PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN DALAM TRANSAKSI *E-COMMERCE* DI INDONESIA

Velita Date Rugi[1], Adji Darmo[2], Yulita Yulia Rua[3], Roni Rustandi[4]
[123] PPKN, FKIP, Universitas Pamulang
rugivelitadate@gmail.com , adjidarmo824@mail.com, ruajulita@gmail.com , dosen02176@unpam.ac.id

ABSTRACT

The enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) marks a new chapter in data governance in Indonesia, particularly within the rapidly expanding electronic commerce ecosystem. This study aims to analyze the legal framework for the protection of consumers' personal data in e-commerce transactions following the enforcement of the PDP Law, as well as to identify normative gaps that may undermine the effectiveness of such protection. This research employs a normative legal research method with a statute approach and a conceptual approach, utilizing primary legal materials in the form of relevant legislation and secondary legal materials comprising scholarly literature, legal doctrine, and pertinent judicial decisions. The findings reveal that the PDP Law has established a more comprehensive legal foundation than its predecessor regulations, particularly through the codification of the consent principle, data subject rights, and obligations incumbent upon data controllers; nevertheless, several normative disharmonies were identified between the PDP Law and Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions, as well as Law Number 8 of 1999 on Consumer Protection, with the absence of a functionally operational independent supervisory body during the transitional period constituting a structural impediment to legal enforcement. This study concludes that cross-sectoral regulatory harmonization and the establishment of an effective data protection authority are indispensable prerequisites for the substantive realization of consumer personal data protection in Indonesia's e-commerce transactions.

Keywords*: Stock Prices. Personal Data Protection; E-Commerce; PDP Law; Digital Consumer; Regulatory Harmonization*

ABSTRAK.

Pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai babak baru dalam tata kelola data di Indonesia, khususnya dalam ekosistem perdagangan elektronik yang terus berkembang pesat.

Penelitian ini bertujuan untuk menganalisis kerangka hukum perlindungan data pribadi konsumen dalam transaksi e-commerce pascaberlakunya UU PDP, serta mengidentifikasi celah normatif yang berpotensi melemahkan efektivitas perlindungan tersebut. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*), dengan bahan hukum primer berupa peraturan perundang-undangan terkait serta bahan hukum sekunder berupa literatur, doktrin, dan putusan yang relevan. Hasil penelitian menunjukkan bahwa UU PDP telah memberikan landasan hukum yang lebih komprehensif dibandingkan regulasi sebelumnya, khususnya melalui pengaturan prinsip persetujuan (*consent*), hak-hak subjek data, dan kewajiban pengendali data; namun demikian, ditemukan sejumlah disharmoni normatif antara UU PDP dengan Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, di samping ketiadaan lembaga pengawas independen yang fungsional selama masa transisi sebagai hambatan struktural dalam penegakan hukum. Penelitian ini menyimpulkan bahwa harmonisasi regulasi lintas sektoral dan pembentukan otoritas perlindungan data yang efektif merupakan prasyarat utama bagi terwujudnya perlindungan data pribadi konsumen yang substansial dalam transaksi e-commerce di Indonesia.

Kata Kunci: Perlindungan Data Pribadi; E-Commerce; Undang-Undang PDP; Konsumen Digital; Harmonisasi Regulasi

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi selama satu dekade terakhir telah mendorong transformasi fundamental dalam perilaku ekonomi masyarakat Indonesia, khususnya dalam hal pola konsumsi yang bergeser dari transaksi konvensional menuju perdagangan berbasis platform digital atau *electronic commerce* (e-commerce). Fenomena ini tidak bersifat gradual, melainkan terjadi secara akseleratif, terutama sejak pandemi Covid-19 pada 2020 yang memaksa masyarakat beralih ke kanal digital sebagai satu-satunya alternatif berbelanja. Nilai transaksi e-commerce di Indonesia selalu meningkat sejak 2017, dan lonjakan tertinggi terjadi pada 2021 ketika nilai transaksi mencapai Rp401 triliun, kemudian naik menjadi Rp476 triliun pada 2022. Meskipun sempat mengalami penurunan 4,7% secara tahunan menjadi Rp454 triliun pada 2023, transaksi kembali menguat sebesar 7,3% menjadi Rp487 triliun

pada 2024 (Mandiri Institute, 2025: 12). Dari sisi pengguna, jumlah pengguna e-commerce bertambah sebesar 69% selama lima tahun terakhir, dari 38 juta pengguna pada 2020 menjadi 65 juta pada 2024, dan diproyeksikan terus meningkat hingga mencapai 99 juta pengguna pada 2029 (Badan Pusat Statistik, 2024: 7). Angka-angka tersebut menempatkan Indonesia sebagai pasar e-commerce terbesar di kawasan Asia Tenggara dengan nilai penjualan neto (*net merchandise value*) sebesar US$64 miliar atau setara 42,6% dari total nilai penjualan di ASEAN (Cube Asia, 2024: 3), sekaligus mengisyaratkan besarnya volume data pribadi konsumen yang mengalir dan tersimpan dalam ekosistem digital setiap harinya.

Dalam setiap transaksi e-commerce, konsumen diwajibkan menyerahkan sejumlah data pribadi mulai dari nama lengkap, alamat, nomor telepon, informasi instrumen pembayaran, hingga riwayat pembelian sebagai prasyarat fungsional layanan. Data-data tersebut diproses, disimpan, dan sering kali dibagikan kepada pihak ketiga, baik mitra logistik, agregator pembayaran, maupun penyedia layanan iklan, tanpa pemahaman penuh dari konsumen mengenai lingkup pemanfaatannya (Rosadi & Pratama, 2020: 149). Kondisi asimetri informasi antara platform dan konsumen inilah yang menjadikan ekosistem e-commerce sebagai salah satu titik paling rentan terhadap ancaman kebocoran, penyalahgunaan, dan perdagangan ilegal data pribadi. Lebih dari 2,3 miliar data pribadi yang diduga milik warga negara Indonesia telah beredar di berbagai forum gelap (*dark web*) selama tiga tahun terakhir, sebagaimana dilaporkan dalam Indonesian Cyber Security Forum 2024 (Kompas, 2025: 1).

Deretan insiden kebocoran data di Indonesia mencerminkan betapa seriusnya ancaman tersebut secara empiris. Pada 2020, sebanyak 91 juta data pribadi pengguna Tokopedia bocor dan diperdagangkan di forum gelap, mencakup nama lengkap, alamat email, serta kata sandi pengguna (IDN Times, 2024: 1). Pada 2021, kebocoran data menimpa 279 juta peserta BPJS Kesehatan, mencakup NIK, alamat, nomor telepon, hingga riwayat penyakit yang kemudian diperjualbelikan di forum *dark web* (GoodStats, 2024: 1).

Memasuki 2023, sekitar 409 juta data bocor dari berbagai layanan termasuk platform e-commerce besar, dan data dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) pada Januari 2024 mengindikasikan bahwa sedikitnya 668 juta rekam data pribadi bocor dari enam platform digital besar, mencakup NIK, nomor kartu keluarga, riwayat transaksi, hingga data biometrik (Kompas, 2025: 1). Secara keseluruhan, Kementerian Komunikasi dan Informatika menangani 124 kasus dugaan pelanggaran perlindungan data pribadi sepanjang 2019 hingga Mei 2024, dan 111 di antaranya dikategorikan sebagai kasus kebocoran data (Kompas.id, 2024: 1). Puncak dari rangkaian insiden ini terjadi pada Juni 2024, ketika serangan *ransomware Brain Cipher* melumpuhkan Pusat Data Nasional Sementara (PDNS), mengunci data di 282 kementerian dan lembaga, dengan pelaku meminta tebusan sebesar US$8 juta atau setara Rp121,4 miliar (IDN Times, 2024: 1). Rentetan kasus tersebut secara tegas menunjukkan bahwa kerentanan terhadap kebocoran data bukan semata persoalan teknis keamanan siber, melainkan juga cerminan dari kelemahan struktural dalam tata kelola hukum perlindungan data pribadi di Indonesia.

Merespons urgensi tersebut, Indonesia akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada 17 Oktober 2022, yang kemudian berlaku penuh pada 17 Oktober 2024 setelah masa transisi dua tahun. UU PDP hadir sebagai regulasi *lex specialis* yang pertama kali mengatur secara komprehensif hak-hak subjek data, kewajiban pengendali dan prosesor data, klasifikasi data pribadi umum dan sensitif, serta mekanisme sanksi administratif dan pidana bagi pelanggarnya (Fadhli & Shalihah, 2021: 82). Kehadiran undang-undang ini merupakan respons normatif terhadap ketidakmemadaian kerangka hukum sebelumnya yang tersebar dalam berbagai peraturan sektoral, yakni Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), yang terbukti tidak memadai dalam mengakomodasi kompleksitas

perlindungan data di era ekonomi digital (Riswandi & Astuti, 2022: 38). Namun demikian, ketiadaan lembaga pengawas independen yang fungsional sebagaimana diamanatkan UU PDP telah menciptakan kekosongan hukum dalam pemrosesan data sensitif, sehingga masyarakat tidak memiliki mekanisme pengaduan yang jelas ketika terjadi pelanggaran data pribadi (Arifiyadi & Latifah, 2024: 60).

Berbagai penelitian terdahulu telah mencoba mengkaji problematika perlindungan data pribadi dalam konteks e-commerce di Indonesia, namun masing-masing masih menyisakan celah (*research gap*) yang belum terjawab secara tuntas. Rosadi dan Pratama (2020) menyimpulkan bahwa Indonesia belum memiliki regulasi perlindungan data yang komprehensif dan merekomendasikan pembentukan undang-undang khusus, namun kajian tersebut berhenti pada tataran urgensi normatif tanpa memeriksa efektivitas implementasinya. Fadhli dan Shalihah (2021) mengkonstruksi perlindungan data pribadi sebagai derivasi hak asasi manusia atas privasi dalam perdagangan online, tetapi belum mengintegrasikan analisis terhadap mekanisme penegakan hukum yang konkret dalam ekosistem e-commerce. Riswandi dan Astuti (2022) merekomendasikan adopsi prinsip-prinsip *General Data Protection Regulation* (GDPR) Uni Eropa ke dalam sistem hukum Indonesia dengan menekankan pentingnya prinsip *consent* dan *data minimization*, namun penelitian tersebut bersifat komparatif dan belum menyentuh realitas implementasi pasca berlakunya UU PDP. Rani dan Widodo (2023) mengidentifikasi potensi perlindungan yang ditawarkan UU PDP bagi konsumen e-commerce secara umum, tetapi tidak memeriksa disharmoni normatif antar-regulasi terkait yang justru menjadi hambatan utama penegakan hukum. Terakhir, Arifiyadi dan Latifah (2024) mengkritisi tidak terbentuknya lembaga pengawas independen dan kelemahan sanksi administratif, namun tidak menganalisis korelasinya secara spesifik dengan sektor e-commerce dan hak-hak konsumen digital. Dengan demikian, belum ada kajian yang secara simultan membahas efektivitas norma UU PDP dalam melindungi data pribadi konsumen e-commerce, disharmoni antara UU PDP dengan regulasi

perlindungan konsumen dan transaksi elektronik yang berlaku, serta implikasi kekosongan kelembagaan pengawas terhadap penegakan hak-hak konsumen digital. Celah inilah yang menjadi *raison d'être* penelitian ini.

Berdasarkan uraian latar belakang di atas, penelitian ini merumuskan dua permasalahan hukum pokok sebagai berikut: pertama, bagaimana kerangka normatif Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan hukum terhadap data pribadi konsumen dalam transaksi e-commerce di Indonesia; dan kedua, apakah terdapat disharmoni normatif antara UU PDP dengan regulasi terkait lainnya dan bagaimana implikasinya terhadap efektivitas perlindungan konsumen digital. Sehubungan dengan rumusan masalah tersebut, penelitian ini bertujuan untuk menganalisis dan mendeskripsikan kerangka perlindungan hukum data pribadi konsumen dalam transaksi e-commerce berdasarkan UU PDP beserta regulasi turunannya, sekaligus mengidentifikasi dan mengkritisi disharmoni normatif yang ada serta merumuskan rekomendasi normatif bagi penguatan perlindungan data pribadi konsumen e-commerce di Indonesia secara komprehensif dan sistematis.

B. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*), yakni penelitian yang mengkaji hukum sebagai norma, asas, doktrin, dan sistem peraturan perundang-undangan yang berlaku, bukan sebagai gejala sosial empiris. Pilihan terhadap jenis penelitian ini didasarkan pada karakteristik permasalahan yang diteliti, yaitu pengkajian kerangka normatif perlindungan data pribadi konsumen dalam transaksi e-commerce serta identifikasi disharmoni antar-regulasi yang bersifat doktrinal. Sebagaimana dikemukakan oleh Marzuki (2021: 35), penelitian hukum normatif pada hakikatnya merupakan proses menemukan aturan hukum, prinsip hukum, maupun doktrin hukum guna menjawab isu hukum yang dihadapi.

Penelitian ini menggunakan dua pendekatan secara simultan. Pertama, pendekatan perundang-undangan (*statute approach*), yaitu pendekatan yang dilakukan dengan

menelaah seluruh peraturan perundang-undangan yang bersangkut paut dengan isu hukum yang dikaji (Marzuki, 2021: 133). Pendekatan ini diterapkan dengan mengkaji secara mendalam substansi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta regulasi turunan dan peraturan pelaksana yang relevan. Melalui pendekatan ini, peneliti dapat memeriksa konsistensi norma, mengidentifikasi celah regulasi, serta menganalisis relasi hierarkis antar-peraturan perundang-undangan yang mengatur perlindungan data pribadi konsumen dalam transaksi elektronik. Kedua, pendekatan konseptual (*conceptual approach*), yaitu pendekatan yang beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum guna membangun argumentasi hukum dalam memecahkan isu yang dihadapi (Marzuki, 2021: 178). Pendekatan ini digunakan untuk mengkaji konsep-konsep fundamental seperti perlindungan hukum, privasi, data pribadi, hak subjek data, dan tanggung jawab pengendali data, sebagaimana dikonstruksikan dalam doktrin hukum nasional maupun komparatif, termasuk merujuk pada kerangka konseptual *General Data Protection Regulation* (GDPR) Uni Eropa sebagai instrumen perbandingan.

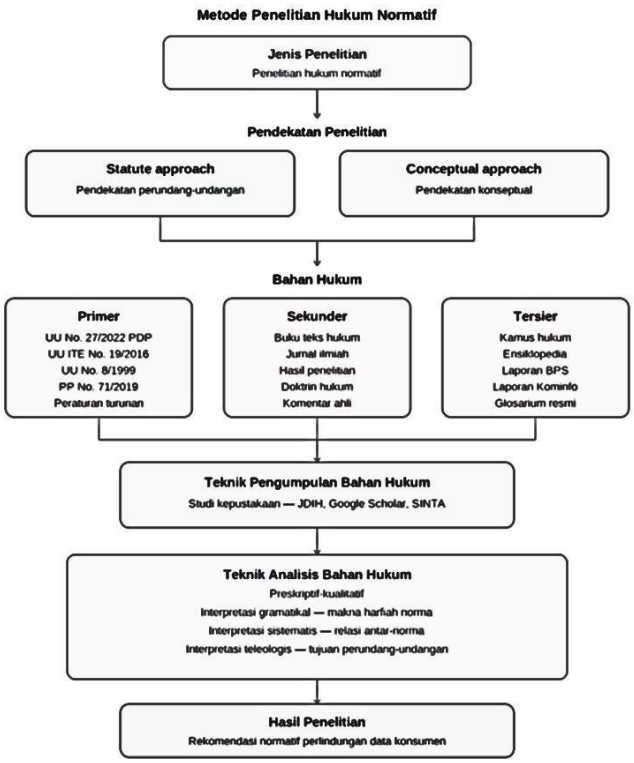
Bahan hukum dalam penelitian ini diklasifikasikan ke dalam tiga kategori. Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif dan mengikat, mencakup seluruh peraturan perundang-undangan yang relevan dengan objek penelitian, meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta berbagai peraturan menteri dan regulasi teknis yang berkaitan. Bahan hukum

sekunder merupakan bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, mencakup literatur ilmiah berupa buku-buku teks hukum, jurnal hukum nasional dan internasional terakreditasi, hasil penelitian terdahulu, makalah ilmiah, serta komentar para ahli hukum yang relevan dengan topik perlindungan data pribadi dan hukum e-commerce. Bahan hukum tersier berfungsi sebagai pelengkap yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, mencakup kamus hukum, ensiklopedia hukum, glosarium resmi lembaga negara, serta laporan institusional dari Badan Pusat Statistik, Kementerian Komunikasi dan Informatika, dan lembaga riset yang kredibel.

Teknik pengumpulan bahan hukum yang digunakan adalah studi kepustakaan (*library research*), yaitu dengan menginventarisasi, mengklasifikasikan, dan mengkaji seluruh bahan hukum yang relevan secara sistematis. Bahan hukum primer ditelusuri melalui basis data resmi peraturan perundang-undangan seperti jaringan dokumentasi dan informasi hukum (JDIH), sementara bahan hukum sekunder diperoleh melalui penelusuran pangkalan data jurnal nasional dan internasional, termasuk Google Scholar, SINTA, dan portal jurnal hukum bereputasi lainnya.

Teknik analisis bahan hukum yang digunakan adalah analisis preskriptif-kualitatif. Bahan-bahan hukum yang telah dikumpulkan dianalisis secara mendalam dengan menggunakan metode interpretasi hukum, meliputi interpretasi gramatikal untuk memahami makna harfiah norma, interpretasi sistematis untuk memahami relasi antar-norma dalam satu kesatuan sistem hukum, serta interpretasi teleologis untuk menelaah tujuan diundangkannya suatu peraturan dalam konteks perlindungan konsumen digital. Hasil analisis kemudian disajikan secara deskriptif-preskriptif, yakni tidak sekadar menggambarkan kondisi normatif yang ada, melainkan juga memberikan penilaian ilmiah dan rekomendasi hukum yang konstruktif guna menjawab permasalahan penelitian secara komprehensif.

Gambar 1 Bagan Metode Penelitian



C. Hasil Penelitian dan Pembahasan.

Perlindungan hukum terhadap data pribadi konsumen dalam transaksi e-commerce tidak dapat dilepaskan dari konstruksi teoritis yang melatarbelakangi urgensi pengaturannya. Philipus M. Hadjon (1987: 29) membedakan perlindungan hukum ke dalam dua bentuk, yakni perlindungan hukum preventif yang bertujuan mencegah terjadinya sengketa, dan perlindungan hukum represif yang berfungsi menyelesaikan sengketa setelah pelanggaran terjadi. Dalam konteks data pribadi konsumen e-commerce, kedua bentuk perlindungan ini idealnya bekerja secara simultan: norma-norma preventif mengatur standar pengumpulan, pemrosesan, dan penyimpanan data, sementara norma-norma represif menyediakan mekanisme pemulihan bagi konsumen yang dirugikan akibat kebocoran atau penyalahgunaan datanya. Persoalannya, sebagaimana akan diuraikan dalam subbab ini, kerangka regulasi yang ada di Indonesia masih memperlihatkan ketidakseimbangan antara keduanya, dengan perlindungan preventif yang belum sepenuhnya operasional dan perlindungan represif yang minim instrumen pemulihan efektif bagi konsumen.

1. Konstruksi Konsep Data Pribadi dalam Kerangka Hukum Indonesia

Sebelum menganalisis pengaturannya, perlu dipahami terlebih dahulu bagaimana hukum Indonesia mengkonstruksi konsep data pribadi itu sendiri. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi

lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik" (Pasal 1 angka 1 UU PDP). Definisi ini mengadopsi pendekatan fungsional yang berkembang dalam literatur hukum internasional, di mana identifikabilitas bukan sekadar jenis datam enjadi kriteria penentu apakah suatu informasi termasuk dalam cakupan perlindungan (Kuner, 2020: 47). Pendekatan ini secara teoritis lebih adaptif terhadap perkembangan teknologi, karena data yang semula tampak anonim dapat menjadi data pribadi ketika dikombinasikan dengan data lain melalui teknik *re-identification* yang kian canggih (Ohm, 2010: 1701).

UU PDP selanjutnya membedakan data pribadi menjadi dua kategori: data pribadi umum dan data pribadi sensitif. Data pribadi sensitif mencakup data kesehatan, data biometrik, data genetika, kehidupan seksual, pandangan politik, keyakinan agama, dan data keuangan (Pasal 4 ayat 2 UU PDP). Pembedaan ini penting secara praktis dalam konteks e-commerce, karena platform digital dewasa ini tidak lagi sekadar mengumpulkan nama dan alamat konsumen, melainkan juga data biometrik untuk verifikasi identitas, data kesehatan dalam layanan asuransi berbasis platform, serta data keuangan yang terintegrasi dalam dompet digital. Dengan demikian, mayoritas data yang diproses oleh platform e-commerce kontemporer sesungguhnya masuk dalam kategori sensitif yang membutuhkan standar perlindungan lebih tinggi, namun kenyataannya banyak platform belum menerapkan prosedur yang berbeda antara keduanya (Rani & Widodo, 2023: 208).

2. Hak-Hak Subjek Data dan Kewajiban Pengendali Data dalam Transaksi E-Commerce

UU PDP mengakui delapan hak fundamental subjek data yang merupakan inti dari kerangka perlindungan data pribadi, mencakup hak untuk mendapatkan informasi, hak mengakses data, hak memperbaiki data yang tidak akurat, hak menghapus data (*right to erasure*), hak menarik persetujuan, hak mengajukan keberatan, hak menuntut ganti rugi, serta hak atas portabilitas data (Pasal 5 hingga Pasal 13 UU PDP). Secara normatif, rangkaian hak ini merepresentasikan pendekatan *rights-based* yang selaras dengan prinsip-prinsip yang

dikembangkan dalam *General Data Protection Regulation* (GDPR) Uni Eropa maupun *APEC Privacy Framework*. Akan tetapi, pengakuan hak secara normatif saja tidaklah cukup. Sebagaimana ditekankan oleh Bygrave (2020: 198), efektivitas hak-hak subjek data sangat bergantung pada tersedianya mekanisme pelaksanaan yang mudah diakses, prosedur pengaduan yang tidak memberatkan, serta lembaga pengawas yang responsif dan independen.

Dalam konteks transaksi e-commerce, hak atas *right to erasure* dan hak menarik persetujuan memiliki implikasi teknis yang kompleks. Ketika konsumen meminta penghapusan datanya dari platform, platform tidak hanya wajib menghapus data dari server utamanya, tetapi juga dari seluruh sistem *backup*, basis data mitra pihak ketiga, dan sistem analitik terintegrasi yang mungkin telah memproses data tersebut jauh sebelum permintaan penghapusan diajukan. UU PDP mengatur kewajiban penghapusan ini dalam Pasal 10, namun tidak memberikan petunjuk teknis mengenai standar penghapusan yang memenuhi syarat, batas waktu pelaksanaan yang terukur, maupun mekanisme verifikasi bahwa penghapusan telah benar-benar dilakukan secara menyeluruh. Kekosongan teknis ini membuka celah bagi platform untuk mengklaim telah memenuhi kewajiban penghapusan padahal data masih tersimpan dalam sistem tersier yang tidak termonitor (Mahesa & Wulandari, 2023: 91).

Di sisi pengendali data, UU PDP mewajibkan setiap penyelenggara sistem elektronik yang memproses data pribadi untuk mematuhi serangkaian kewajiban, meliputi: menetapkan dasar pemrosesan yang sah, menerapkan langkah-langkah keamanan teknis dan organisasional yang memadai, menunjuk petugas perlindungan data (*data protection officer*) bagi pengendali yang memproses data dalam skala tertentu, serta menyusun dan memublikasikan kebijakan privasi yang mudah dipahami (Pasal 20 hingga Pasal 35 UU PDP). Kewajiban-kewajiban ini pada dasarnya mengadopsi prinsip *accountability* yang menjadi tulang punggung GDPR. Namun, berbeda dengan GDPR yang secara eksplisit mewajibkan *Data Protection Impact Assessment* (DPIA) untuk pemrosesan berisiko tinggi, UU PDP

tidak mengatur secara tegas kewajiban serupa, padahal dalam ekosistem e-commerce yang melibatkan pemrosesan data dalam skala masif, penilaian risiko semacam itu sangat krusial untuk mencegah pelanggaran sebelum terjadi (Riswandi & Astuti, 2022: 45).

3. Kerangka Regulasi Transaksi Elektronik dan Relasi Normatifnya dengan UU PDP

Sebelum UU PDP hadir, perlindungan data pribadi konsumen dalam transaksi e-commerce bertumpu pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). UU ITE hanya mengatur perlindungan data pribadi secara fragmentaris dalam Pasal 26, yang menyatakan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Ketentuan ini terlalu sederhana untuk mengakomodasi kompleksitas pemrosesan data dalam ekosistem e-commerce modern yang melibatkan rantai panjang pihak ketiga, algoritma pemrosesan otomatis, dan transfer data lintas yurisdiksi (Fadhli & Shalihah, 2021: 85).

PP PSTE memberikan elaborasi yang lebih rinci melalui Pasal 14 hingga Pasal 17 yang mengatur kewajiban penyelenggara sistem elektronik untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi. Namun demikian, PP PSTE memiliki kelemahan mendasar dalam hal sanksi: pelanggaran atas kewajiban perlindungan data hanya diancam dengan sanksi administratif berupa teguran tertulis, denda, penghentian sementara, atau pemutusan akses, tanpa mekanisme pemulihan kerugian yang berpihak pada konsumen (Pasal 100 PP PSTE). Absennya hak gugat perdata yang tegas bagi konsumen dalam PP PSTE menjadikan regulasi ini lebih berfungsi sebagai instrumen pengawasan administratif ketimbang instrumen perlindungan konsumen yang substantif.

Hadirnya UU PDP seharusnya menjadi titik konvergensi yang menyelesaikan fragmentasi regulasi ini. Akan tetapi, alih-alih menyederhanakan kerangka hukum

yang ada, kehadiran UU PDP justru menambah lapisan regulasi baru tanpa secara tegas mencabut atau mengharmonisasi ketentuan-ketentuan lama yang tumpang tindih. Pasal 26 UU ITE misalnya, masih berlaku dan mengatur persetujuan penggunaan data pribadi, sementara UU PDP mengatur hal serupa dengan standar yang berbeda namun tanpa klausul *lex posterior* yang jelas mengenai hubungan antara keduanya. Kondisi ini menciptakan ambiguitas normatif yang dalam praktiknya merugikan konsumen, karena pelaku usaha dapat memilih regulasi mana yang lebih menguntungkan posisi mereka dalam menghadapi gugatan pelanggaran data (Arifiyadi & Latifah, 2024: 64).

4. Kewajiban Pelaku Usaha E-Commerce sebagai Pengendali dan Prosesor Data

Dalam ekosistem e-commerce, struktur pemrosesan data pribadi konsumen umumnya melibatkan setidaknya tiga pihak: platform e-commerce sebagai pengendali data utama (*data controller*), mitra pihak ketiga seperti penyedia layanan logistik, *payment gateway*, dan penyedia iklan sebagai prosesor data (*data processor*), serta sub-prosesor yang bekerja dalam rantai layanan yang lebih panjang. UU PDP membedakan tanggung jawab antara pengendali dan prosesor data dalam Pasal 36 hingga Pasal 45, dengan menegaskan bahwa pengendali data bertanggung jawab atas kepatuhan pemrosesan secara keseluruhan, termasuk memastikan bahwa prosesor yang ditunjuknya juga mematuhi standar perlindungan yang sama.

Konstruksi tanggung jawab ini secara teoritis sudah tepat, namun lemah dalam implementasinya. Persoalan mendasar terletak pada fakta bahwa dalam ekosistem platform digital, batas antara pengendali dan prosesor data sering kali kabur. Platform e-commerce seperti Tokopedia atau Shopee secara bersamaan bertindak sebagai pengendali data terhadap konsumen akhir, tetapi juga sebagai prosesor data bagi para penjual yang menggunakan platformnya. Ambiguitas peran ini tidak diantisipasi secara memadai dalam UU PDP, padahal implikasinya terhadap rantai tanggung jawab hukum sangat signifikan (Kuner, 2020: 53). Ketika terjadi kebocoran data yang melibatkan pihak ketiga misalnya

mitra logistik yang sistem keamanannya lemah konsumen tidak memiliki jalur hukum yang jelas untuk meminta pertanggungjawaban, karena UU PDP tidak secara eksplisit mengatur mekanisme tanggung jawab bersama (*joint liability*) antara pengendali dan prosesor dalam konteks sengketa konsumen.

Lebih jauh, kewajiban pengendali data untuk melaksanakan *privacy by design* dan *privacy by default* yang secara implisit terkandung dalam prinsip-prinsip UU PDP belum diterjemahkan ke dalam standar teknis yang terukur dan dapat diaudit. Berbeda dengan GDPR yang telah dilengkapi dengan berbagai panduan teknis dari *European Data Protection Board* (EDPB), UU PDP belum memiliki padanan regulasi teknis yang memandu pelaku usaha e-commerce dalam mengimplementasikan kewajiban perlindungan data secara konkret (Rosadi & Pratama, 2020: 158). Ketiadaan panduan teknis ini pada gilirannya menciptakan kesenjangan kepatuhan yang lebar antara platform besar yang memiliki sumber daya untuk membangun sistem keamanan data yang canggih dan platform UMKM yang tidak memiliki kapasitas serupa, padahal keduanya menghadapi kewajiban normatif yang sama di bawah UU PDP.

Berdasarkan uraian di atas, dapat disimpulkan bahwa kerangka pengaturan perlindungan data pribadi konsumen dalam transaksi e-commerce di Indonesia pasca berlakunya UU PDP telah mengalami kemajuan normatif yang signifikan dibandingkan dengan rezim regulasi sebelumnya. Pengakuan terhadap hak-hak subjek data, pembedaan antara data umum dan sensitif, serta penetapan kewajiban pengendali dan prosesor data mencerminkan upaya serius pembentuk undang-undang untuk menghadirkan standar perlindungan yang lebih komprehensif. Akan tetapi, kemajuan normatif ini belum diikuti oleh infrastruktur implementasi yang memadai: panduan teknis yang operasional, harmonisasi regulasi lintas sektoral yang tuntas, dan mekanisme pemulihan konsumen yang efektif masih menjadi pekerjaan rumah besar yang harus diselesaikan agar UU PDP dapat benar-benar berfungsi sebagai instrumen perlindungan konsumen digital yang substansial, bukan sekadar dokumen normatif yang indah di atas kertas.

D. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat ditarik dua simpulan pokok yang menjawab rumusan masalah penelitian ini secara langsung.

Pertama, kerangka normatif Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan hukum yang secara substansial lebih komprehensif dibandingkan rezim regulasi sebelumnya dalam melindungi data pribadi konsumen pada transaksi e-commerce. Pengakuan terhadap delapan hak subjek data, pembedaan antara data pribadi umum dan sensitif, penetapan prinsip pemrosesan yang sah, serta konstruksi tanggung jawab pengendali dan prosesor data merupakan kemajuan normatif yang signifikan. Akan tetapi, kemajuan tersebut masih bersifat parsial karena tidak disertai panduan teknis yang operasional, tidak ditopang oleh lembaga pengawas independen yang fungsional, dan tidak dilengkapi mekanisme pemulihan kerugian konsumen yang efektif. Akibatnya, hak-hak subjek data yang secara normatif diakui oleh UU PDP belum dapat dinikmati secara nyata oleh konsumen e-commerce dalam kehidupan sehari-hari, sehingga undang-undang ini masih lebih berfungsi sebagai pernyataan kebijakan daripada instrumen perlindungan yang operatif.

Kedua, terdapat disharmoni normatif yang nyata antara UU PDP dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Disharmoni tersebut bermanifestasi dalam tumpang tindih pengaturan persetujuan penggunaan data, perbedaan standar kewajiban pelaku usaha, serta ketiadaan klausul koordinasi yang jelas di antara ketiga regulasi tersebut. Kondisi ini tidak hanya menciptakan ketidakpastian hukum bagi pelaku usaha, tetapi secara struktural melemahkan posisi konsumen yang seharusnya menjadi pihak yang paling dilindungi dalam ekosistem e-commerce.

Bertolak dari dua simpulan di atas, penelitian ini merekomendasikan dua hal. Secara akademis, diperlukan kajian lebih lanjut mengenai model kelembagaan otoritas perlindungan data yang paling sesuai dengan

sistem hukum dan kapasitas institusional Indonesia, dengan merujuk pada pengalaman komparatif negara-negara yang telah berhasil mengoperasionalkan lembaga serupa. Secara praktis, pembentuk undang-undang perlu segera menyelesaikan tiga agenda regulasi yang mendesak: pertama, menerbitkan peraturan pemerintah turunan UU PDP yang memuat standar teknis pemrosesan data dalam sektor e-commerce secara spesifik; kedua, melakukan harmonisasi menyeluruh antara UU PDP, UU ITE, dan UUPK melalui mekanisme omnibus regulasi sektoral; dan ketiga, membentuk lembaga pengawas perlindungan data pribadi yang independen, memiliki kewenangan investigasi yang memadai, dan dilengkapi kapasitas penegakan sanksi yang proporsional. Tanpa ketiga agenda tersebut, UU PDP akan terus menjadi regulasi yang kuat secara normatif namun lemah secara implementatif, dan konsumen e-commerce Indonesia akan terus menanggung risiko penyalahgunaan data pribadinya tanpa jaminan pemulihan yang memadai.

DAFTAR PUSTAKA.

Arouri, M. E. H., & Fouquau, J. (2009). On the short-term influence of oil price changes on stock markets in GCC countries: linear and nonlinear analyses.

Arifiyadi, T., & Latifah, N. A. (2024). Problematika penegakan hukum perlindungan data pribadi di Indonesia pascaberlakunya UU PDP. *Jurnal Legislasi Indonesia, 21*(1), 55-72.

Badan Pusat Statistik. (2024). *Statistik e-commerce 2024*. Badan Pusat Statistik Republik Indonesia.

Badan Siber dan Sandi Negara. (2024). *Laporan keamanan siber nasional 2024*. BSSN.

Bygrave, L. A. (2020). *Data privacy law: An international perspective*. Oxford University Press.

CNN Indonesia. (2023, 31 Desember). *Daftar dugaan kebocoran data 2023, termasuk data pemilih dan bank*. CNN Indonesia.

Cube Asia. (2024). *Southeast Asia e-commerce report 2024: Net merchandise value analysis*. Cube Asia Research.

European Data Protection Board. (2023). *Guidelines on data protection impact assessment (DPIA)*. EDPB.

Fadhli, Y. Z., & Shalihah, F. (2021). Perlindungan hukum data pribadi sebagai bagian dari hak asasi manusia atas privasi dalam perdagangan online.

Jurnal Hukum Ius Quia Iustum, 28(1), 78-99.

Friedman, L. M. (2021). *The legal system: A social science perspective*. Russell Sage Foundation.

GoodStats. (2024, 2 Juli). *300 juta data pribadi tersebar, kapan Indonesia merdeka dari serangan siber?* GoodStats.

GoodStats. (2025, 29 Maret). *Nilai transaksi e-commerce Indonesia capai Rp487 triliun pada 2024*. GoodStats.

Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat Indonesia*. Bina Ilmu.

IDN Times. (2024, 24 September). *Kasus kebocoran data pribadi di era Presiden Jokowi*. IDN Times.

Indonesian Cyber Security Forum. (2024). *Laporan tahunan keamanan siber Indonesia 2024*. ICSF.

Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

Indonesia. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Katadata. (2023, 31 Juli). *Data pribadi terserak, nasib sial masyarakat hadapi kebocoran data*. Katadata.co.id.

Kementerian Komunikasi dan Informatika. (2024). *Laporan penanganan kasus kebocoran data pribadi 2019–2024*. Kemenkominfo.

Kementerian Perdagangan Republik Indonesia. (2025). *Kinerja perdagangan melalui sistem elektronik 2024–2025*. Badan Kajian dan Pengembangan Perdagangan Kemendag.

Kompas.id. (2024, 3 Juni). *Kemenkominfo tangani 111 kasus kebocoran data pribadi pada 2019–14 Mei 2024*. Kompas.id.

Kompas.id. (2025, 29 November). *Kebocoran data pribadi terus mengancam, lembaga pengawas tak kunjung dibentuk*. Kompas.id.

Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.

Kuner, C. (2020). International governance of data protection: Convergence and divergence in global frameworks. *International Data Privacy Law, 10*(3), 208-224.

LBS Urun Dana. (2025, 27 Februari). *Orang Indonesia doyan belanja online, transaksinya tembus triliunan*. LBS Urun Dana.

Lembaga Studi dan Advokasi Masyarakat. (2024). *Laporan kebocoran data pribadi platform digital di Indonesia*. ELSAM.

Mahesa, R., & Wulandari, T. (2023). Implementasi perlindungan data pribadi dalam platform e-commerce pasca UU PDP. *Jurnal Hukum dan Teknologi, 4*(2), 82-98.

Mandiri Institute. (2025). *Cashing in on the digital boom: E-commerce transaction report March 2025*. Bank Mandiri.

Marzuki, P. M. (2021). *Penelitian hukum* (Edisi Revisi). Kencana Prenada Media Group.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*(6), 1701-1777.

Rani, M., & Widodo, R. B. (2023). Perlindungan konsumen dalam transaksi e-commerce: Analisis terhadap Undang-Undang Nomor 27 Tahun 2022. *Jurnal Hukum dan Pembangunan, 53*(2), 201-220.

Riswandi, B. A., & Astuti, S. R. D. (2022). Kebijakan hukum perlindungan data pribadi di era ekonomi digital: Studi perbandingan Indonesia dan Uni Eropa. *Jurnal Dinamika Hukum, 22*(1), 35-54.

Rosadi, S. D., & Pratama, G. G. (2020). Protecting privacy of personal data in the digital economic era: The urgency of establishing legal framework. *Padjadjaran Journal of Law, 7*(2), 147-165.

Solove, D. J. (2022). *The digital person: Technology and privacy in the information age*. New York University Press.

Solove, D. J. (2022). The myth of the privacy paradox. *George Washington Law Review, 89*(1), 1-51.