

Perlindungan Hukum Data Pribadi Konsumen E-Commerce Berdasarkan Undang-Undang Perlindungan Data Pribadi

Muhammad Ihya Ulumudin¹, Rosiana Laela Nurul Syahna¹, Intan Nur Kasanah¹, Raihan Abdillah¹

¹ Universitas Pamulang, Indonesia

Received: 17/04/2026

Revised: 26/05/2026

Accepted: 24/06/2026

Abstract

The rapid growth of the digital economy in Indonesia brings significant challenges in the form of personal data breach risks in e-commerce transactions. This study aims to analyze the legal protection framework for consumers and the responsibility of business actors based on Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The research method used is normative juridical with a statutory and conceptual approach. The results show that the PDP Law provides a strong legal foundation through the regulation of data subject rights, data controller obligations, and strict administrative and criminal sanctions. Legal protection is carried out through preventive mechanisms such as explicit consent (informed consent) and repressive measures in the form of compensation lawsuits and sanction enforcement. However, its effectiveness still faces challenges such as low public digital literacy and the technical readiness of electronic system operators.

Keywords

E-commerce; Personal Data; Consumer Protection; PDP Law.

Corresponding Author

Muhammad Ihya Ulumudin

Universitas Pamulang, Indonesia; ulumudinmuhammadihya1@gmail.com

1. PENDAHULUAN

Era globalisasi dan transformasi digital telah mengubah pola konsumsi masyarakat secara fundamental, dari transaksi konvensional yang bersifat tatap muka menuju platform digital atau e-commerce yang serba instan dan lintas batas. Perkembangan ekonomi digital yang masif ini menuntut adanya kedaulatan data dan reorientasi perlindungan hukum bagi konsumen agar tidak menjadi pihak yang dieksploitasi dalam transaksi digital (Fathoni dkk., 2026). Pertumbuhan e-commerce di Indonesia yang mencapai angka signifikan dalam satu dekade terakhir memberikan kemudahan akses belanja bagi masyarakat luas, namun di sisi lain memperbesar kerentanan terhadap penyalahgunaan data pribadi sebagai konsekuensi logis dari masifnya pertukaran informasi digital antara konsumen dan pelaku usaha. Setiap transaksi yang dilakukan melalui platform digital pada dasarnya merupakan pertukaran data, mulai dari identitas diri, nomor kontak, alamat domisili, riwayat pembelian, hingga data finansial yang tersimpan pada sistem elektronik penyelenggara.



Berbagai kasus kebocoran data besar yang menimpa beberapa platform e-commerce di Indonesia telah mengancam privasi jutaan pengguna dan menurunkan kepercayaan publik terhadap ekosistem digital secara keseluruhan. Ketimpangan instrumen kepatuhan antarpelaku usaha turut memperburuk situasi ini, mengingat standarisasi tata kelola pada platform belanja berskala besar masih belum seragam dan acap kali bergantung pada kapasitas teknis serta komitmen internal masing-masing penyelenggara sistem elektronik (Anggriawan dkk., 2023). Kondisi tersebut diperparah oleh sektor penegakan hukum siber yang menghadapi tantangan besar karena maraknya korban kejahatan siber melalui modus operandi yang manipulatif seperti phishing (Wahyuningtias, 2025), serta risiko kebocoran data siber yang sistemik dan terstruktur, yang tidak lagi bersifat insidental melainkan telah menjadi ancaman laten bagi seluruh ekosistem digital nasional (Akbar & Wicaksana, 2025). Tanpa adanya keseragaman tata kelola dan penegakan hukum yang konsisten, upaya mewujudkan ekosistem perlindungan data konsumen yang akuntabel di seluruh sektor digital akan sangat sulit dicapai (Pohan & Nasution, 2023).

Menanggapi fenomena ini, pakar hukum siber Shinta Dewi Rosadi menegaskan bahwa perlindungan data pribadi di era digital bukan lagi sekadar masalah perlindungan privasi individual semata, melainkan telah bergeser menjadi bagian dari Hak Asasi Manusia (HAM) yang wajib dijamin dan dilindungi oleh negara dalam ruang siber tanpa batas (*borderless*). Pemikiran ini relevan mengingat data pribadi pada hakikatnya merupakan perpanjangan dari martabat dan otonomi individu, sehingga setiap bentuk penyalahgunaannya berimplikasi langsung pada perampasan hak-hak dasar warga negara. Secara konstitusional di Indonesia, perlindungan ini merupakan mandat dari Pasal 28G ayat (1) UUD 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk melakukan atau tidak melakukan sesuatu yang merupakan hak asasi.

Sebelum tahun 2022, regulasi mengenai data pribadi tersebar di berbagai peraturan sektoral yang sering kali menimbulkan ketidakharmonisan hukum, baik dari segi terminologi, ruang lingkup, maupun mekanisme penegakannya. Fragmentasi regulasi semacam ini menyebabkan tumpang tindih kewenangan antarlembaga serta menciptakan kekosongan hukum (*rechtsvacuum*) pada aspek-aspek tertentu yang belum terjangkau oleh undang-undang sektoral, sehingga para akademisi melihat adanya urgensi pembaharuan hukum yang responsif karena regulasi lama tidak lagi akomodatif terhadap dinamika risiko digital kontemporer (Sangojoyo dkk., 2022). Urgensi ini diperkuat oleh argumentasi bahwa pendekatan sektoral semata tidak mampu memberikan kepastian hukum yang komprehensif bagi seluruh pemangku kepentingan, sehingga mendesaknya pembentukan undang-undang khusus yang berfungsi sebagai *lex specialis* di bidang perlindungan data pribadi menjadi kebutuhan yang tidak

dapat ditawarkan lagi (Pardede & Rasji, 2022). Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi langkah krusial pemerintah untuk memberikan kepastian hukum yang komprehensif di era ekonomi digital dan memetakan perlindungan hak-hak konstitusional warga negara secara menyeluruh, sekaligus menyelaraskan Indonesia dengan tren global dalam pengaturan data pribadi (Rauf dkk., 2025).

Urgensi regulasi yang komprehensif ini juga tidak dapat dilepaskan dari relasi antara UU PDP dengan instrumen hukum siber lain yang telah ada sebelumnya. Sinergi antara Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dengan UU PDP menjadi kunci dalam membangun kerangka hukum siber yang utuh, di mana UU ITE berfungsi sebagai payung hukum aktivitas siber secara umum, sementara UU PDP hadir sebagai regulasi substansif yang lebih mendalam mengenai privasi data (Gustryan & Hoesein, 2025). Tanpa harmonisasi semacam ini, risiko tumpang tindih norma dan ketidakpastian hukum dalam penanganan kasus-kasus kebocoran data akan tetap menjadi persoalan struktural. Lebih jauh, persoalan kebocoran data pribadi konsumen e-commerce juga memiliki keterkaitan erat dengan kejahatan sekunder di sektor jasa keuangan digital. Kebocoran atau penyalahgunaan data pribadi yang bersumber dari transaksi e-commerce kerap dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan penyalahgunaan data pada layanan pinjaman online ilegal (Lambanon dkk., 2023; Fritiana dkk., 2025), bahkan meluas menjadi pelanggaran hak privasi nasabah dalam ekosistem pinjam-meminjam digital secara umum (Syifa & Adam, 2024). Fenomena rantai kerentanan data semacam ini menunjukkan bahwa lemahnya perlindungan data pada satu sektor dapat menimbulkan efek domino yang merugikan konsumen pada sektor lainnya, sehingga memperkuat urgensi adanya kerangka hukum yang berlaku lintas sektor seperti UU PDP.

Berdasarkan uraian latar belakang tersebut, penelitian ini berupaya menjawab dua permasalahan utama, yaitu: pertama, bagaimana kerangka perlindungan hukum bagi konsumen atas data pribadinya dalam transaksi e-commerce berdasarkan UU PDP; dan kedua, bagaimana bentuk tanggung jawab hukum pelaku usaha e-commerce selaku pengendali data terhadap risiko kebocoran dan penyalahgunaan data pribadi konsumen. Penelitian ini bertujuan untuk menganalisis secara komprehensif kerangka perlindungan hukum tersebut serta mengidentifikasi tantangan implementasinya di lapangan. Nilai kebaruan dari penelitian ini terletak pada upaya mensintesis teori perlindungan hukum klasik dengan perkembangan regulasi siber terbaru, termasuk pasca-perubahan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024, sehingga diharapkan dapat memberikan kontribusi akademik bagi pengembangan hukum perlindungan data pribadi yang adaptif terhadap dinamika ekonomi digital di Indonesia.

2. METODE

Penelitian ini menggunakan jenis penelitian hukum normatif yang berfokus pada kajian terhadap norma-norma hukum positif yang berlaku. Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) untuk menelaah regulasi terkait perlindungan data pribadi secara hierarkis dan sistematis, serta pendekatan konseptual (*conceptual approach*) untuk memahami prinsip-prinsip perlindungan data pribadi melalui pandangan para ahli hukum dan doktrin yang berkembang dalam literatur akademik. Sumber data yang digunakan adalah data sekunder yang terdiri dari bahan hukum primer seperti UUD 1945, UU PDP, UU ITE, dan UU Perlindungan Konsumen, serta bahan hukum sekunder berupa buku, norma hukum, dan jurnal akademik yang relevan dengan tema penelitian. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri dan menginventarisasi bahan-bahan hukum yang relevan, kemudian dianalisis secara kualitatif-deskriptif untuk memberikan gambaran sistematis mengenai permasalahan hukum normatif yang diteliti. Analisis dilakukan dengan menghubungkan norma-norma yang berlaku dengan teori perlindungan hukum, sehingga diperoleh konstruksi argumentasi yuridis yang utuh mengenai kerangka perlindungan data pribadi konsumen dalam transaksi e-commerce.

3. HASIL DAN PEMBAHASAN

A. Klasifikasi dan Dasar Hukum Pemrosesan Data Pribadi Konsumen

Berdasarkan analisis terhadap UU PDP, data pribadi diklasifikasikan menjadi dua jenis: data pribadi bersifat umum (seperti nama lengkap dan jenis kelamin) dan data pribadi bersifat spesifik (seperti data kesehatan, biometrik, dan genetika). Klasifikasi ini penting karena menentukan tingkat kehati-hatian dan mekanisme pengamanan yang harus diterapkan oleh pengendali data, mengingat data pribadi yang bersifat spesifik memerlukan perlindungan yang lebih ketat akibat potensi dampak yang lebih besar apabila terjadi kebocoran. UU PDP menetapkan bahwa pemrosesan data pribadi harus memiliki dasar hukum yang sah, di mana salah satu yang utama adalah persetujuan eksplisit dari subjek data. Perlindungan ini menjadi instrumen esensial dalam transaksi komersial digital (Priliasari, 2023) demi melindungi hak identitas agar tidak disalahgunakan untuk profiling tanpa izin (Kurniastuti & Prastyanti, 2025). Dalam perspektif hukum keperdataan, perlindungan data dalam perjanjian online wajib bersandar pada asas iktikad baik dan keseimbangan para pihak (Azharudin dkk., 2025), sehingga pelaku usaha tidak dapat secara sepihak menentukan klausula pemrosesan data tanpa memperhatikan kepentingan dan hak-hak konsumen sebagai subjek data.

Kebutuhan akan dasar hukum yang jelas ini sesungguhnya merupakan jawaban atas fragmentasi regulasi yang telah berlangsung lama. Sebagaimana telah diuraikan sebelumnya, ketiadaan undang-undang khusus mengenai data pribadi sebelum tahun 2022 menyebabkan ketidakharmonisan hukum

yang signifikan, sehingga urgensi pembaharuan hukum mengenai perlindungan data pribadi e-commerce menjadi sangat mendesak untuk segera direalisasikan (Sangojoyo dkk., 2022). UU PDP pada akhirnya menjawab kebutuhan tersebut dengan menghadirkan norma yang lebih spesifik dan berfungsi sebagai *lex specialis*, sejalan dengan argumentasi mengenai urgensi pembentukan undang-undang khusus perlindungan data pribadi di Indonesia (Pardede & Rasji, 2022). Dengan demikian, dasar pemrosesan data pribadi konsumen kini tidak lagi bertumpu pada interpretasi yang beragam dari berbagai peraturan sektoral, melainkan merujuk pada satu kerangka hukum yang terpadu dan komprehensif.

B. Hak Subjek Data dan Posisi Tawar Konsumen dalam Ekosistem Digital

Konsumen sebagai subjek data diberikan hak-hak yang luas, meliputi hak untuk mendapatkan informasi tujuan pemrosesan, hak mengakses, memperbaiki, menghapus (*right to be forgotten*), hingga hak untuk menarik kembali persetujuan. Terkait hak subjek data ini, Sutan Remy Sjahdeini dalam doktrin hukum konsumennya menyatakan bahwa dalam ekosistem digital, konsumen selalu berada pada posisi tawar (*bargaining position*) yang lemah karena kerap dihadapkan pada skema klausula baku bersyarat (*take-it-or-leave-it*). Doktrin ini menegaskan bahwa ketimpangan struktural antara pelaku usaha yang menguasai teknologi dan informasi dengan konsumen yang berada pada posisi pasif sebagai penerima syarat dan ketentuan menjadikan konsumen rentan terhadap praktik-praktik yang merugikan, terutama dalam hal pemrosesan data pribadi yang dilakukan tanpa pemahaman yang utuh dari pihak konsumen.

Oleh karena itu, kehadiran hak subjek data dalam UU PDP berfungsi sebagai penyeimbang kedudukan hukum tersebut, dengan memberikan instrumen hukum yang dapat digunakan konsumen untuk menuntut transparansi dan akuntabilitas dari pelaku usaha. Melalui pembaruan hukum terkini, termasuk pasca-perubahan regulasi siber dalam UU No. 1 Tahun 2024, posisi tawar konsumen atas kedaulatan data pribadinya dalam transaksi e-commerce menjadi jauh lebih kuat (Putra dkk., 2026). Penguatan posisi tawar ini sejalan dengan temuan mengenai pentingnya perlindungan hukum terhadap data konsumen pada platform marketplace, yang menunjukkan bahwa ketimpangan instrumen kepatuhan antarpelaku usaha masih menjadi tantangan nyata dalam mewujudkan standarisasi tata kelola platform belanja berskala besar (Anggriawan dkk., 2023). Tanpa adanya keseragaman standar kepatuhan, hak-hak subjek data yang secara normatif telah dijamin oleh UU PDP berpotensi tidak terimplementasi secara konsisten pada level praktik, sehingga konsumen pada platform yang berbeda dapat memperoleh tingkat perlindungan yang berbeda pula.

Di sisi lain, pelaku usaha e-commerce sebagai pengendali data wajib menjamin keamanan sistem melalui langkah teknis dan administratif, serta wajib melaporkan adanya kegagalan perlindungan data

dalam waktu maksimal 72 jam. Kewajiban pelaporan yang ketat ini dimaksudkan untuk memberikan kesempatan kepada subjek data melakukan mitigasi risiko sedini mungkin, misalnya dengan mengganti kata sandi atau memantau aktivitas transaksi yang tidak wajar. Penyelesaian sengketa dapat ditempuh melalui jalur litigasi maupun non-litigasi seperti arbitrase atau mediasi, yang bertujuan memberikan perlindungan nyata bagi hak-hak privasi konsumen (Saly dkk., 2023). Ketersediaan jalur penyelesaian sengketa yang beragam ini penting mengingat tidak semua konsumen memiliki kapasitas finansial dan pengetahuan hukum yang memadai untuk menempuh jalur litigasi yang formal dan memakan waktu, sehingga mekanisme non-litigasi seperti mediasi dapat menjadi alternatif yang lebih aksesibel bagi pemulihan hak-hak konsumen yang dirugikan.

C. Tanggung Jawab Pelaku Usaha dan Prinsip Strict Liability

Implementasi UU PDP membawa paradigma baru yang mengedepankan prinsip strict liability bagi platform e-commerce, di mana tanggung jawab hukum melekat tanpa perlu pembuktian unsur kesalahan jika terjadi kegagalan sistem pengamanan. Pergeseran dari prinsip fault-based liability ke strict liability ini merupakan perubahan paradigmatik yang signifikan dalam hukum pertanggungjawaban siber, karena beban pembuktian yang sebelumnya berada pada pihak yang dirugikan (konsumen) kini bergeser kepada pengendali data untuk membuktikan bahwa kegagalan sistem bukan disebabkan oleh kelalaiannya. Menurut pemikiran Jimly Asshiddiqie mengenai penegakan hukum siber, pola pertanggungjawaban hukum di era digital harus bertransformasi dari yang bersifat reaktif-punitif menjadi proaktif-komplementer (proactive compliance). Pemikiran ini relevan karena pendekatan hukum yang semata-mata bersifat reaktif, yaitu baru bertindak setelah terjadi pelanggaran, dinilai tidak lagi memadai untuk mengantisipasi kompleksitas dan kecepatan risiko siber kontemporer.

Pelaku usaha wajib membangun arsitektur sistem yang mengedepankan perlindungan data sejak awal sistem dirancang (privacy by design). Prinsip ini menuntut agar pertimbangan privasi tidak diperlakukan sebagai fitur tambahan yang bersifat opsional, melainkan menjadi bagian integral dari setiap tahap pengembangan sistem elektronik, mulai dari perancangan basis data hingga antarmuka pengguna. Sinergi antara UU ITE dan UU PDP menjadi kunci dalam mendukung implementasi prinsip ini; UU ITE berfungsi sebagai payung hukum aktivitas siber secara umum, sementara UU PDP menjadi regulasi substansif yang mendalam mengenai privasi data (Gustryan & Hoesein, 2025). Tinjauan yuridis terhadap UU PDP 2022 ini sangat krusial dalam memetakan kepatuhan dan menangani potensi kebocoran data pelanggan secara preventif (Arief & Purwanto, 2025), karena pemahaman yang komprehensif terhadap norma yang berlaku merupakan prasyarat bagi pelaku usaha untuk dapat menyusun standar operasional prosedur keamanan data yang sesuai dengan ketentuan hukum.

Perlindungan hukum ini juga harus dimaknai secara kontekstual pada operasional retail modern berbasis digital (Sugita & Sudharma, 2026), mengingat karakteristik transaksi pada sektor retail digital memiliki kekhasan tersendiri dibandingkan sektor lain, terutama terkait volume data yang sangat besar dan frekuensi transaksi yang tinggi. Tanggung jawab pelaku usaha dalam konteks ini juga harus diperluas cakupannya hingga ke pihak ketiga yang mengelola dokumen dan tanda tangan elektronik (Aribowo dkk., 2025), mengingat ekosistem e-commerce modern tidak lagi bersifat tunggal melainkan melibatkan banyak pihak penyedia layanan pendukung, seperti penyedia jasa pembayaran, logistik, dan verifikasi identitas digital, yang masing-masing turut mengelola data pribadi konsumen. Tanpa pengaturan yang jelas mengenai tanggung jawab pihak ketiga ini, celah hukum dapat muncul pada titik-titik penyerahan data antara pelaku usaha utama dan mitra penyedia layanan pendukungnya.

D. Teori Perlindungan Hukum Phillipus M. Hadjon: Bentuk Preventif dan Represif

Jika dibedah menggunakan Teori Perlindungan Hukum dari Phillipus M. Hadjon, instrumen perlindungan konsumen dalam UU PDP dapat diklasifikasikan menjadi dua bentuk, yaitu perlindungan preventif dan perlindungan represif. Kedua bentuk perlindungan ini saling melengkapi dan tidak dapat dipisahkan satu sama lain, karena perlindungan preventif berfungsi untuk mencegah terjadinya pelanggaran sejak awal, sementara perlindungan represif berfungsi sebagai upaya pemulihan dan penjatuhan konsekuensi hukum setelah pelanggaran terjadi.

Perlindungan Preventif diwujudkan melalui kewajiban pengendali data untuk memperoleh persetujuan eksplisit (*informed consent*) serta transparansi pemrosesan data, sebagaimana diatur dalam Pasal 5 sampai Pasal 7 UU PDP. Mekanisme preventif ini menempatkan kontrol pemrosesan data sejak tahap paling awal, yaitu pada momen pemberian persetujuan oleh subjek data, sehingga konsumen memiliki kendali atas keputusan apakah data pribadinya akan diproses oleh pelaku usaha atau tidak. Persoalannya, penerapan persetujuan eksplisit ini dalam praktik tidak selalu berjalan ideal. Pengkajian normatif terhadap kebijakan privasi (*privacy policy*) pada platform belanja digital seperti Tokopedia menunjukkan pentingnya harmonisasi aturan dengan prinsip hak asasi manusia (Fajar & Aji, 2024), yang mengindikasikan bahwa kebijakan privasi yang disusun secara sepihak oleh platform belum tentu sepenuhnya mencerminkan keseimbangan hak antara pelaku usaha dan konsumen. Begitu pula dengan analisis terhadap klausula baku privasi platform Lazada yang menunjukkan bahwa potensi kerentanan hukum di dalamnya berisiko menurunkan tingkat kepercayaan publik secara signifikan (Simarmata dkk., 2024; Al Fahri, 2023). Kerentanan semacam ini umumnya muncul akibat redaksi klausula yang terlalu umum (*general clause*) sehingga memberikan ruang interpretasi yang luas bagi pengendali data dalam memproses data pribadi konsumen melampaui tujuan awal yang disepakati.

Perlindungan Represif diwujudkan melalui penyediaan hak bagi konsumen untuk mengajukan gugatan ganti rugi atas pelanggaran data serta penjatuhan sanksi administratif maupun pidana yang tegas, sebagaimana diatur dalam Pasal 12 dan Bab Sanksi UU PDP. Bentuk perlindungan ini menjadi penting terutama ketika mekanisme preventif gagal mencegah terjadinya kebocoran data, sebagaimana terlihat pada kajian terhadap aplikasi belanja online Shopee yang menunjukkan bahwa kelemahan klausula proteksi berpotensi mengekspos data pribadi konsumen pada risiko eksternal (Dewi, 2026). Dalam situasi semacam ini, ketersediaan sanksi administratif dan pidana yang tegas menjadi instrumen represif yang penting untuk memberikan efek jera (*deterrent effect*) bagi pelaku usaha agar lebih serius dalam menerapkan standar keamanan data, sekaligus memberikan kompensasi yang layak bagi konsumen yang menjadi korban kebocoran data.

E. Problematika Mekanisme Persetujuan Digital (Clickwrap Agreement)

Namun, ditemukan problematika dalam mekanisme persetujuan digital seperti *clickwrap agreement*. Banyak konsumen yang memberikan persetujuan tanpa pemahaman yang memadai karena syarat dan ketentuan yang panjang dan rumit, sehingga pada praktiknya persetujuan tersebut lebih bersifat formalitas administratif daripada cerminan kehendak bebas (*free will*) yang sesungguhnya dari subjek data. Validitas *clickwrap agreement* dalam transaksi e-commerce ini memicu ambiguitas jika diperhadapkan antara kebebasan berkontrak dalam KUHPerdara dan keharusan persetujuan eksplisit dalam UU PDP (Afrilia dkk., 2026). Ambiguitas ini muncul karena asas kebebasan berkontrak secara tradisional mengandaikan adanya kesetaraan kedudukan antarpihak yang berkontrak, sementara dalam relasi konsumen-pelaku usaha digital, kesetaraan semacam itu pada praktiknya jarang terwujud akibat ketimpangan akses informasi dan kapasitas negosiasi, sebagaimana telah diuraikan dalam doktrin posisi tawar lemah konsumen sebelumnya.

Kelemahan ini diperparah oleh penerapan perjanjian standar yang sepihak oleh pelaku usaha, yang kerap mendegradasi posisi tawar konsumen (Ibrahim, 2024). Perjanjian standar atau klausula baku pada dasarnya memberikan efisiensi bagi pelaku usaha dalam menjalankan transaksi massal, namun di sisi lain berpotensi menjadi instrumen yang merugikan konsumen apabila tidak diimbangi dengan pengawasan substantif terhadap materi klausulanya. Dalam konteks ini, asas iktikad baik dan keseimbangan para pihak yang ditegaskan dalam perspektif hukum keperdataan (Azharudin dkk., 2025) menjadi rujukan penting untuk menilai apakah suatu klausula baku dalam *clickwrap agreement* masih berada dalam batas kepatutan hukum atau telah melampaui batas yang merugikan konsumen secara tidak proporsional. Pengadilan dan lembaga pengawas dengan demikian dituntut untuk tidak hanya menilai keabsahan formal persetujuan, tetapi juga substansi dan keseimbangan materi yang terkandung di dalamnya.

F. Tantangan Literasi Digital dan Disparitas Kepatuhan Regulasi

Tantangan lain yang mengemuka adalah rendahnya literasi digital konsumen dan tingkat kepatuhan regulasi oleh pelaku usaha yang bervariasi secara normatif pada tatanan regional (Purnamasari dkk., 2025). Rendahnya literasi digital ini menyebabkan konsumen sering kali tidak menyadari hak-haknya sebagai subjek data, sehingga jarang menggunakan instrumen hukum yang telah disediakan oleh UU PDP, seperti hak untuk mengakses atau menghapus data pribadinya. Ketimpangan instrumen kepatuhan ini sangat riskan terhadap standarisasi tata kelola platform belanja berskala besar (Anggriawan dkk., 2023), karena pelaku usaha besar dengan sumber daya yang memadai cenderung lebih siap menerapkan standar keamanan data dibandingkan pelaku usaha skala kecil dan menengah yang masih terbatas kapasitas teknisnya.

Jika ditinjau dari instrumen norma hukum siber, kelemahan klausula proteksi berpotensi mengekspos data pribadi konsumen pada risiko eksternal (Dewi, 2026). Risiko eksternal ini dapat berupa serangan siber dari pihak ketiga yang memanfaatkan celah keamanan sistem, maupun penyalahgunaan data oleh pihak internal yang memiliki akses terhadap basis data konsumen. Pengkajian normatif terhadap kebijakan privasi (privacy policy) pada platform belanja digital seperti Tokopedia menunjukkan pentingnya harmonisasi aturan dengan prinsip hak asasi manusia (Fajar & Aji, 2024). Begitu pula dengan analisis terhadap klausula baku privasi platform Lazada yang menunjukkan bahwa potensi kerentanan hukum di dalamnya berisiko menurunkan tingkat kepercayaan publik secara signifikan (Simarmata dkk., 2024; Al Fahri, 2023).

Ketika kerangka data pribadi komersial mengalami celah hukum, hal ini kerap berkorelasi normatif dengan tindak kejahatan sekunder di sektor keuangan digital, seperti penyalahgunaan data pada layanan pinjaman online ilegal (Lambanon dkk., 2023; Fritiana dkk., 2025) maupun pelanggaran hak privasi nasabah dalam ekosistem pinjam-meminjam digital secara umum (Syifa & Adam, 2024). Korelasi ini menunjukkan bahwa kebocoran data pada satu platform e-commerce tidak berhenti pada kerugian di platform tersebut saja, melainkan dapat memicu rantai eksploitasi data lanjutan pada sektor lain yang sama sekali tidak memiliki relasi kontraktual langsung dengan konsumen yang bersangkutan. Fenomena ini menegaskan urgensi pengaturan transfer dan pertukaran data pribadi antarpelaku usaha secara lebih ketat, agar data yang telah diberikan konsumen pada satu platform tidak dengan mudah berpindah tangan dan dimanfaatkan oleh pihak lain tanpa persetujuan yang sah.

Ketika kerangka data pribadi komersial mengalami celah hukum, hal ini kerap berkorelasi normatif dengan tindak kejahatan sekunder di sektor keuangan digital, seperti penyalahgunaan data pada layanan pinjaman online ilegal (Lambanon dkk., 2023; Fritiana dkk., 2025) maupun pelanggaran hak privasi nasabah dalam ekosistem pinjam-meminjam digital secara umum (Syifa & Adam, 2024). Korelasi ini menunjukkan bahwa kebocoran data pada satu platform e-commerce tidak berhenti pada

kerugian di platform tersebut saja, melainkan dapat memicu rantai eksploitasi data lanjutan pada sektor lain yang sama sekali tidak memiliki relasi kontraktual langsung dengan konsumen yang bersangkutan. Fenomena ini menegaskan urgensi pengaturan transfer dan pertukaran data pribadi antarpelaku usaha secara lebih ketat, agar data yang telah diberikan konsumen pada satu platform tidak dengan mudah berpindah tangan dan dimanfaatkan oleh pihak lain tanpa persetujuan yang sah.

G. Urgensi Lembaga Pengawas dan Penguatan Tata Kelola Data

Oleh karena itu, penegakan hukum yang konsisten dan akuntabel mutlak diperlukan demi mewujudkan tata kelola perlindungan data konsumen yang seragam di seluruh ekosistem digital (Pohan & Nasution, 2023). Keberadaan lembaga pengawas independen sebagaimana diamanatkan UU PDP menjadi sangat mendesak untuk segera dibentuk guna menjalankan fungsi pengawasan dan penindakan yang efektif. Lembaga pengawas semacam ini idealnya memiliki kewenangan yang memadai untuk melakukan investigasi, menjatuhkan sanksi administratif, serta mengeluarkan panduan teknis yang mengikat bagi seluruh penyelenggara sistem elektronik, sehingga kepatuhan terhadap UU PDP tidak lagi bergantung sepenuhnya pada kesadaran sukarela pelaku usaha.

Penguatan regulasi, khususnya kepastian hukum dalam klausul transfer data dan penjatuhan sanksi seperti yang diatur dalam Pasal 56 UU PDP, harus dikawal ketat agar tidak menimbulkan celah hukum baru (Aulia, 2024). Kepastian hukum dalam klausul transfer data menjadi sangat penting mengingat praktik bisnis digital modern sering kali melibatkan pemindahan data lintas yurisdiksi, baik antarperusahaan dalam satu grup usaha maupun kepada mitra penyedia layanan di luar negeri, sehingga tanpa pengaturan yang jelas, perlindungan data pribadi konsumen Indonesia dapat melemah ketika datanya diproses di luar wilayah hukum nasional. Analisis yuridis normatif yang tajam terhadap sinkronisasi aturan sektoral dan UU PDP dipandang krusial demi membangun iklim e-commerce yang sehat, aman, dan terpercaya (Mubarok & Febriadi, 2026). Sinkronisasi ini penting agar tidak terjadi kontradiksi norma antara UU PDP dengan peraturan sektoral lain, seperti peraturan di bidang perbankan, telekomunikasi, maupun perlindungan konsumen, yang masing-masing memuat ketentuan tersendiri mengenai pengelolaan data nasabah atau pelanggannya.

Dengan terbentuknya lembaga pengawas yang kuat serta sinkronisasi regulasi yang baik, diharapkan tata kelola data pribadi konsumen e-commerce di Indonesia dapat bertransformasi dari pendekatan yang bersifat parsial dan reaktif menuju pendekatan yang terintegrasi dan proaktif, sejalan dengan paradigma proactive compliance yang telah diuraikan sebelumnya. Hal ini pada akhirnya akan memperkuat kepercayaan publik terhadap ekosistem digital secara keseluruhan, yang menjadi prasyarat fundamental bagi keberlanjutan pertumbuhan ekonomi digital Indonesia di masa mendatang.

4. KESIMPULAN

Perlindungan hukum terhadap data pribadi konsumen e-commerce di Indonesia kini telah memiliki landasan normatif yang kuat pasca berlakunya UU PDP Tahun 2022. Perlindungan ini mencakup aspek preventif melalui kewajiban persetujuan eksplisit dan transparansi klausula, sebagaimana ditegaskan dalam Teori Perlindungan Hukum Phillipus M. Hadjon, serta aspek represif melalui sanksi administratif, perdata, hingga penegakan sanksi pidana bagi pelanggar. Hak-hak subjek data yang luas turut memperkuat posisi tawar konsumen yang sebelumnya lemah dalam relasi kontraktual dengan pelaku usaha digital, sementara prinsip strict liability dan privacy by design mendorong pelaku usaha untuk bertransformasi dari pendekatan reaktif-punitif menjadi proaktif-komplementer dalam menjaga keamanan data.

Meski demikian, efektivitas UU PDP masih menghadapi sejumlah tantangan struktural, antara lain ambiguitas validitas clickwrap agreement, rendahnya literasi digital masyarakat, disparitas kepatuhan regulasi antarpelaku usaha, serta korelasi kebocoran data dengan kejahatan sekunder di sektor keuangan digital. Untuk mewujudkan ekosistem ekonomi digital yang aman secara holistik, diperlukan penguatan koordinasi antarlembaga, segera dibentuknya lembaga pengawas independen yang berwenang penuh, peningkatan literasi digital hukum bagi masyarakat, serta komitmen proaktif dari pelaku usaha untuk merevisi kebijakan privasi mereka agar selaras dengan standar akuntabilitas UU PDP. Penelitian lebih lanjut disarankan untuk mengkaji secara empiris efektivitas penegakan sanksi UU PDP pada platform-platform e-commerce skala kecil dan menengah, mengingat kapasitas kepatuhan pada segmen tersebut relatif berbeda dengan platform skala besar yang telah menjadi fokus sebagian besar kajian terdahulu.

REFERENSI

- Afrilia, E. T., dkk. (2026). Validitas Clickwrap Agreement dalam Transaksi E-Commerce Menurut KUHPperdata dan UU PDP. Al-Zayn.
- Akbar, H., & Wicaksana, P. B. (2025). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Akibat Tindak Pidana Siber. Jurnal Serambi Hukum.
- Al Fahri, S. M. (2023). Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce (Studi Kasus Lazada). Skripsi UIN Jakarta.
- Anggriawan, Z., dkk. (2023). Analisis Perlindungan Hukum terhadap Data Konsumen Marketplace di Indonesia. Jurnal Humaniorum.
- Arief, L. S., & Purwanto, R. (2025). Tinjauan Yuridis UU PDP Tahun 2022 dalam Menangani Kebocoran Data Pelanggan E-Commerce. Pemuliaan Keadilan.
- Aribowo, Y., dkk. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan

- Elektronik oleh Pihak Ketiga. Cendekia.
- Aulia, E. (2024). Analisis Pasal 56 UU PDP dari Perspektif Kepastian Hukum. *Unes Law Review*.
- Azharudin, F., dkk. (2025). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Perjanjian Online Perspektif Hukum Perdata. *Prosiding Nasional*.
- Dewi, K. V. A. (2026). Perlindungan Hukum terhadap Data Pribadi dalam Penggunaan Aplikasi Belanja Online (Shopee). Aliansi.
- Fajar, A. R., & Aji, M. P. (2024). Analisis Kebijakan UU PDP Sebagai Pemenuhan HAM: Studi Kasus Tokopedia. *Jipolis*.
- Fathoni, L. A., dkk. (2026). Perlindungan Hukum bagi Konsumen dalam Menghadapi Perkembangan Ekonomi Digital. *Fundamental Justice*.
- Fritiana, A., dkk. (2025). Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online. *Al-Zayn*.
- Gustryan, M., & Hoesein, Z. A. (2025). Peran Undang-Undang ITE dan UU PDP dalam Perlindungan Data dan Privasi. *Jurnal Minfo Polgan*.
- Ibrahim, A. (2024). Perlindungan Hukum Konsumen Terhadap Perjanjian Standar Dalam Transaksi Jual Beli Melalui E-Commerce. *JIEMAS*.
- Kurniastuti, D. F., & Prastyanti, R. A. (2025). Perlindungan Data Identitas Konsumen Dalam Transaksi E-Commerce. *Hukum Dinamika Ekselensia*.
- Lambanon, J. E., dkk. (2023). Kajian Yuridis Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online. *Innovative*.
- Mubarok, M. A., & Febriadi, H. (2026). Perlindungan Hukum Konsumen Dalam Transaksi E-Commerce Di Indonesia Tahun 2025. *PESHUM*.
- Pardede, D. E. P., & Rasji. (2022). Urgensi Pembentukan UU Khusus Perlindungan Data Pribadi di Indonesia. *Jurnal Hukum Adigama*.
- Pohan, T. D., & Nasution, M. I. P. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E-Commerce. *Sammajiva*.
- Prihasari, E. (2023). Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce menurut Peraturan Perundang-undangan di Indonesia. *Jurnal Rechts Vinding*.
- Purnamasari, P., dkk. (2025). Perlindungan Hukum Data Pribadi Konsumen dalam Transaksi E-commerce di Bekasi. *Sabajaya*.
- Putra, F. J., dkk. (2026). Perlindungan Konsumen Atas Data Pribadi Dalam Transaksi E-Commerce Pasca UU No. 1 Tahun 2024. *Jurnal Jurisprudentialia*.
- Rauf, A., dkk. (2025). Pelindungan Hukum Terhadap Data Pribadi Di Indonesia. *Prosiding Seminar Ilmiah*.
- Saly, J. N., dkk. (2023). Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022. *Jurnal Serina*

Sosial Humaniora.

Sangojoyo, B. F., dkk. (2022). Urgensi Pembaharuan Hukum mengenai Perlindungan Data Pribadi E-Commerce. Kosmik Hukum.

Simarmata, R., dkk. (2024). Perlindungan Data Pribadi Konsumen Lazada Dalam Transaksi E-Commerce. Palasrev.

Sugita, I M., & Sudharma, I M. (2026). Perlindungan Hukum Terhadap Data Pribadi Konsumen dalam E-Commerce. Jurnal Hukum Hindu.

Syifa, A. R., & Adam, R. C. (2024). Perlindungan Data Pribadi Nasabah Peminjam dalam Layanan Pinjam Meminjam. Unes Law Review.

Wahyuningtias, N. A. (2025). Analisis Normatif Perlindungan Hukum Terhadap Korban Kejahatan Siber Dalam Modus Phishing. Judge: Jurnal Hukum.

