

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **A. Konsep Dasar Perlindungan Data Pribadi**

Data pribadi didefinisikan sebagai informasi apa pun yang dapat digunakan untuk mengidentifikasi individu secara langsung atau tidak langsung, seperti nama, alamat email, nomor telepon, atau data biometrik. Konsep ini berasal dari standar internasional seperti *General Data Protection Regulation* (GDPR) Uni Eropa, yang menetapkan bahwa data pribadi mencakup informasi yang berkaitan dengan identitas seseorang, termasuk data sensitif seperti kesehatan atau orientasi seksual. Dalam konteks global, definisi ini telah berkembang untuk mencakup data yang dihasilkan oleh teknologi digital, seperti jejak online atau data lokasi. Menurut Solove, data pribadi bukan hanya fakta statistik, tetapi juga konteks sosial yang membuat individu dapat dilacak, sehingga perlindungan harus melampaui batas hukum formal. Hal ini penting untuk memahami data pribadi bukanlah entitas statistik, melainkan elemen dinamis yang terus berkembang seiring kemajuan teknologi.<sup>10</sup>

Prinsip-prinsip perlindungan data pribadi mencakup beberapa elemen dasar yang dirancang untuk memastikan kontrol individu atas data mereka. Prinsip utama mencakup persetujuan beberapa elemen dasar yang dirancang untuk memastikan kontrol individu atas data mereka. Prinsip utama mencakup persetujuan eksplisit, dimana individu harus memberikan izin yang jelas sebelum data dikumpulkan; minimalisasi data, yang mengharuskan pengumpulan data hanya sebanyak yang diperlukan dan akuntabilitas, dimana

---

<sup>10</sup> Daniel J. Solove, 2021, *The Myth of the Privacy Paradox*, George Washington Law Review, George Washington University, Vol. 89 No. 1, hal. 1–51.

mengontrol data bertanggung jawab atas kepatuhan. Greenleaf dalam laporannya tentang hukum privasi data global menyatakan bahwa prinsip-prinsip ini telah dianut oleh lebih dari 160 negara dengan variasi lokal untuk menyesuaikan dengan budaya masing-masing. Hal ini memungkinkan perbandingan tujuan antara negara seperti Indonesia dan Malaysia, dimana prinsip persetujuan sering kali menjadi titik fokus dalam implementasi.<sup>11</sup>

Tantangan global dalam perlindungan data pribadi semakin kompleks di era digital, terutama dengan munculnya big data, kecerdasan buatan (AI), dan kebocoran data massal. Salah satu tantangan utama transfer data lintas batas, dimana data bergerak melampaui batas nasional, sehingga sulit diterapkan regulasi tunggal. Privacy Internasional dalam laporan tren privasi globalnya menyoroti bahwa kebocoran data telah meningkat 20% sejak tahun 2020, dengan kasus seperti pelanggaran di platform media sosial yang memengaruhi jutaan pengguna. Tantangan lain adalah keseimbangan kekuatan antara individu dan korporasi besar, dimana perusahaan teknologi sering kali mengumpulkan data tanpa pengawasan yang memadai. Hal ini menunjukkan bahwa regulasi nasional perlu disesuaikan dengan dinamika global untuk mencapai efektivitas.

Teori privasi memberikan landasan filosofis dan etis untuk perlindungan data pribadi, dengan akar dari hak asasi manusia (HAM). Teori

---

<sup>11</sup> National Laws dkk., 2023, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills*, Privacy Laws & Business International Report, Vol. 181.

klasik dari Warren dan Brandeis tentang “hak untuk dibiarkan sendiri” telah berevolusi menjadi argumen bahwa privasi adalah hak fundamental, seperti yang diakui dalam Deklarasi Universal Hak Asasi Manusia PBB. Solove memperluas ini dengan teori “taksonomi kerugian privasi”, yang mengidentifikasi berbagai bentuk kerugian privasi, seperti pencurian identitas atau deskriminasi. Dalam konteks modern, teori ini mendukung integrasi perlindungan data ke dalam HAM, dimana negara berkewajiban melindungi warga negara dari eksploitasi data. Hal ini relevan untuk kajian komparatif, karena teori ini memungkinkan evaluasi apakah regulasi di Indonesia dan Malaysia memenuhi standar HAM internasional.

Secara keseluruhan konsep dasar data pribadi dan perlindungannya menyediakan kerangka universal yang netral, memungkinkan analisis objektif terhadap hukum spesifik negara. Dengan menggabungkan definisi, prinsip, tantangan, dan teori, subbab ini menegaskan bahwa perlindungan data adalah hak fundamental di era digital, yang harus disesuaikan dengan konteks nasional untuk menghadapi tantangan global. Greenleaf (2023) menekankan bahwa harmonisasi internasional, seperti melalui ASEAN diperlukan untuk mengatasi kesinambungan, sementara Privacy Internasional (2024) mendorong reformasi regulasi untuk melindungi individu dan risiko teknologi baru. Ini membuka jalan untuk perbandingan antara negara Indonesia dengan negara Malaysia pada subbab selanjutnya.

## B. Prinsip-Prinsip Perlindungan Data Pribadi

Konsep perlindungan data mengisyaratkan bahwa individu memiliki hak untuk menentukan apakah mereka akan membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Lebih jauh, perlindungan privasi. Hak privasi telah berkembang sehingga dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.<sup>12</sup> Dengan dasar hukum tersebut, maka hak privasi terhadap data pribadi harus dilakukan dan perlindungan terhadap data pribadi sebagai hak privasi merupakan Hak Konstitusional warga negara Indonesia. Hak konstitusional adalah kewajiban bagi negara untuk memberikan perlindungan secara hukum untuk aspek kehidupan masyarakat Indonesia. Hak konstitusional harus didapatkan oleh setiap warga negara Indonesia. Hak konstitusional harus memiliki tujuan hukum yaitu kepastian hukum, keadilan hukum dan kemanfaatan hukum. Dengan dasar hukum tersebut juga beberapa peraturan perundang–undangan di Indonesia mengatur secara tersirat mengenai perlindungan data pribadi.<sup>13</sup>

Prinsip pertama dan yang paling fundamental adalah legalitas, kejujuran, dan transparansi dalam setiap tahap pemrosesan. Hal ini berarti setiap institusi atau korporasi yang bertindak sebagai pengendali data wajib memiliki dasar hukum yang sah (seperti persetujuan eksplisit atau kewajiban

---

<sup>12</sup> EErna Priliyasi, 2019, *Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending)*, Majalah Hukum Nasional, BPHN, No. 2, hal. 1–27.

<sup>13</sup> Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, 2021, *Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*, Jurnal Al-Wasath, Universitas Islam Jakarta, Vol. 2 No. 1, hal. 23

kontraktual) sebelum menyentuh data seseorang. Proses ini tidak boleh dilakukan dengan cara yang manipulatif atau tersembunyi; pemilik data harus diberikan gambaran yang sangat terang mengenai siapa yang mengelola data mereka, untuk kepentingan apa, dan bagaimana cara mereka bisa menarik kembali data tersebut. Transparansi ini menjadi fondasi kepercayaan antara masyarakat sebagai subjek data dengan penyelenggara sistem elektronik.<sup>14</sup>

Kemudian juga ada prinsip pembatasan tujuan dan minimalisasi data yang berfungsi sebagai rem terhadap ambisi pengumpulan data yang berlebihan. Di era *big data*, sering kali organisasi cenderung ingin mengambil informasi sebanyak mungkin "untuk berjaga-jaga", namun UU PDP secara tegas melarang hal ini. Pengumpulan data harus memiliki tujuan yang spesifik, jelas, dan sah secara hukum, serta hanya boleh mengambil jenis data yang benar-benar relevan dan diperlukan untuk tujuan tersebut. Jika sebuah aplikasi belanja hanya membutuhkan alamat untuk pengiriman, maka mereka tidak memiliki pembenaran moral maupun hukum untuk meminta akses ke daftar kontak telepon atau riwayat kesehatan pengguna tanpa urgensi yang nyata.

Dikenal pula aspek yang berkaitan dengan kualitas, keamanan, dan akuntabilitas. Pengendali data memikul tanggung jawab besar untuk memastikan data yang mereka kelola tetap akurat, lengkap, dan mutakhir agar tidak terjadi malapraktik data yang merugikan individu (misalnya kesalahan skor kredit akibat data yang usang). Selain itu, perlindungan harus mencakup

---

<sup>14</sup> Muhammad Akbar Eka Pradana dan Horadin Saragih, 2024, *Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya*, Innovative: Journal Of Social Science Research, Universitas Pahlawan, Vol. 4 No. 4, hal. 3412–25

aspek keamanan tingkat tinggi untuk menangkal ancaman siber dan kebocoran data yang kian marak. Prinsip akuntabilitas menegaskan bahwa jika terjadi kegagalan sistem atau kebocoran, pengendali data tidak bisa sekadar berdalih; mereka harus mempertanggungjawabkan langkah pengamanan yang telah diambil dan siap menghadapi sanksi hukum jika terbukti lalai dalam menjaga privasi warga negara.<sup>15</sup>

Terakhir, prinsip pembatasan masa simpan dan hak subjek data memastikan bahwa data seseorang tidak hidup selamanya di server perusahaan. Data wajib dimusnahkan atau dihapus segera setelah tujuan pemrosesannya tercapai atau ketika masa retensinya habis, kecuali ada ketentuan undang-undang lain yang mengatur sebaliknya. Hal ini memberikan kepastian bahwa individu memiliki kendali atas jejak digital mereka. Seluruh rangkaian prinsip ini menciptakan ekosistem di mana data pribadi diperlakukan sebagai aset berharga milik individu yang dipinjamkan secara bertanggung jawab, bukan sebagai komoditas bebas yang bisa dieksploitasi tanpa batas.<sup>16</sup>

### **C. Landasan Hukum Perlindungan Data Pribadi Di Indonesia**

Landasan hukum perlindungan data pribadi di Indonesia diatur dalam Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mulai berlaku efektif pada Oktober 2024 setelah masa transisi. Undang-

---

<sup>15</sup> Made Emy Andayani Citra dkk., 2023, *Perlindungan Hukum Terhadap Data Diri Pribadi Di Era Ekonomi Digital: Peluang Dan Tantangan (Studi Komparasi Indonesia Dan Malaysia)*, Jurnal Hukum Saraswati (JHS), Universitas Mahasaraswati Denpasar, Vol. 5 No. 2, hal. 519–34.

<sup>16</sup> Xynexis.com, “UU PDP: Langkah Awal Melindungi Data Pribadi,” xynexis.com, tanpa tahun, <https://xynexis.com/uu-pdp-langkah-awal-melindungi-data-pribadi/>.

undang ini menggantikan regulasi sebelumnya yang terfragmentasi, seperti Peraturan Pemerintah Nomor 71 tahun 2019 tentang Sistem Dan Transaksi Elektronik, dan menetapkan kerangka komprehensif untuk melindungi data pribadi warga negara. Landasan ini di dasarkan pada prinsip-prinsip di internasional seperti *General Data Protection Personal* (GDPR), namun disesuaikan dengan konteks nasional Indonesia, termasuk pengakuan hak asasi manusia dalam Undang Undang Dasar Tahun 1945. Undang-undang perlindungan data pribadi (PDP) mendefinisikan data pribadi sebagai informasi yang dapat mengidentifikasi individu, baik langsung maupun tidak langsung, dan menekan perlindungan dari perlindungan oleh pihak swasta dan pemerintah.

Salah satu aspek kunci dalam Undang-Undang Perlindungan Data Pribadi adalah prinsip yang mencakup eksplisit, minimalisasi data, dan akuntabilitas. Pengendalian data (*data controllers*) wajib mendapatkan persetujuan yang jelas dari subjek data sebelum pengumpulan, sedangkan pemproses data atau pengolah data harus memastikan keamanan. Undang-undang ini juga mengatur hak subjek data, seperti hak akses, koreksi,, penghapusan dan portabilitas data, yang mirip dengan hak-hak dalam GDPR. Namun ada yang menyampaikan untuk data publik atau kepentingan negara, yang memungkinkan terjadinya dalam konteks keamanan nasional. Hal ini menunjukan bahwa landasan hukum indonesia lebih menekankan keseimbangan antara privasi individu dan kepentingan publik.

Peran lembaga Otoritas Pelindungan Data Pribadi sebagai entitas pengawas independen merupakan komponen fundamental dalam eksekusi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaga ini diberi mandat untuk memenuhi kepatuhan terhadap norma-norma perlindungan data, mengelola aduan dari subjek data, serta menerapkan sanksi administratif dan pidana yang ketat. Didirikan secara eksplisit melalui ketentuan Undang-undang Perlindungan Data Pribadi, Otoritas PDP dilengkapi dengan otoritas investigasi mendalam dan berwenang untuk mengenakan denda maksimal sebesar Rp 2 miliar bagi pelanggaran signifikan. Dalam operasionalnya, lembaga diantisipasi akan berkolaborasi erat dengan Kementerian Komunikasi dan Informatika (Kominfo) guna mengatur ekosistem platform digital, termasuk media sosial dan layanan e-commerce. Meskipun demikian, hambatan awal mencakup defisiensi pada kapasitas sumber daya manusia dan infrastruktur teknis, yang berpotensi mengurangi efektivitas pengawasan dan memperlambat respons terhadap kejadian pelanggaran data. Analisis komparatif dengan lembaga serupa di negara tetangga, seperti *Personal Data Protection Commissioner* (PDPC) di Malaysia, menunjukkan bahwa Otoritas PDP perlu memperkuat mekanisme pelatihan dan teknologi untuk mencapai standar internasional, sehingga memastikan perlindungan data pribadi yang efektif di tengah kompleksitas ketahanan nasional.<sup>17</sup>

---

<sup>17</sup> Sinta Amalia, 2023, *Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura*, Jurnal Hukum & Pembangunan, Universitas Indonesia, Vol. 53 No. 1.



Perbandingan dengan regulasi sebelumnya menunjukkan evolusi landasan hukum Indonesia menuju standar global. Sebelum Undang-Undang Perlindungan Data Pribadi, perlindungan data bergantung pada Undang-Undang Informasi Dan Transaksi Elektronik Tahun 2008 yang lebih fokus pada transaksi elektronik daripada privasi data secara spesifik. Undang-undang perlindungan data pribadi memperkenalkan mekanisme notifikasi pelanggaran dalam 72 jam dan audit rutin, yang tidak ada dalam regulasi lama. Hal ini mencerminkan respons terhadap kasus pelanggaran data di e-commerce dan media sosial. Meskipun demikian muncul kritik bahwa undang-undang perlindungan data pribadi masih kurang tegas dalam sanksi pelanggaran oleh entitas asing, yang sering kali beroperasi diluar mengakui Indonesia.

Tantangan penerapan landasan hukum ini meliputi kesenjangan antara teori dan praktik terutama di era digital yang cepat berubah. Dengan maraknya AI undang-undang perlindungan data pribadi perlu di uji melalui putusan pengadilan dan regulasi turunan. Studi awal menunjukkan bahwa kesadaran masyarakat tentang hak data masih rendah, sehingga diperlukan pendidikan dan sosialisasi. Selain itu integrasi dengan hukum internasional, seperti APEC privacy framework, menjadi penting untuk menangani transfer data melewati batas. Secara keseluruhan landasan hukum ini menandai langkah maju indonesia dalam perlindungan data pribadi, meskipun tetap memerlukan penyempurnaan untuk menghadapi tantangan masa depan.<sup>18</sup>

---

<sup>18</sup> Fachrul Razi dan Dwi Pratiwi Markus, 2024, *Implementation and Challenges of the Personal Data Protection Law in Indonesia*, International Journal of Economic and Business Applied, Vol. 5 No. 12, hal. 6015–21.

#### **D. Landasan Hukum Perlindungan Data Pribadi Di Malaysia**

Di Malaysia fondasi hukum untuk melindungi data pribadi individu tercantum dalam *Personal Data Protection Act 2010* (PDPA), ini merupakan Undang-undang pertama di Asia Tenggara yang secara khusus mengatur privasi data secara komprehensif. Undang-undang ini diberlakukan secara bertahap mulai tahun 2013, dengan fokus pengumpulan, pemrosesan, dan penyimpanan data pribadi oleh organisasi komersial. *Personal Data Protection Act* (PDPA) menetapkan delapan prinsip utama perlindungan data, termasuk kepatuhan umum, pemberitahuan, pilihan, integritas data, retensi, transfer, akses, dan keamanan, yang bertujuan untuk melindungi hak individu terhadap penyalahgunaan informasi pribadi di era digital. Kerangka ini mencerminkan komitmen Malaysia untuk menyeimbangkan kepentingan ekonomi dengan perlindungan hak asasi manusia, meskipun awalnya tidak mencakup sektor publik atau data sensitif.

Sejak berlakunya *personal data protection act* implementasinya telah mengalami berbagai tantangan, termasuk kurangnya mekanisme penegakan yang kuat dan sanksi yang relatif ringan, yang menyebabkan kepatuhan organisasi masih rendah. *Personal data protection commissioner* (PDPC) ditunjuk sebagai otoritas pengawas untuk menangani keluhan dan memberikan panduan, tetapi hingga sebelum amandemen terbaru, undang-undang ini dianggap kurang adaptif terhadap perkembangan teknologi seperti kecerdasan buatan (AI). Studi akademik menunjukkan bahwa *personal data protection act* 2010 terinspirasi dari model Eropa seperti *data protection directive* 1995,

namun disesuaikan dengan konteks lokal Malaysia yang menekankan pada sektor swasta.<sup>19</sup>

Pada tahun 2024 Malaysia melakukan reformasi signifikan melalui Personal Data Protection (Amendment) Act 2024, yang disahkan oleh parlemen pada Juli 2024 dan menerima persetujuan Kerajaan pada Oktober 2024. Amandemen ini diperkuat landasan hukum dengan memperkenalkan ketentuan baru mengenai penegakan, termasuk peningkatan denda hingga RM10 juta atau 2% dari omset global untuk pelanggaran serius, serta kewajiban pelaporan insiden data dalam waktu 72 jam. Reformasi ini juga memperluas cakupan *personal data protection act* (PDPA) untuk mencakup transfer data lintas batas dengan persyaratan yang lebih ketat, seperti penilaian dampak transfer data, guna mencegah eksploitasi data oleh entitas asing. Perubahan ini menandai evolusi dari pendekatan reaktif menjadi proaktif dalam perlindungan data pribadi.

Implikasi amandemen 2024 terhadap organisasi bisnis di Malaysia sangat luas, karena mengharuskan penyesuaian kebijakan internal, pelatihan karyawan, dan audit kepatuhan reguler. Jurnal akademik ini menyoroti bahwa reformasi ini tidak hanya meningkatkan kredibilitas Malaysia sebagai pusat digital di Asia, tetapi juga mempengaruhi rantai pasok global terutama bagi perusahaan multinasional yang beroperasi di sektor fintech dan e-commerce. Selain itu, pengenalan *Data Protection Officer* (DPO) wajib untuk organisasi

---

<sup>19</sup> Zaiton Hamin dkk., 2025, *Recent Reforms to the Personal Data Protection Act 2010 and Its Implications for Business Organisations in Malaysia*, International Journal of Research and Innovation in Social Science (IJRISS), Vol. IX No. 2454, hal. 410–22.

besar memperkuat akuntabilitas, meskipun tantangan implementasi seperti kurangnya sumber daya di kalangan UKM menjadi isu krusial.<sup>20</sup> Dengan demikian landasan hukum ini selaras dengan tuntutan ekonomi digital pasca pandemi.

Secara keseluruhan landasan hukum perlindungan data pribadi di Malaysia melalui *Personal Data Protection Act* (PDPA) dan amandemennya mencerminkan adaptasi berkelanjutan terhadap dinamika global, dengan tujuan utama melindungi hak privasi sambil mendukung inovasi. Meskipun masih ada ruang untuk perbaikan, seperti integrasi dengan regulasi AI etis, kerangka ini telah menempatkan Malaysia sebagai pemimpin regional dalam tata kelola data. Prospek masa depan yang menjanjikan dengan potensi harmonisasi lebih lanjut melalui kerjasama ASEAN, yang memperkuat posisi hukum nasional dalam menghadapi ancaman siber yang kompleks.

---

<sup>20</sup> Sakshi Shivhare, "Malaysia Menentukan Arah Digitalnya: Panduan Kerangka Kerja Baru Untuk Perlindungan Data Dan Etika AI," Sakshi Shivhare, 2025.