Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 9400-9414

Implikasi Yuridis Undang-Undang Perlindungan Data Pribadi terhadap Model Bisnis Digital di Indonesia

Kristina Andini[1]
[1]Universitas Muhammadiyah Ahmad Dahlan Palembang
Corresponding Author: Kristina Andini, e-mail: kristinaandini1003@gmail.com

Published: February, 2026

ABSTRAK
Perkembangan ekonomi digital di Indonesia mendorong munculnya berbagai model bisnis berbasis teknologi yang sangat bergantung pada pemrosesan data pribadi pengguna. Data pribadi telah bertransformasi menjadi aset ekonomi strategis yang digunakan untuk personalisasi layanan, analisis perilaku konsumen, serta monetisasi berbasis data. Di sisi lain, intensitas pemanfaatan data tersebut meningkatkan risiko pelanggaran privasi, kebocoran data, dan ketimpangan posisi antara pelaku usaha dan konsumen. Penelitian ini bertujuan menganalisis pengaturan perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta implikasi hukumnya terhadap model bisnis digital di Indonesia. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan konseptual (*conceptual approach*) serta dianalisis secara kualitatif deskriptif. Hasil penelitian menunjukkan bahwa UU PDP menetapkan prinsip legalitas, pembatasan tujuan, transparansi, keamanan, dan akuntabilitas dalam pemrosesan data pribadi, sekaligus memperkuat hak subjek data serta kewajiban pengendali dan prosesor data. Ketentuan tersebut membawa konsekuensi langsung terhadap struktur dan strategi model bisnis digital, khususnya yang berbasis personalisasi, profiling, dan integrasi data lintas layanan. UU PDP tidak hanya berfungsi sebagai instrumen perlindungan hak privasi, tetapi juga membentuk standar baru tata kelola bisnis digital melalui penerapan perlindungan data sejak tahap perancangan sistem dan penguatan manajemen risiko kepatuhan. Dengan demikian, keberlanjutan bisnis digital di Indonesia sangat ditentukan oleh kemampuan pelaku usaha mengintegrasikan perlindungan data pribadi ke dalam strategi bisnisnya.

Kata Kunci: Perlindungan Data Pribadi, UU PDP, Bisnis Digital

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan teknologi yang berlangsung sangat cepat, baik di Indonesia maupun secara global, telah memberikan pengaruh signifikan terhadap berbagai aspek kehidupan, termasuk sektor ekonomi dan bisnis. Dalam konteks era digital, transformasi pada bidang ekonomi dan bisnis menjadi suatu keniscayaan seiring dengan hadirnya inovasi teknologi yang semakin maju (Khairi et al., 2025). Sejalan dengan percepatan perkembangan teknologi, transformasi menuju ekonomi digital telah berkembang menjadi fenomena global dalam beberapa tahun terakhir. Ekonomi digital dipahami sebagai suatu konsep ekonomi kontemporer yang mengintegrasikan layanan serta teknologi berbasis internet ke dalam beragam model bisnis dan komoditas. Konsep ini mencakup pemanfaatan teknologi digital sebagai sarana untuk menunjang dan mengoptimalkan berbagai aktivitas ekonomi (Faisal & Fasa, 2025). Transformasi digital telah mendorong lahirnya berbagai model bisnis berbasis teknologi informasi, seperti E-commerce, fintech, marketplace, dan platform media sosial.

Perdagangan elektronik atau electronic commerce (E-commerce) merupakan proses transaksi jual beli barang maupun jasa yang dilakukan melalui media internet. Aktivitas ini mencakup pemindahan dana, pertukaran data, serta pelaksanaan transaksi bisnis, baik antara perusahaan dan konsumen (Business to Consumer/B2C), antarperusahaan (Business to Business/B2B), maupun antar konsumen (Customer to Customer/C2C). Kehadiran E-commerce telah mentransformasi praktik bisnis secara signifikan dengan membuka akses pasar yang bersifat global serta menjangkau basis konsumen yang lebih luas. Fenomena ini juga mendorong perubahan mendasar dalam pola masyarakat berbelanja, menjalankan usaha, dan melakukan interaksi ekonomi (Ma'sumatul Maghfiroh et al., 2023). Model bisnis tersebut sangat bergantung pada pengumpulan, pemrosesan, dan analisis data pribadi pengguna sebagai dasar pengambilan keputusan bisnis dan strategi pemasaran.

Data pribadi tidak lagi semata-mata dipahami sebagai informasi individual, tetapi telah berkembang menjadi komoditas ekonomi yang memiliki nilai strategis tinggi dalam ekosistem bisnis digital. Walaupun E-commerce menyediakan kemudahan serta efisiensi dalam transaksi, praktik ini juga menimbulkan berbagai risiko keamanan. Keamanan pada dasarnya merujuk pada upaya perlindungan terhadap sumber daya fisik maupun konseptual dari ancaman yang berasal dari faktor alam maupun tindakan manusia. Dalam konteks sumber daya konseptual, perlindungan tersebut mencakup data dan informasi. Oleh karena itu, isu utama dalam lingkungan E-commerce saat ini berkaitan erat dengan persoalan privasi dan keamanan data pribadi (Kehista et al., 2023). Namun, intensitas pemanfaatan data pribadi yang tinggi juga menimbulkan berbagai permasalahan hukum, khususnya terkait pelanggaran hak privasi, kebocoran data, dan penyalahgunaan informasi pribadi.

Berbagai kasus kebocoran data mencerminkan masih lemahnya perlindungan hukum terhadap data pribadi sebelum terbentuknya regulasi khusus yang bersifat komprehensif. Peristiwa tersebut tidak hanya merupakan pelanggaran terhadap hak atas privasi, tetapi juga berpotensi menimbulkan dampak kerugian sosial dan ekonomi yang signifikan, baik bagi individu maupun Lembaga (Lesmana & Nasution, 2025). Kondisi tersebut berimplikasi pada penurunan tingkat kepercayaan publik terhadap penyelenggara sistem elektronik maupun pelaku usaha berbasis digital. Dari perspektif penyedia platform, insiden kebocoran data berpotensi merusak reputasi perusahaan, mengurangi tingkat kepercayaan investor, serta menimbulkan konsekuensi berupa sanksi hukum. Oleh sebab itu, perlindungan data pribadi semestinya tidak hanya dimaknai sebagai kewajiban etis, melainkan juga sebagai tanggung jawab yuridis yang melekat pada setiap pengendali dan pengelola data, khususnya dalam penyelenggaraan platform E-commerce (Diah & Wiraguna, 2025).

Sebagai respon atas kebutuhan perlindungan hukum tersebut, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini memberikan pengaturan yang tegas mengenai hak subjek data, kewajiban pengendali data, serta sanksi atas pelanggaran pengelolaan data pribadi. Berbagai penelitian sebelumnya umumnya menempatkan Undang-Undang Perlindungan Data Pribadi sebagai instrumen perlindungan hak privasi individu dan penguatan hak subjek data dalam ruang digital. Namun, kajian yang secara khusus menelaah bagaimana keberlakuan UU PDP memengaruhi struktur, strategi, dan model monetisasi bisnis digital masih relatif terbatas. Padahal, model bisnis digital modern sangat bergantung pada pemrosesan data pribadi sebagai aset ekonomi utama. Oleh karena itu, penelitian ini tidak hanya membahas aspek perlindungan hukum terhadap data pribadi, tetapi juga menganalisis secara normatif implikasi struktural UU PDP terhadap model bisnis digital, khususnya terkait praktik monetisasi data, personalisasi layanan, dan tata kelola perusahaan berbasis data.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk mengkaji norma hukum yang berlaku terkait perlindungan data pribadi dalam konteks bisnis digital. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menelaah ketentuan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta pendekatan konseptual (*conceptual approach*) yang berkaitan dengan konsep perlindungan data pribadi dan model bisnis digital. Analisis dilakukan melalui penafsiran sistematis dan gramatikal terhadap norma dalam UU PDP serta pengaitannya dengan konsep model bisnis digital. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Teknik analisis data dilakukan secara kualitatif dengan metode deskriptif-analitis.

HASIL DAN PEMBAHASAN

1. Pengaturan Perlindungan Data Pribadi dalam Undang-Undang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur secara komprehensif perlindungan data pribadi sebagai bagian dari hak asasi manusia. Pasal 1 UU PDP mendefinisikan data pribadi sebagai setiap data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, 2022), data pribadi didefinisikan sebagai setiap data tentang orang perseorangan yang

teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya. UU PDP menegaskan prinsip-prinsip dasar perlindungan data pribadi, antara lain prinsip legalitas, transparansi, pembatasan tujuan, akurasi data, keamanan, dan akuntabilitas.

Hadirnya UU PDP memiliki signifikansi yang krusial dalam memperkuat jaminan hak-hak dasar warga negara Indonesia, khususnya yang berkaitan dengan privasi dan perlindungan diri. Regulasi ini memberikan landasan hukum yang memadai bagi perlindungan data pribadi, sehingga dapat meningkatkan kepercayaan masyarakat dalam memberikan data pribadinya tanpa kekhawatiran akan penyalahgunaan (Sulistianingsih et al., 2023). UU PDP juga memberikan hak-hak kepada subjek data, seperti hak untuk mendapatkan informasi, hak akses, hak perbaikan, hak penghapusan, dan hak penarikan persetujuan. Di sisi lain, pengendali data dan prosesor data dibebani kewajiban hukum untuk menjamin keamanan data pribadi, memperoleh persetujuan yang sah, serta mencegah kebocoran data.

Dalam rangka memastikan kepatuhan terhadap ketentuan Undang-Undang Perlindungan Data Pribadi (UU PDP), pelanggaran terhadap aturan tersebut dapat dikenai sanksi administratif, perdata, maupun pidana. Sanksi administratif yang diatur dalam Bab XI Pasal 57–60 mencakup peringatan tertulis, penghentian sementara aktivitas pemrosesan data, penghapusan atau pemusnahan data pribadi, serta denda administratif kepada pengendali atau pemroses data atas pelanggaran terhadap kewajiban dalam UU PDP, misalnya tidak memproses data sesuai tujuan atau gagal mencegah akses tidak sah terhadap data. Denda administratif tersebut dapat mencapai persentase tertentu dari pendapatan tahunan pihak yang bersangkutan. Selain itu, Bab XII mengatur sanksi pidana bagi pihak yang dengan sengaja dan secara melawan hukum mengungkapkan atau menyebarluaskan data pribadi, termasuk ancaman pidana kurungan dan/atau denda finansial untuk pelanggaran tersebut sebagaimana tercantum dalam ketentuan pasal yang relevan (Kaharuddin et al., 2025). Ketentuan sanksi tersebut menunjukkan keseriusan negara dalam menegakkan perlindungan data pribadi dan mendorong kepatuhan pelaku usaha.

2. Model Bisnis Digital dan Peran Data Pribadi

Bisnis digital merupakan model kegiatan usaha yang memanfaatkan sistem elektronik, jaringan internet, serta pemrosesan data sebagai infrastruktur utama dalam penciptaan nilai dan interaksi dengan konsumen (Cahyadi et al., 2022). Karakteristik utama dari model bisnis ini terletak pada optimalisasi data sebagai sumber daya strategis dalam penciptaan nilai ekonomi. Dalam implementasinya, data pribadi dimanfaatkan untuk mendukung personalisasi layanan, analisis perilaku konsumen, penargetan

periklanan, serta pengembangan produk yang disesuaikan dengan kebutuhan pengguna. Dalam konteks ekonomi digital, data kerap diposisikan sebagai "minyak baru" (new oil) yang berperan sebagai sumber utama nilai tambah dalam ekosistem ekonomi berbasis platform (Couldry & Mejias, 2020).

Model bisnis digital berkembang dalam berbagai bentuk, antara lain model layanan gratis (free model), freemium, E-commerce, marketplace pendekatan peer-to-peer atau two-sided, layanan berbasis permintaan (on-demand), sharing model, ekosistem digital (super-app), layanan berlangganan (subscription), open-source, serta model berbasis pengalaman digital (Cahyadi et al., 2022). Meskipun memiliki mekanisme operasional yang berbeda, seluruh model tersebut memiliki kesamaan mendasar, yaitu ketergantungan pada pengumpulan dan pemrosesan data pribadi pengguna sebagai dasar pengambilan keputusan bisnis dan pengembangan layanan.

Dalam konteks Indonesia, pesatnya pertumbuhan E-commerce, marketplace, fintech, serta platform berbasis aplikasi telah menghasilkan akumulasi data pribadi dalam skala besar. Setiap aktivitas pengguna mulai dari pendaftaran akun, transaksi, hingga interaksi dalam platform menghasilkan jejak data yang kemudian diolah menjadi profil perilaku konsumen (Kurnianingrum, 2020). Kondisi ini menempatkan pelaku usaha digital dalam posisi yang dominan karena memiliki kendali atas informasi pribadi pengguna, sehingga berpotensi menimbulkan ketidakseimbangan hubungan hukum antara pelaku usaha dan konsumen.

Ketergantungan yang tinggi terhadap data pribadi juga meningkatkan risiko hukum apabila pemrosesan data tidak disertai sistem perlindungan yang memadai. Praktik pemanfaatan data untuk promosi, penyusunan profil pelanggan, maupun pemindahtanganan data kepada pihak ketiga tanpa dasar hukum yang jelas menunjukkan adanya potensi pelanggaran terhadap hak privasi dan prinsip perlindungan data pribadi.

Tabel 1. Keterkaitan Model Bisnis Digital dengan Peran Data Pribadi

Model Bisnis Digital	Jenis Data Pribadi yang Diproses	Peran Data Dalam Model Bisnis	Risiko Hukum yang Muncul	Pasal UU PDP yang Terkait
Free Model	Data identitas, preferensi, lokasi, Riwayat interaksi	Personalisasi konten & iklan tertarget, profiling perilaku	Pemrosesan tanpa dasar hukum jelas,	Pasal 5, Pasal 6, dan Pasal 7 (dasar

	pengguna		profiling tanpa transparansi	pemrosesan & consent); Pasal 12 (hak akses informasi); Pasal 15 (hak menolak pemrosesan tertentu)
Marketplace (Two-Sided Platform)	Data pembeli, penjual, transaksi, ulasan, riwayat pencarian	Algoritma rekomendasi, reputasi penjual, promosi	Kebocoran data akun dan transaksi, penyalahgunaan data oleh pihak ketiga	Pasal 20 dan Pasal 21 (tanggung jawab pengendali & prosesor); Pasal 35 (keamanan data); Pasal 46 (pemrosesan oleh pihak lain)
E-commerce	Nama, alamat, kontak, data pembayaran, histori transaksi	Pemrosesan pesanan, logistik, pemasaran berbasis histori pembelian	Penyimpanan data berlebihan, penggunaan di luar tujuan awal	Pasal 5 (pembatasan tujuan); Pasal 9 (minimisasi data); Pasal 16 (hak penghapusan); Pasal 20 (tanggung jawab pengendali)
On-Demand Services	Lokasi real-time, riwayat perjalanan, preferensi layanan	Penentuan rute, tarif dinamis, personalisasi layanan	Pelacakan lokasi berlebihan, pelanggaran privasi	Pasal 5 (tujuan spesifik); Pasal 15 (hak membatasi pemrosesan);

			pergerakan	Pasal 35 (keamanan data)
Fintech & Dompet Digital	Data identitas, biometrik (jika ada), data keuangan, histori transaksi	Verifikasi pengguna, credit scoring, pencegahan fraud	Kebocoran data finansial, pencurian identitas	Pasal 4(2) (data pribadi spesifik); Pasal 20 (tanggung jawab pengendali); Pasal 35 (keamanan); Pasal 67, Pasal 68, Pasal 69, Pasal 70, dan Pasal 71 (sanksi pidana bila disalahgunakan)
Subscription & Streaming	Preferensi tontonan/musik, histori penggunaan	Rekomendasi konten, retensi pelanggan	Profiling tanpa transparansi, penggunaan data berlebihan	Pasal 5, Pasal 6, dan Pasal 7 (legalitas & consent); Pasal 12 (hak akses informasi); Pasal 15 (hak keberatan)
Ekosistem Digital / Super-App	Data lintas layanan (transportasi, belanja, pembayaran)	Integrasi layanan, analisis perilaku komprehensif	Penggabungan data tanpa persetujuan baru	Pasal 6 (dasar hukum tiap tujuan); Pasal 24 (perlindungan sejak perancangan sistem); Pasal

				20 (akuntabilitas pengendali); Pasal 35 (keamanan terpadu)
Sharing Economy	Identitas, reputasi digital, riwayat transaksi	Sistem kepercayaan antar pengguna	Penyimpanan reputasi permanen, kesalahan data merugikan subjek	Pasal 13 (hak perbaikan); Pasal 16 (hak penghapusan); Pasal 5 (akurasi & tujuan pemrosesan)
Freemium Apps	Data penggunaan fitur, preferensi layanan, perangkat	Strategi konversi ke layanan premium	Pemantauan perilaku tanpa pemahaman memadai dari pengguna	Pasal 5, Pasal 6, dan Pasal 7 (legalitas & persetujuan); Pasal 12–13 (hak akses & perbaikan data)
Experience-Based Digital Services	Data interaksi pengguna, preferensi personalisasi	Peningkatan pengalaman pengguna berbasis data	Personalisasi invasif & profiling mendalam	Pasal 5 (pembatasan tujuan); Pasal 6 dan Pasal 7 (dasar hukum & consent); Pasal 15 (hak menolak profiling tertentu)

Pemetaan pada tabel menunjukkan bahwa seluruh model bisnis digital pada dasarnya beroperasi dengan menjadikan data pribadi sebagai infrastruktur utama penciptaan nilai ekonomi. Perbedaannya tidak terletak pada ada atau tidaknya pemrosesan data, melainkan pada intensitas, jenis data, serta tujuan pemrosesan. Model berbasis iklan seperti free model dan freemium menempatkan data perilaku sebagai komoditas

utama melalui teknik profiling dan personalisasi, sehingga isu hukum yang paling dominan berkaitan dengan legalitas pemrosesan dan keabsahan persetujuan sebagaimana diatur dalam Pasal 5–7 UU PDP. Risiko meningkat ketika pengguna tidak memperoleh informasi yang memadai mengenai cakupan pemrosesan, yang berpotensi melanggar prinsip transparansi dan pembatasan tujuan.

Pada sisi lain, model platform dua sisi seperti marketplace dan ekosistem digital (super-app) menghadirkan kompleksitas hukum yang lebih tinggi karena melibatkan banyak aktor pemrosesan data dalam satu ekosistem. Dalam model ini, data pribadi tidak hanya diproses oleh satu pengendali, tetapi juga dibagikan kepada mitra, penjual, atau penyedia layanan lain. Situasi ini meningkatkan potensi pelanggaran prinsip akuntabilitas dan keamanan data sebagaimana diatur dalam Pasal 20 dan Pasal 35 UU PDP. Risiko hukum tidak hanya berasal dari kegagalan internal pengendali utama, tetapi juga dari lemahnya pengawasan terhadap pihak ketiga yang memproses data dalam satu rantai layanan digital.

Model bisnis dengan pemrosesan data spesifik dan berisiko tinggi, seperti fintech dan layanan berbasis lokasi (on-demand services), memiliki tingkat kerentanan hukum paling signifikan. Pemrosesan data finansial, biometrik, dan lokasi real-time bersinggungan langsung dengan kategori data pribadi spesifik sebagaimana dimaksud dalam Pasal 4 ayat (2) UU PDP. Kebocoran atau penyalahgunaan data dalam sektor ini dapat menimbulkan kerugian langsung bagi subjek data, baik secara ekonomi maupun keamanan pribadi, sehingga tidak hanya memicu tanggung jawab administratif, tetapi juga membuka kemungkinan pertanggung jawaban pidana berdasarkan Pasal 67–71 UU PDP.

Sementara itu, model berbasis personalisasi pengalaman digital seperti streaming dan experience-based services memperlihatkan kecenderungan menuju pemrosesan data yang semakin invasif melalui analisis perilaku mendalam. Dalam konteks ini, isu hukum yang menonjol berkaitan dengan hak subjek data untuk menolak pemrosesan tertentu dan meminta penghapusan data sebagaimana diatur dalam Pasal 15 dan Pasal 16 UU PDP. Ketentuan ini membatasi praktik eksploitasi data jangka panjang yang selama ini menjadi fondasi algoritma bisnis digital.

Dengan demikian, dapat disimpulkan bahwa semakin kompleks model bisnis digital dan semakin sensitif jenis data yang diproses, semakin tinggi pula tingkat risiko hukum yang menyertainya. UU PDP berfungsi sebagai instrumen normatif yang menyeimbangkan kepentingan ekonomi berbasis data dengan perlindungan hak privasi individu, sekaligus mendorong transformasi tata kelola perusahaan digital menuju pendekatan privacy by design dan akuntabilitas korporasi. Dalam praktik, masih ditemukan

pemrosesan data pribadi yang tidak disertai dasar hukum yang memadai, misalnya dengan menggunakannya untuk keperluan promosi, profil pelanggan, atau bahkan menjualnya kepada pihak ketiga (Simanjuntak, 2024). Ketergantungan yang tinggi terhadap data pribadi menjadikan model bisnis digital rentan terhadap risiko hukum apabila tidak diimbangi dengan sistem perlindungan data yang memadai.

3. Implikasi Hukum UU PDP terhadap Model Bisnis Digital

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir untuk memberikan kerangka hukum yang jelas terhadap pengelolaan data pribadi di Indonesia, terutama bagi pelaku ekosistem bisnis digital yang intensif mengumpulkan, memproses, dan menyimpan data konsumen (Akbar et al., 2025). Pengaturan ini menandai pergeseran paradigma dari pendekatan sektoral menuju rezim perlindungan data berbasis hak asasi manusia, di mana pemrosesan data pribadi tidak lagi dipandang sebagai aktivitas bisnis semata, tetapi sebagai tindakan hukum yang tunduk pada prinsip legalitas, akuntabilitas, dan perlindungan hak individu. Pemberlakuan UU PDP membawa implikasi hukum yang signifikan terhadap model bisnis digital yaitu pelaku usaha wajib menyesuaikan mekanisme pengumpulan dan pemrosesan data dengan prinsip persetujuan yang sah dan transparan. Hal ini berdampak pada praktik pemasaran digital yang sebelumnya bersifat masif dan agresif.

Dampak utamanya pada bisnis digital yaitu adanya kewajiban persetujuan (*consent*) sebelum data diproses (Wijayanto et al., 2025). Secara normatif, prinsip dasar pemrosesan data pribadi diatur dalam Pasal 5 UU PDP, yang menegaskan bahwa pemrosesan data harus dilakukan secara terbatas, spesifik, sah, dan transparan. Selanjutnya, Pasal 6 mensyaratkan bahwa setiap pemrosesan data harus memiliki dasar hukum yang jelas, salah satunya berupa persetujuan subjek data. Ketentuan ini diperjelas dalam Pasal 7, yang menegaskan bahwa persetujuan harus diberikan secara eksplisit dan dapat ditarik kembali. Norma tersebut secara langsung memengaruhi model bisnis digital yang selama ini bertumpu pada pengumpulan data dalam skala besar untuk kepentingan analisis perilaku konsumen, personalisasi layanan, dan periklanan berbasis data. Dengan berlakunya UU PDP, pemrosesan data tidak lagi dapat dilakukan secara luas tanpa batas tujuan, melainkan harus selalu ditautkan pada dasar hukum yang sah dan tujuan yang telah diberitahukan kepada subjek data.

Hak subjek data (*data subject rights*) seperti hak akses, koreksi, penghapusan, dan keberatan atas data (Wijayanto et al., 2025). Penguatan posisi individu sebagai pemilik kendali atas data pribadinya juga terlihat dalam pengaturan hak subjek data sebagaimana diatur dalam Pasal 12 sampai dengan Pasal 15 UU PDP. Hak untuk mengakses, memperbaiki, menghapus, serta menarik kembali persetujuan atas pemrosesan data

mengubah hubungan hukum antara pengguna dan penyedia layanan digital. Dalam konteks model bisnis berbasis personalisasi dan profiling, ketentuan ini membatasi keleluasaan perusahaan dalam mempertahankan dan memanfaatkan data historis pengguna secara berkelanjutan. Secara yuridis, hak penghapusan dan pencabutan persetujuan berpotensi mengurangi stabilitas basis data komersial yang menjadi fondasi berbagai algoritma bisnis digital. Hal ini menunjukkan bahwa UU PDP secara tegas memprioritaskan perlindungan hak individu dibanding kepentingan ekonomi berbasis data.

Kewajiban pengendali/prosesor data untuk mengimplementasikan prinsip perlindungan data sejak awal (*privacy by design*) (Wijayanto et al., 2025). Dari sisi kelembagaan, UU PDP memperluas tanggung jawab pelaku usaha digital sebagai Pengendali Data Pribadi. Pasal 20 sampai dengan Pasal 23 UU PDP menegaskan kewajiban pengendali dan prosesor data untuk menjamin keamanan data, memastikan kepatuhan terhadap prinsip perlindungan data, serta melaporkan kegagalan perlindungan data pribadi. Kewajiban ini menempatkan perlindungan data sebagai bagian dari tata kelola korporasi, bukan sekadar aspek teknis teknologi informasi. Dalam praktik bisnis digital, hal ini berdampak pada meningkatnya kebutuhan investasi dalam sistem keamanan, audit internal, pelatihan sumber daya manusia, serta pembentukan mekanisme kepatuhan internal. Dengan demikian, UU PDP mendorong transformasi perlindungan data dari fungsi operasional menjadi fungsi strategis dalam manajemen risiko perusahaan. Lebih lanjut, Pasal 24 UU PDP menuntut agar perlindungan data pribadi telah dipertimbangkan sejak tahap perancangan sistem elektronik. Meskipun istilah privacy by design tidak disebutkan secara eksplisit, ketentuan ini secara konseptual mencerminkan prinsip tersebut, yaitu integrasi perlindungan data sejak tahap awal pengembangan produk dan layanan digital. Konsekuensinya, perusahaan digital dituntut membangun koordinasi lintas divisi khususnya antara unit teknologi informasi, hukum, dan manajemen risiko agar kepatuhan terhadap perlindungan data menjadi bagian inheren dari desain sistem.

Sanksi administratif dan pidana bagi pelanggar UU PDP (Wijayanto et al., 2025), diperkuat melalui pengaturan sanksi dalam Pasal 58 sampai dengan Pasal 63 mengenai sanksi administratif serta Pasal 67 sampai dengan Pasal 71 UU PDP mengenai sanksi pidana. Ancaman sanksi ini menggeser risiko bisnis digital dari sekadar risiko reputasi menjadi risiko hukum yang konkret. Pelanggaran terhadap ketentuan persetujuan, pemrosesan tanpa dasar hukum, atau kelalaian dalam melindungi data dapat berujung pada denda administratif yang signifikan, penghentian kegiatan pemrosesan data, bahkan pertanggungjawaban pidana. Dengan demikian, kepatuhan terhadap UU PDP menjadi prasyarat legal bagi keberlanjutan model bisnis digital.

UU PDP membuka kemungkinan penunjukan Pejabat Perlindungan Data (Data Protection Officer) bagi pengendali data yang melakukan pemrosesan data dalam skala besar atau memproses data spesifik, sebagai bagian dari penguatan tata kelola perlindungan data. Pengaturan ini tidak hanya mencakup penerapan teknologi keamanan informasi seperti enkripsi dan kontrol akses, tetapi juga menempatkan kepatuhan sebagai bagian integral dari tata kelola perusahaan, yang secara operasional menimbulkan konsekuensi biaya tambahan seperti investasi teknologi, audit internal, pelatihan sumber daya manusia, dan pembentukan unit compliance yang fokus pada perlindungan data. Penelitian menunjukkan bahwa tanpa adanya alokasi sumber daya yang memadai, pelaku usaha terutama di sektor E-commerce kesulitan memenuhi kewajiban UU PDP secara optimal (Wiraguna et al., 2024). UU PDP menuntut perubahan serius dalam tata kelola perusahaan. Meski menambah biaya operasional, kewajiban ini merupakan investasi penting untuk menekan risiko hukum, melindungi reputasi, dan membangun kepercayaan konsumen dalam bisnis digital.

Kewajiban tersebut berimplikasi pada perubahan struktur operasional perusahaan, karena unit yang bertanggung jawab atas aspek keamanan dan kepatuhan data perlu berkolaborasi secara intensif dengan divisi lain, seperti teknologi informasi, pemasaran, dan hukum. Kondisi ini berpotensi meningkatkan kompleksitas organisasi sekaligus menuntut keberadaan Pejabat Pelindungan Data (Data Protection Officer) yang memiliki kompetensi komprehensif di bidang regulasi maupun teknologi. Sejumlah analisis juga menunjukkan bahwa penerapan pendekatan keamanan data yang terintegrasi mampu meningkatkan kesiapan organisasi dalam mengantisipasi risiko kebocoran data serta potensi sengketa hukum (Gunawan, 2025). Hal ini menegaskan bahwa integrasi lintas divisi dan peran DPO memang menambah kompleksitas organisasi, tetapi hal itu justru memperkuat tata kelola data. Pendekatan terkoordinasi ini membuat perusahaan lebih siap mencegah kebocoran data dan menghadapi risiko hukum.

Selain itu, potensi penerapan sanksi hukum yang tegas mendorong pelaku usaha untuk lebih cermat dan bertanggung jawab dalam pengelolaan data pribadi. Undang-Undang Perlindungan Data Pribadi (UU PDP) memperkenalkan ancaman sanksi administratif maupun pidana bagi pihak yang melanggar, termasuk kewajiban pelaporan insiden kebocoran data kepada otoritas yang berwenang. Ketentuan tersebut dapat menimbulkan konsekuensi berupa kerugian reputasi perusahaan serta dampak finansial yang tidak kecil. Sejumlah kajian mengenai implementasi perlindungan data pribadi di sektor E-commerce menunjukkan bahwa perusahaan cenderung meningkatkan transparansi kebijakan privasi serta memperkuat mekanisme pelaporan insiden sebagai langkah mitigasi risiko hukum sekaligus upaya membangun dan menjaga kepercayaan konsumen (Wiraguna et al., 2024). Namun demikian, dapat dicermati bahwa perluasan kewajiban

hukum ini juga berpotensi menimbulkan beban kepatuhan yang tidak ringan, terutama bagi pelaku usaha digital berskala kecil dan menengah. Kewajiban dokumentasi, penerapan standar keamanan, dan integrasi prinsip privacy by design memerlukan kapasitas teknis dan finansial yang tidak selalu seimbang di antara pelaku usaha. Oleh karena itu, efektivitas pengaturan UU PDP dalam konteks model bisnis digital tidak hanya bergantung pada norma yang tertulis, tetapi juga pada kebijakan turunan, pedoman teknis, serta pendekatan penegakan hukum yang proporsional dan adaptif terhadap dinamika ekonomi digital.

Dengan demikian, UU PDP tidak semata berfungsi sebagai instrumen pembatas pemrosesan data pribadi, melainkan juga sebagai kerangka regulatif yang membentuk tata kelola bisnis digital yang bertanggung jawab dan berkelanjutan. Pengaturan yang lebih ketat terhadap perlindungan data tidak sekadar mengatur batasan, tetapi juga mendorong inovasi dalam manajemen risiko, pengembangan prosedur kepatuhan, dan peningkatan sistem pengamanan data yang pada akhirnya memberi nilai tambah kompetitif bagi perusahaan yang berhasil mengintegrasikannya ke dalam model bisnis (Taufiq & Kenyo, 2025). Transformasi ini menunjukkan bahwa keberlanjutan ekonomi digital di Indonesia ke depan akan sangat ditentukan oleh kemampuan pelaku usaha dalam mengintegrasikan kepatuhan hukum perlindungan data ke dalam struktur dan strategi bisnisnya.

KESIMPULAN

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa perlindungan data pribadi merupakan bagian dari hak asasi manusia yang memiliki konsekuensi hukum langsung terhadap praktik bisnis digital di Indonesia. Dalam ekosistem ekonomi digital, data pribadi telah berkembang menjadi aset strategis yang mendukung personalisasi layanan, pengembangan produk, serta efektivitas model monetisasi berbasis teknologi. Namun, ketergantungan tinggi terhadap pemrosesan data juga meningkatkan risiko pelanggaran privasi, ketimpangan posisi antara pelaku usaha dan konsumen, serta potensi penyalahgunaan data dalam skala besar. Pengaturan dalam UU PDP menghadirkan perubahan mendasar terhadap model bisnis digital melalui penegasan prinsip legalitas, pembatasan tujuan, transparansi, keamanan, dan akuntabilitas pemrosesan data. Hak subjek data untuk mengakses, memperbaiki, menghapus, serta menolak pemrosesan tertentu memperkuat posisi individu dalam hubungan hukum dengan penyelenggara sistem elektronik. Di sisi lain, pelaku usaha digital dibebani kewajiban hukum yang lebih ketat, termasuk penerapan perlindungan data sejak tahap perancangan sistem, penguatan tata kelola keamanan data, serta kesiapan menghadapi sanksi administratif maupun pidana apabila terjadi pelanggaran. Dengan demikian, kepatuhan terhadap UU PDP tidak lagi dapat dipandang

sebagai kewajiban administratif semata, melainkan sebagai elemen strategis dalam keberlanjutan model bisnis digital. Regulasi ini berfungsi sebagai instrumen penyeimbang antara kepentingan ekonomi berbasis data dan perlindungan hak privasi individu, sekaligus mendorong transformasi tata kelola perusahaan menuju praktik bisnis digital yang lebih etis, transparan, dan bertanggung jawab..

DAFTAR PUSTAKA

Akbar, N., Sitorus, H. K., & Nasution, M. Y. A. P. (2025). Perlindungan Hukum Terhadap Data Diri Konsumen Dalam Transaksi Digital. *Indonesian Journal Of Law*, *2*(1), 12–22.

Cahyadi, N., Junianto, P., Hakim, A. L., Fuadi, F., Nuryanto, U. W., Nalendra, A. K., Pratiwi, I., Prihatin, J., Nababn, H. S., Gunawan, A., & Mahanani, E. (2022). *Bisnis Digital Sebuah Peluang Di Era Digital* (Kodri (ed.); 1st ed.). CV. Adanu Abimata.

Couldry, N., & Mejias, U. A. (2020). The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism. *Stanford University Press*, *99*(1), e6. https://doi.org/https://doi.org/10.1093/sf/soz172

Diah, A. S., & Wiraguna, S. A. (2025). *Tanggung Jawab Hukum Platform E-commerce atas Kebocoran Data Pribadi dalam Tanggung Jawab Hukum Platform E-commerce atas Kebocoran Data dalamPerspektif UU No . 27 Tahun 2022*. *2*(2), 1089–1096. https://doi.org/10.58344/jws.v3i3.584.6

Faisal, M. T., & Fasa, M. I. (2025). Transformasi Digital : Peran *E-commerce* Dalam Pertumbuhan Ekonomi Digital Di Indonesia. *Jurnal Media Akademik (JMA)*, *3*(4). https://doi.org/10.62281

Gunawan, P. W. (2025). Kesadaran Keamanan Data Pribadi : Perbandingan Implementasi UU PDP dan GDPR. *Jurnal Teknik Informatika Unika ST. Thomas (JTIUST)*, *10*(02), 254–258.

Kaharuddin, Fakhirah, N. R., Hisyam, C. M., & Wirasmara, A. P. (2025). Urgensi Penerapan UU PDP Nomor 27 Tahun 2022 dalam Pertanggungjawaban Hukum atas Kasus Kebocoran Data NPWP. *Jurnal Takuana*, *4*(3), 876–887. https://doi.org/10.56113/takuana.v4i3.249

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna *E-commerce* : Ancaman, Risiko, Strategi Keamanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632.

Khairi, M., Rianto, B., & Jalil, M. (2025). Pengaruh Teknologi Dalam Transformasi Ekonomi dan Bisnis di Era Digital. *Jurnal Perangkat Lunak*, *7*, 71–78. https://doi.org/https://doi.org/10.32520/jupel.v7i1.3947

Kurnianingrum, T. P. (2020). Urgensi Perlindungan Data Pribadi Konsumen Di Era Ekonomi Digital. *Jurnal Kajian*, *25*(3), 197–216.

Lesmana, R., & Nasution, M. I. P. (2025). *Kebocoran Data di Media Sosial : Analisis Pola dan Strategi Pencegahannya*. *2*(10), 123–128. https://doi.org/https://doi.org/10.5281/zenodo.15388529 Kebocoran

Ma'sumatul Maghfiroh, F., Natalina, S. A., & Efendi, R. (2023). Transformasi Ekonomi Digital : Connection Integration *E-commerce* Dan S-Commerce Dalam Upaya Perkembangan Ekonomi Berkelanjutan Penyebaran Novel Coronavirus Disease atau biasa disebut Covid-19 telah. *Proceedings Of Islamic Economics, Business, and Philanthropy*, *2*(1).

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Uundan Perlindungan Data Pribadi). *Jurnal Masalah-Masalah Hukum*, *52*(1), 97–106.

Taufiq, M., & Kenyo, A. S. (2025). *The Legal Protection of Personal Data in the Digital Era : A Comparative Study of Indonesian Law and the GDPR*. *6*(2), 1260–1268.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (2022).

Wijayanto, D. D., Indrayanti, K. W., & W, D. A. W. (2025). Personal Data Protection in Digital Business Based on the Law on Personal Data Protection. *International Journal of Research in Social Science and Humanities (IJRSS)*, *6*(8), 6–12. https://doi.org/10.47505/IJRSS.2025.8.2

Wiraguna, S. A., Sulaiman, A., & Barthos, M. (2024). Impelmentation Of Consumer Personal Data Protection In *E-commerce* From The Perspective Of Law No. 27 Of 2022. *Journal Of World Science*, *3*(3), 410–418. https://doi.org/10.58344/jws.v3i3.584