kepada apa-apa syarat atau sekatan yang difikirkan wajar untuk dikenakan oleh Pesuruhjaya. (3) Jika Pendaftar menolak permohonan untuk pendaftaran menurut subseksyen (1), dia hendaklah memaklumkan pemohon melalui suatu notis bertulis bahawa permohonan itu ditolak dan sebab-sebab baginya. (4) Seseorang yang berada dalam golongan pengguna data yang dinyatakan dalam perintah yang dibuat di bawah subseksyen 14(1) dan yang memproses data peribadi tanpa suatu perakuan pendaftaran yang dikeluarkan menurut perenggan 16(1)(a) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi lima ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi tiga tahun atau kedua-duanya

Penerapan sistem pendaftaran wajib bagi kelas pengguna data tertentu sebagaimana diatur dalam Seksyen 14 hingga 16 menunjukkan pendekatan proaktif Malaysia dalam memitigasi risiko penyalahgunaan data pada sektor-sektor berisiko tinggi. Dengan mewajibkan entitas strategis seperti perbankan, telekomunikasi, dan kesehatan untuk terdaftar, pemerintah menjalankan fungsi pengawasan preventif yang memastikan bahwa organisasi-organisasi tersebut tidak hanya tunduk pada aturan secara pasif, tetapi juga berada dalam pantauan langsung Pesuruhjaya sejak awal operasionalnya. Kewajiban ini, yang diperkuat dengan ancaman sanksi pidana berat pada Seksyen 16, menciptakan standar kepatuhan yang lebih ketat sekaligus memberikan jaminan keamanan bagi subjek data bahwa entitas yang mengelola informasi sensitif mereka telah divalidasi dan diawasi oleh otoritas negara.

Hak subjek data dalam pengaturan Malaysia dijamin secara eksplisit, terutama mengenai hak untuk mengakses dan memperbaiki data yang tidak akurat. Seksyen 30 (1) memberikan wewenang bagi individu untuk

mengajukan permintaan akses data, yang berbunyi "(1) *Seseorang individu berhak untuk diberitahu oleh seorang pengguna data sama ada data peribadi yang mengenainya individu itu ialah subjek data sedang diproses oleh atau bagi pihak pengguna data itu.*" Hak ini memastikan bahwa data yang beredar di pasar komersial tetap terjaga akurasinya dan mencerminkan kondisi sebenarnya dari sang pemilik data.

Selain hak akses, Malaysia juga mengatur hak individu untuk mencegah pemrosesan data yang dapat menimbulkan kerusakan atau kesusahan yang tidak beralasan melalui Seksyen 35:

"(1) Tertakluk kepada subseksyen (2), (3) dan (5) dan seksyen 36, jika seseorang pengguna data berpuas hati bahawa data peribadi yang dengannya suatu permintaan pembetulan data adalah berhubungan adalah tidak tepat, tidak lengkap, mengelirukan atau tidak terkini, dia hendaklah, tidak lewat daripada dua puluh satu hari dari tarikh penerimaan permintaan pembetulan data itu: (a) membuat pembetulan yang perlu kepada data peribadi itu; (b) memberi peminta suatu salinan data peribadi yang telah dibetulkan; dan (c) tertakluk kepada subseksyen (4), jika: (i) data peribadi itu telah dizahirkan kepada suatu pihak ketiga dalam masa dua belas bulan sebaik sebelum hari yang pembetulan itu dibuat; dan (ii) pengguna data itu tidak mempunyai apa-apa sebab untuk mempercayai bahawa pihak ketiga itu telah berhenti menggunakan data peribadi bagi maksud, termasuklah apa-apa maksud yang berkaitan secara langsung, yang baginya data peribadi itu telah dizahirkan kepada pihak ketiga itu, mengambil segala langkah praktikal untuk memberi pihak ketiga suatu salinan data peribadi yang telah dibetulkan sedemikian berserta dengan suatu notis bertulis yang menyatakan sebab-sebab bagi pembetulan itu. (2) Seseorang pengguna data yang tidak dapat mematuhi permintaan pembetulan data dalam tempoh yang dinyatakan dalam subseksyen (1) hendaklah sebelum habis tempoh itu: (a) melalui notis bertulis memaklumkan peminta bahawa dia tidak dapat mematuhi permintaan pembetulan data dalam tempoh itu dan sebab-sebab kenapa dia tidak dapat berbuat demikian; dan (b) mematuhi permintaan pembetulan data itu ke apa-apa takat yang dapat dibuat olehnya. (3) Walau apa pun subseksyen (2), pengguna data hendaklah mematuhi keseluruhan permintaan pembetulan data itu tidak lewat daripada empat belas hari selepas habis tempoh yang dinyatakan dalam subseksyen (1). (4) Seseorang pengguna data tidak dikehendaki untuk mematuhi perenggan (1)(c) dalam apaapa hal jika penzahiran data peribadi

kepada pihak ketiga terdiri daripada pemeriksaan sendiri daftar oleh pihak ketiga itu: (a) yang dalamnya data peribadi itu dimasukkan atau selainnya direkodkan; dan (b) yang tersedia untuk pemeriksaan oleh orang awam. (5) Jika seseorang pengguna data diminta untuk membetulkan data peribadi di bawah subseksyen 34(1) dan data peribadi itu sedang diproses oleh pengguna data lain yang berada dalam kedudukan yang lebih baik untuk memberikan maklum balas kepada permintaan pembetulan data itu— (a) pengguna data yang mula-mula disebut itu hendaklah dengan serta-merta memindahkan permintaan pembetulan data itu kepada pengguna data itu, dan memberitahu peminta itu mengenai fakta ini; dan (b) seksyen 34, 35, 36 dan 37 hendaklah terpakai seolah-olah sebutan dalamnya kepada seorang pengguna data ialah sebutan kepada pengguna data lain itu."

Seksyen 35 di atas memuat ketentuan bahwa secara khusus memberikan hak kepada individu untuk mencegah pemrosesan data yang berpotensi menimbulkan kerusakan atau kesusahan yang tidak beralasan (*unwarranted distress*),

Lebih lanjut, individu memiliki kontrol atas pemasaran langsung yang sering kali mengganggu privasi. Seksyen 43 (1) menyatakan:

"(1) Seseorang subjek data boleh, pada bila-bila masa melalui notis bertulis kepada pengguna data, menghendaki pengguna data itu pada penghujung apa-apa tempoh yang munasabah dalam hal keadaan itu untuk memberhentikan atau tidak memulakan pemprosesan data peribadinya bagi maksud pemasaran langsung."

Ketentuan ini memberikan perlindungan nyata bagi warga Malaysia dari gangguan iklan yang tidak diinginkan. Dalam ketentuan Seksyen 43 (1) di atas juga memberikan kedaulatan penuh kepada individu untuk menarik diri dari praktik pemasaran langsung yang sering kali invasif dan mengganggu ruang privat. Dengan hak untuk menghentikan pemrosesan data kapan saja melalui notis bertulis, undang-undang ini memaksa pelaku usaha untuk beralih dari model pemasaran agresif menuju pendekatan berbasis izin. Pengaturan ini sangat krusial di era digital, karena tidak

hanya melindungi subjek data dari gangguan komunikasi yang tidak diinginkan, tetapi juga memastikan bahwa data pribadi tidak dieksploitasi untuk kepentingan komersial tanpa kendali pemiliknya, sehingga tercipta keseimbangan yang adil antara kepentingan bisnis dan hak privasi individu.

Dalam hal penegakan hukum, Komisioner di Malaysia dilandasi dengan kekuatan investigasi yang setara dengan aparat kepolisian. Saksyen 112 (2) menegaskan:

> "(2) Bagi mengelakkan keraguan, diisytiharkan bahawa bagi maksud Akta ini, pegawai diberi kuasa hendaklah mempunyai segala atau mana-mana kuasa khas seorang pegawai polis daripada apa-apa jua pangkat berhubungan dengan penyiasatan polis dalam kes boleh tangkap seperti yang diperuntukkan di bawah Kanun Tatacara Jenayah [Akta 593], dan kuasa itu adalah sebagai tambahan kepada kuasa yang diperuntukkan di bawah Akta ini dan bukan pengurangan baginya."

Wewenang tersebut mencakup penggeledahan, penyitaan alat elektronik, hingga akses terhadap data terkomputerisasi termasuk kunci enkripsi dan kata sandi sebagaimana diatur dalam Seksyen 115 yang berbunyi:

> "(1) Seorang pegawai diberi kuasa yang menjalankan suatu penggeledahan di bawah seksyen 113 dan 114 hendaklah diberi capaian kepada data berkomputer sama ada disimpan dalam suatu komputer atau selainnya. (2) Bagi maksud seksyen ini, "capaian": (a) termasuklah diberi kata laluan, kod penyulitan, kod penyahsulitan, perisian atau perkakasan yang perlu dan apa-apa cara lain yang dikehendaki untuk membolehkan data berkomputer itu difahami; dan (b) mempunyai erti yang diberikan kepadanya oleh subseksyen 2(2) dan (5) Akta Jenayah Komputer 1997 [Akta 563]."

Ketentuan di atas menunjukkan bahwa Malaysia tidak berkompromi terhadap pelanggaran data yang bersifat kriminal.

Mekanisme keberatan hukum di Malaysia diatur melalui pembentukan Tribunal Rayuan yang memberikan jalur formal bagi pihak yang merasa dirugikan oleh keputusan Komisioner. Berdasarkan Seksyen 83: "*Suatu Tribunal Rayuan ditubuhkan bagi maksud mengkaji semula mana-mana perkara dalam rayuan yang dinyatakan dalam seksyen 93*." (Telah dibentuk sebuah Tribunal Banding untuk tujuan meninjau kembali hal-hal yang diajukan dalam banding sebagaimana ditetapkan dalam pasal 93).

Mengenai transfer data ke luar wilayah Malaysia, Akta 709 menerapkan aturan yang ketat untuk mencegah kebocoran data di yurisdiksi asing. Pasal 129 (1) mengatur:

> "(1) Seseorang pengguna data tidak boleh memindahkan mana-mana data peribadi mengenai seorang subjek data ke suatu tempat di luar Malaysia melainkan jika ke mana-mana tempat yang ditentukan oleh Menteri, atas syor Pesuruhjaya, melalui pemberitahuan yang disiarkan dalam Warta"

Menteri akan menetapkan daftar negara (*whitelist*) yang dianggap memiliki tingkat perlindungan yang setara. Namun, Seksyen 129 (3) memberikan pengecualian jika subjek data telah memberikan persetujuan atau jika transfer tersebut diperlukan untuk pelaksanaan kontrak, yang memberikan fleksibilitas namun tetap dalam koridor perlindungan. [40] Adapun bunyi Seksyen 129 (3):

> (3) Walau apa pun subseksyen (1), seseorang pengguna data boleh memindahkan mana-mana data peribadi ke suatu tempat di luar Malaysia jika: (a) subjek data telah memberikan persetujuannya terhadap

[40] Muhammad Adnan Pitchan dan Siti Zobidah Omar, 2019, *Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang*, Jurnal Komunikasi: Malaysian Journal of Communication, Universiti Kebangsaan Malaysia, Vol. 35 No. 1, hal. 116.

pemindahan itu; (b) pemindahan itu perlu bagi pelaksanaan suatu kontrak antara subjek data dengan pengguna data itu; (c) pemindahan itu perlu bagi penyempurnaan atau pelaksanaan suatu kontrak antara pengguna data itu dengan suatu pihak ketiga yang: (i) dibuat atas permintaan subjek data itu; atau (ii) adalah untuk kepentingan subjek data; (d) pemindahan itu adalah bagi maksud mana-mana prosiding undang-undang atau bagi maksud untuk mendapatkan nasihat undang-undang atau untuk mewujudkan, menjalankan atau mempertahankan hak di sisi undang-undang; (e) pengguna data itu mempunyai alasan yang munasabah untuk mempercayai bahawa dalam segala hal keadaan mengenai hal itu: (i) pemindahan itu adalah bagi mengelakkan atau mengurangkan tindakan yang memudaratkan terhadap subjek data; (ii) adalah tidak praktikal untuk mendapatkan persetujuan subjek data secara bertulis mengenai pemindahan itu; dan (iii) jika adalah praktikal untuk mendapatkan persetujuan itu, subjek data itu akan memberikan persetujuannya; (f) pengguna data itu telah mengambil segala langkah berjagajaga yang munasabah dan telah menjalankan segala usaha yang wajar untuk memastikan bahawa data peribadi itu tidak akan diproses di tempat itu mengikut apa-apa cara yang, sekiranya tempat itu ialah Malaysia, akan menjadi suatu pelanggaran Akta ini; (g) pemindahan itu perlu untuk melindungi kepentingan vital subjek data; atau (h) pemindahan itu perlu oleh sebab ia berkepentingan awam dalam hal keadaan yang ditentukan oleh Menteri."

Pelanggaran terhadap ketentuan perlindungan data di Malaysia membawa konsekuensi pidana yang berat, terutama bagi pengurus korporasi. Seksyen 133 (1) menegaskan tanggung jawab kolektif pengurus:

"Jika sesuatu pertubuhan perbadanan melakukan suatu kesalahan di bawah Akta ini, manamana orang yang pada masa pelakuan kesalahan itu ialah seorang pengarah, ketua pegawai eksekutif, ketua pegawai operasi, pengurus, setiausaha atau pegawai lain yang seumpamanya dalam pertubuhan perbadanan itu atau yang berupa bertindak atas mana-mana sifat sedemikian atau yang mengikut apa-apa cara atau sehingga apa-apa takat bertanggungjawab bagi pengurusan apa-apa hal-ehwal pertubuhan perbadanan itu atau yang membantu dalam pengurusan sedemikian: (a) boleh dipertuduh secara berasingan atau bersesama dalam prosiding yang sama bersekali dengan pertubuhan perbadanan itu; dan (b) jika pertubuhan perbadanan itu didapati telah melakukan kesalahan itu, hendaklah disifatkan telah melakukan kesalahan itu melainkan jika, dengan mengambil kira jenis fungsinya atas sifat itu dan segala hal keadaan, dia membuktikan: (i) bahawa kesalahan itu telah dilakukan tanpa pengetahuannya, persetujuannya atau pembiarannya; dan (ii) bahawa dia telah mengambil segala langkah berjagajaga yang munasabah dan telah

menjalankan segala usaha yang wajar untuk mengelakkan pelakuan kesalahan itu."

Hal ini memaksa para pemimpin perusahaan di Malaysia untuk memprioritaskan kepatuhan data pribadi sebagai agenda utama dalam tata kelola perusahaan guna menghindari risiko pemidanaan pribadi.

Selain sanksi pidana, Malaysia juga mengenal mekanisme kompensasi atau damai administratif untuk penyelesaian pelanggaran tertentu. Seksyen 132 (1) menyatakan:

"(1) Pesuruhjaya boleh, dengan keizinan secara bertulis Pendakwa Raya, mengkompaun apaapa kesalahan yang dilakukan oleh mana-mana orang di bawah Akta ini dan yang ditetapkan menjadi suatu kesalahan boleh kompaun dengan membuat suatu tawaran bertulis kepada orang yang disyaki telah melakukan kesalahan itu untuk mengkompaun kesalahan itu apabila dibayar kepada Pesuruhjaya suatu amaun wang yang tidak melebihi lima puluh peratus daripada amaun denda maksimum bagi kesalahan itu dalam masa yang dinyatakan dalam tawaran bertulisnya."

Mekanisme ini memberikan efisiensi dalam penegakan hukum bagi pelanggaran yang bersifat teknis-administratif, di mana pelanggar dapat membayar denda tanpa harus melalui proses pengadilan yang panjang, namun tetap memberikan efek jera secara finansial.

Pengaturan Malaysia juga sangat progresif dalam melindungi mereka yang membantu mengungkap kejahatan data pribadi melalui Pasal 140 mengenai perlindungan informan. Sekksyen 140 (1) berbunyi:

"(1) Kecuali sebagaimana yang diperuntukkan dalam subseksyen (2) dan (3), tiada saksi dalam mana-mana prosiding sivil atau jenayah menurut Akta ini boleh dikehendaki atau dibenarkan untuk menzahirkan nama atau alamat mana-mana pemberi maklumat atau isi dan jenis maklumat yang diterima daripadanya atau untuk menyatakan apa-apa perkara yang mungkin menyebabkan dia diketahui."

Perlindungan identitas ini sangat krusial dalam latar belakang masyarakat digital, di mana orang sering kali takut melaporkan pelanggaran data yang dilakukan oleh perusahaan besar karena kekhawatiran akan pembalasan.

Terakhir, pengaturan perlindungan data pribadi di Malaysia melalui Akta 709 mencerminkan sebuah sistem yang mapan dan memiliki struktur yang sangat detail, mulai dari prinsip dasar hingga mekanisme teknis penegakan hukum. Dengan menyeimbangkan hak subjek data dan kewajiban pengguna data melalui pengawasan Komisioner yang kuat dan didukung oleh Tribunal Rayuan, Malaysia telah menciptakan kerangka hukum yang kokoh. Pengaturan ini tidak hanya bertujuan untuk melindungi privasi individu, tetapi juga untuk memperkuat posisi Malaysia sebagai destinasi investasi digital yang aman dan terpercaya di kancah global melalui kepastian hukum yang ditawarkan oleh Akta 709.

B. Kelebihan Dan Kekurangan Pengaturan Perlindungan Hak Subjek Data Pribadi Di Indonesia Dan Malaysia

1. Perbandingan Pengaturan Terhadap Perlindungan Hak Subjek Data Pribadi Di Indonesia Dan Malaysia

Perbandingan pengaturan perlindungan hak subjek data pribadi antara Indonesia dan Malaysia menunjukkan adanya persamaan mendasar dalam beberapa prinsip-prinsip privasi, namun memiliki perbedaan khususnya dalam dalam struktur kelembagaan, mekanisme penegakan, dan teknis implementasi hak subjek data. Indonesia melalui UU No. 27

Tahun 2022 (UU PDP) dirumsukan sebagai regulasi modern yang sangat dipengaruhi oleh standar *General Data Protection Regulation* (GDPR) Uni Eropa dengan cakupan luas bagi sektor publik maupun privat.[41] Di sisi lain, Malaysia dengan *Personal Data Protection Act 2010* (Akta 709) menerapkan pendekatan yang lebih spesifik pada transaksi komersial dengan struktur otoritas yang telah mapan.

Perbandingan ini menjadi penting untuk dianalisis guna melihat bagaimana masing-masing negara memberikan kedaulatan kepada warga negaranya atas informasi pribadi mereka, baik melalui pengakuan hak-hak baru seperti portabilitas data di Indonesia maupun melalui struktur Tribunal Banding yang spesialis di Malaysia. Guna memudahkan, penulis merangkum beberapa pasal yang krusial untuk diperbandingkan antara regulasi di Indonesia yakni UU PD dan regulasi di Malaysia yakni *Personal Data Protection Act 2010*:

Tabel 3.1

Perbandingan UU No. 27 tahun 2022 dan *Personal Data Protection Act 2010*

Aspek Perbandingan	Regulasi Indonesia (UU No. 27 tahun 2022)	Regulasi Malaysia (PDPA 2010)	Sanksi Pelanggaran
Cakupan Sektor Pengawasan	Berlaku luas untuk sektor publik (instansi pemerintah) dan sektor privat	Hanya berlaku terbatas bagi transaksi komersial; sektor publik/pemerintah	Indonesia: Sanksi administratif (Pasal 57) dan Pidana

[41] Rizky Banyu, "Belajar Dari Gugatan Terhadap Facebook Di Eropa," law.ui.ac.id, 2025, https://law.ui.ac.id/belajar-dari-gugatan-terhadap-facebook-di-eropa-oleh-rizky-banyu-s-h-ll-m/.

	(swasta/komersial) (Pasal 2).	dikecualikan (Seksyen 3).	(Pasal 67-73). Malaysia: Sanksi administratif dan Pidana (Seksyen 5).
Status Kelembagaan	Lembaga Pemerintah yang ditetapkan oleh dan bertanggung jawab kepada Presiden (Pasal 58).	Komisioner Perlindungan Data Pribadi sebagai badan hukum tunggal (*corporation sole*) (Seksyen 47).	Indonesia: Sanksi administratif jika lembaga tidak menjalankan fungsinya (Pasal 57). Malaysia: Denda hingga RM 500.000 atau penjara hingga 3 tahun (Seksyen 47).
Hak Portabilitas Data	Hak subjek data untuk mendapatkan dan mengirimkan datanya dalam format yang umum digunakan (Pasal 13).	Tidak diatur secara eksplisit dalam ketentuan utama Akta 709.	
Mekanisme Keberatan Hukum	Melalui Lembaga Pengawas atau gugatan ganti rugi secara umum ke Pengadilan Negeri (Pasal 12).	Memiliki lembaga spesialis: Appeal Tribunal untuk meninjau keputusan otoritas (Seksyen 83).	Indonesia: Hak menggugat ganti rugi (Pasal 12). Malaysia: Keputusan Tribunal bersifat mengikat, pelanggaran terhadapnya dikenai sanksi

			pidana (Seksyen 99).
Sistem Transfer Luar Negeri	Berbasis kesetaraan tingkat perlindungan, kontrak standar, atau persetujuan subjek data (Pasal 56).	Menggunakan sistem *Whitelist*; transfer hanya boleh ke negara yang disetujui Menteri (Seksyen 129).	Indonesia: Sanksi administratif (Pasal 57). Malaysia: Denda hingga RM 300.000 atau penjara hingga 2 tahun (Seksyen 129).
Pendanaan Otoritas	Sumber pendanaan berasal dari Anggaran Pendapatan dan Belanja Negara (APBN).	Memiliki dana mandiri: Personal Data Protection Fund yang bersumber dari biaya pendaftaran (Seksyen 61).	Indonesia: Tidak ada sanksi langsung bagi subjek data. Malaysia: Pelanggaran pendaftaran berakibat denda hingga RM 500.000 (Seksyen 16).
Hak Atas Profilasi Otomatis	Hak untuk tidak tunduk pada keputusan yang hanya berdasarkan pemrosesan otomatis/profilasi (Pasal 10).	Tidak diatur secara mendalam mengenai perlindungan terhadap pengambilan keputusan otomatis.	Indonesia: Sanksi administratif (Pasal 57). Malaysia: Tidak ada sanksi (Karena hak tidak diatur).
Daluwarsa Pengaduan	Tidak diatur secara eksplisit mengenai batas waktu maksimal pengetahuan subjek data untuk melapor.	Dibatasi maksimal 2 tahun sejak subjek data mengetahui adanya pelanggaran/tindakan tersebut (Seksyen 106).	Indonesia: Tidak ada sanksi (Mekanisme belum diatur). Malaysia:

			Pengaduan ditolak jika melewati batas waktu (Seksyen 106).

Sumber: Data dianalisis dari uraian Jurnal "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia"[42] dan Jurnal "Penyuluhan Perlindungan Data Pribadi di Indonesia dan Malaysia di Shah Alam Malaysia"[43]

Berdasarkan tabel di atas, dapat dipahami bahwa ada 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 Seksyen 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

[42] Rohmah Dwi Cahyaningsih dkk., 2025, *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia Dan Malaysia*, Abdurrauf Sains Dan Masyarakat, Vol. 1 No. 4, hal. 800–811.

[43] Wahyudi dkk., 2025, *Penyuluhan Perlindungan Data Pribadi Di Indonesia Dan Malaysia Di Shah Alam Malaysia*, Jurnal Medika, Vol. 4 No. 4.

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.[44] Di sisi lain, Malaysia menonjolkan independensi administratif melalui pembentukan Komisioner sebagai badan hukum tunggal (*corporation sole*) menurut Seksyen 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.[45] Sebaliknya, Malaysia tidak mengatur hak portabilitas ini dalam

[44] Danil Erlangga Mahameru dkk., 2023, *Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia*, Jurnal Esensi Hukum, Universitas Pembangunan Nasional Veteran Jakarta, Vol. 5 No. 2, hal. 115–31..

[45] Slamet Mahfud Chushair, Abshoril Fithry, dan Rusfandi, 2025, *Perlindungan Hukum Bagi Korban Atas Kebocoran Pusat Data Nasional Sementara (PDNS) Perspektif Perlindungan Data Pribadi*, Jurnal Jendela Hukum, Vol. 12 No. 2, hal. 89–122.

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 Tribunal Rayuan berdasarkan Seksyen 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 Seksyen 129 PDPA 2010. Dalam sistem ini, transfer data hanya diperbolehkan ke negara-negara yang secara eksplisit disetujui oleh Menteri. [46] 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

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

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.[47] Ketentuan ini merespons kemajuan teknologi kecerdasan buatan (*AI*) dan algoritma yang dapat merugikan hak-hak individu secara tidak terlihat. Dalam Seksyen 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.

Terakhir, mengenai batas waktu pengaduan, Malaysia memberikan kepastian hukum melalui Seksyen 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

[47] Yuni Afifah, "Pakar Hukum Siber UNAIR Jelaskan Prinsip Perlindungan Data Pribadi," fh.unair.ac.id, 2023, https://fh.unair.ac.id/pakar-hukum-siber-unair-jelaskan-prinsip-perlindungan-data-pribadi/.

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.

2. Kelebihan dan Kekurangan Masing-Masing Regulasi Perlindungan Hak Pribadi Indonesia Dan Malaysia

Perbandingan antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) Indonesia dan *Personal Data Protection Act* 2010 (PDPA) Malaysia memberikan gambaran komprehensif mengenai bagaimana dua negara dengan latar belakang hukum yang berbeda merespons tantangan keamanan siber di kawasan ASEAN. Meskipun secara fundamental keduanya memiliki tujuan yang sama dalam menjaga kerahasiaan informasi warga negara, terdapat perbedaan tajam pada aspek jangkauan sektor pengawasan, struktur kemandirian lembaga, hingga kesiapan regulasi dalam menghadapi kemajuan teknologi mutakhir. Guna memberikan pemahaman yang sistematis mengenai kekuatan dan kelemahan dari masing-masing instrumen hukum tersebut, berikut disajikan tabel ringkasan komparatif untuk memudahkan penjabaran kelebihan dan kekurangan masing-masing regulasi perlindungan hak pribadi antara Indonesia dan Malaysia:

Tabel 3.2

Kelebihan dan Kekurangan UU No. 27 tahun 2022 dan *Personal Data Protection Act 2010*

Aspek Analisis	**Negara**	**Kelebihan**	**Kekurangan**
Cakupan yuridiksi	Indonesia	Sektor publik & privat terlindungi (Pasal 2).	-
	Malaysia	Fokus pada kepastian ekonomi digital.	Sektor publik dikecualikan (Pasal 3).
Kemandirian Lembaga	Indonesia	Memiliki landasan lembaga baru (Pasal 58).	Ketergantungan dana pada APBN.
	Malaysia	Mandiri secara dana (Seksyen 61 Fund).	-
Penyelesaian sengketa	Indonesia	Tersedia jalur mediasi dan gugatan perdata.	Belum ada lembaga banding khusus.
	Malaysia	Memiliki Appeal Tribunal spesialis (Seksyen 83).	-
Teknologi masa depan	Indonesia	Perlindungan terhadap profilasi/AI (Pasal 10).	-
	Malaysia	-	Belum mengatur keputusan otomatis.
Hak Portabilitas data	Indonesia	Mendukung kedaulatan data (Pasal 13).	-
	Malaysia	-	Tidak ada hak pindah data.

Instrumen Penegakan	Indonesia	Sanksi pidana sangat berat.	Bergantung pada koordinasi Polri.
	Malaysia	Wewenang setara Polisi (Pasal 115).	-
Kepastian proteksi	Indonesia	Perlindungan saksi secara umum.	Tiada batas daluwarsa aduan yang tegas.
	Malaysia	Proteksi saksi kuat (Pasal 140) & Daluwarsa aduan (Seksyen 106).	-

Sumber: Data dianalisis dari uraian Jurnal "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia"[48] dan Jurnal "Penyuluhan Perlindungan Data Pribadi di Indonesia dan Malaysia di Shah Alam Malaysia"[49]

Berdasarkan paparan tabel di atas, 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 Seksyen 3 justru mengecualikan kekuasaan pemerintah dari kewajiban perlindungan data. Dengan demikian, Indonesia memiliki standar keadilan y ang lebih merata bagi warga negara dalam menuntut

[48] Rohmah Dwi Cahyaningsih dkk., 2025, *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia Dan Malaysia*, Abdurrauf Sains Dan Masyarakat, Vol. 1 No. 4, hal. 800–811.

[49] Wahyudi dkk., 2025, *Penyuluhan Perlindungan Data Pribadi Di Indonesia Dan Malaysia Di Shah Alam Malaysia*, Jurnal Medika, Vol. 4 No. 4.

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 Seksyen 61. Malaysia memiliki kelebihan dalam keberlanjutan operasional karena dana tersebut dikelola secara mandiri dari biaya pendaftaran pengguna data sebagaimana ketentuannya dalam seksyen 61 Seksyen tentang Kumpulan Wang yang berbunyi:

> "(1) Bagi maksud Akta ini, suatu kumpulan wang yang dikenali sebagai "Kumpulan Wang Perlindungan Data Peribadi" ditubuhkan. (2) Kumpulan Wang hendaklah dikawal, disenggarakan dan dikendalikan oleh Pesuruhjaya. (3) Kumpulan Wang hendaklah terdiri daripada (a) apa-apa jumlah wang yang diperuntukkan oleh Parlimen bagi maksud Akta ini dari semasa ke semasa; (b) fi, kos dan apa-apa caj lain yang dikenakan oleh atau kena dibayar kepada Pesuruhjaya di bawah Akta ini; (c) semua wang yang diperoleh daripada penjualan, pelupusan, pemajakan, penyewaan atau apa-apa urus niaga lain mengenai harta alih atau tak alih yang terletak hak atau diperoleh oleh Pesuruhjaya; (d) semua wang yang dibayar kepada Pesuruhjaya dari semasa ke semasa bagi pinjaman yang diberikan oleh Pesuruhjaya; dan (e) semua jumlah wang atau harta lain yang boleh dalam apa-apa cara menjadi kena dibayar kepada atau terletak hak pada Pesuruhjaya berkenaan dengan apa-apa perkara yang bersampingan dengan fungsi dan kuasanya"

Kelebihan lain dari pengaturan di Malaysia adalah adanya mekanisme Tribunal Rayuan yang termaktub dalam Seksyen 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 Rayuan 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 Seksyen 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 Seksyen 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 Seksyen 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.