



Department of Digital Business

**Journal of Artificial Intelligence and Digital Business (RIGGS)**

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 17884-17892

P-ISSN: 2963-9298, e-ISSN: 2963-914X

---

## Tantangan Hukum pada Bisnis *E-Commerce* dalam Memastikan Keamanan Data dan Privasi Pelanggan

Urbanisasi, Eugene Rangga Novandria

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Tarumanagara

[urban528@gmail.com](mailto:urban528@gmail.com), [eugenedria10@gmail.com](mailto:eugenedria10@gmail.com)

### Abstrak

*The rapid expansion of e-commerce in Indonesia has transformed consumer transactions while creating increasingly complex legal risks concerning data security and customer privacy. This study analyzes the legal challenges faced by e-commerce businesses in protecting personal data, maintaining the confidentiality and integrity of digital information, and ensuring accountability when data breaches or misuse occur. A normative juridical method is employed through an examination of statutory regulations, legal principles, and relevant literature, particularly the Personal Data Protection Law, the Electronic Information and Transactions Law, and regulations governing electronic systems and consumer protection. The analysis focuses on platform compliance, consent and transparency, third-party data processing, cybersecurity governance, cross-border data transfers, consumer complaint mechanisms, and the use of artificial intelligence and behavioral profiling. The findings indicate that Indonesia has developed a relatively comprehensive legal framework, but its implementation remains constrained by uneven business compliance, limited supervisory capacity, overlapping sectoral rules, inadequate incident reporting, and low consumer digital literacy. Small and medium-sized digital businesses also face difficulties in translating legal obligations into practical security procedures. Effective protection therefore requires harmonized regulations, stronger institutional supervision, clear allocation of responsibility among platform operators and business partners, privacy-by-design practices, regular security audits, and accessible dispute-resolution mechanisms. These measures are essential to strengthen consumer trust and support a secure, fair, and sustainable e-commerce ecosystem.*

**Keywords:** E-Commerce, Data Security, Consumer Privacy, Personal Data Protection, Digital Law, ITE Law, E-Commerce Regulations.

### 1. Latar Belakang

Perkembangan teknologi digital telah mendorong pertumbuhan pesat bisnis e-commerce di Indonesia. Perubahan ini terlihat dari meningkatnya aktivitas jual beli melalui platform digital yang memberikan kemudahan, kecepatan, dan efisiensi baik bagi konsumen maupun pelaku usaha. Namun, pertumbuhan ini tidak hanya membawa keuntungan ekonomi, tetapi juga menghadapi tantangan serius dalam aspek hukum, terutama yang berkaitan dengan perlindungan data pribadi dan keamanan informasi pelanggan. Di zaman di mana data menjadi aset penting dalam bisnis digital, setiap transaksi elektronik dapat berisiko mengakibatkan kebocoran data, penyalahgunaan identitas, dan penipuan siber.

Di Indonesia, regulasi yang terkait dengan perlindungan data pribadi masih dalam proses memperkuat. Meskipun Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP) telah disahkan, bersama dengan aturan dalam UU ITE dan peraturan yang terkait, penerapan regulasi tersebut sering kali belum berjalan dengan baik. Banyak platform e-commerce yang belum sepenuhnya menerapkan standar keamanan data yang memadai, baik dari aspek teknologi, kebijakan internal maupun manajemen risiko. Ketidakmampuan pelaku usaha untuk memenuhi kewajiban hukum, seperti pemberitahuan atas kebocoran data, izin pemrosesan data, dan prosedur penghapusan data, semakin meningkatkan risiko pelanggaran privasi konsumen.

Selain itu, tantangan hukum dalam e-commerce juga muncul karena inovasi digital yang berjalan cepat dan seringkali melampaui kemampuan regulator untuk beradaptasi. Model bisnis baru seperti marketplace internasional, social commerce, dan penerapan big data atau kecerdasan buatan dalam menyesuaikan layanan menciptakan dinamika hukum yang rumit. Hal ini menjadikan adanya jurang antara praktik bisnis digital dan

peraturan yang berlaku, sehingga menciptakan ketidakpastian hukum bagi konsumen dan pelaku usaha. Kurangnya pengawasan dan sedikitnya mekanisme penegakan hukum juga menyebabkan banyak kasus kebocoran data yang tidak tertangani dengan baik.

Di sisi lain, rendahnya tingkat literasi digital di kalangan masyarakat Indonesia juga meningkatkan risiko pelanggaran privasi. Banyak konsumen yang tidak menyadari bagaimana data pribadi mereka digunakan, disimpan, atau dibagikan oleh platform e-commerce. Kesadaran yang rendah tentang keamanan akun dan perlindungan data pribadi membuat mereka menjadi sasaran mudah bagi kejahatan siber. Oleh karena itu, dibutuhkan kerjasama antara pemerintah, pelaku usaha e-commerce, dan masyarakat untuk memperkuat keamanan data dan memastikan perlindungan privasi konsumen dalam ekosistem perdagangan digital yang terus tumbuh. Penelitian ini bertujuan untuk menggali secara mendalam tantangan hukum yang muncul dan solusi yang diperlukan untuk menciptakan e-commerce yang aman dan adil.

## **2. Metode Penelitian**

Penelitian ini menggunakan metode yuridis normatif, yang fokus pada analisis terhadap peraturan perundang-undangan yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta peraturan yang berhubungan dengan perdagangan elektronik dan keamanan sistem elektronik. Sumber data yang digunakan adalah data sekunder, yang meliputi sumber hukum primer (UU, PP, Peraturan Menteri), sumber hukum sekunder (buku, jurnal, artikel ilmiah), dan sumber hukum tertier (kamus, ensiklopedia, dan rujukan pendukung). Pengumpulan data dilakukan lewat studi pustaka untuk menemukan dan menganalisis norma hukum yang mengatur tanggung jawab pelaku e-commerce dalam menjaga keamanan data dan privasi konsumen.

Analisis terhadap sumber hukum dilakukan secara kualitatif normatif, yaitu metode yang memproses informasi secara deskriptif, terstruktur, dan beralasan berdasarkan prinsip hukum, teori perlindungan data pribadi, serta prinsip-prinsip keamanan informasi. Metode ini memungkinkan peneliti untuk mengevaluasi sejauh mana praktik yang dilakukan oleh pelaku e-commerce sesuai dengan ketentuan hukum yang ada, sekaligus mengidentifikasi tantangan dalam aspek normatif maupun implementatif dalam penegakan perlindungan data dan privasi konsumen. Dengan demikian, metode penelitian ini memberikan gambaran menyeluruh tentang efektivitas regulasi serta kebutuhan untuk melakukan perbaikan hukum di masa depan.

## **3. Hasil dan Diskusi**

Perkembangan sektor e-commerce di Indonesia mengalami pertumbuhan yang sangat cepat, seiring dengan digitalisasi dan penyebaran internet yang semakin luas. Namun, penelitian menunjukkan bahwa kecepatan pertumbuhan ini tidak didukung dengan sistem perlindungan data yang memadai, baik dari aspek peraturan maupun pelaksanaan teknis oleh pelaku bisnis. Dalam hal peraturan, Indonesia memiliki kerangka hukum formal yang cukup menyeluruh, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai peraturan turunan lainnya. Meskipun demikian, masih ada celah normatif dan penerapan yang menghalangi efektivitas perlindungan keamanan data dan privasi konsumen. Hasil utama penelitian ini mengindikasikan adanya perbedaan signifikan antara regulasi hukum yang telah disusun dan praktik keamanan data yang dijalankan oleh platform e-commerce.

Pertama, dari perspektif kepatuhan para pelaku e-commerce terhadap standar keamanan data, penelitian ini menunjukkan bahwa banyak penyelenggara sistem elektronik belum menerapkan mekanisme perlindungan yang memadai. Ini terlihat dari masih seringnya terjadi insiden kebocoran data pribadi, seperti informasi identitas, alamat, nomor telepon, hingga rincian transaksi pelanggan. Kebocoran data ini sering kali disebabkan oleh lemahnya sistem enkripsi, infrastruktur keamanan jaringan yang tidak terbaru, dan minimnya audit rutin terhadap sistem keamanan. Selain itu, pelaku usaha seringkali tidak memiliki kebijakan internal yang ketat dalam mengatur akses data oleh karyawan maupun pihak ketiga. Situasi ini menunjukkan bahwa penguatan aspek teknis keamanan informasi belum menjadi prioritas utama dalam strategi pengelolaan risiko oleh banyak perusahaan di sektor e-commerce.

Selain masalah teknis, ada pula isu dalam hal tata kelola. Banyak platform yang tidak memiliki sistem jelas terkait cara pengumpulan, pengolahan, penyimpanan, dan pembagian data pelanggan. Hasil penelitian menunjukkan bahwa banyak konsumen tidak mendapatkan penjelasan yang cukup mengenai tujuan pengumpulan data dan cara

penggunaan data tersebut oleh platform atau mitra bisnis mereka. Ketidakjelasan ini tidak hanya berpotensi menimbulkan pelanggaran privasi, tetapi juga mengurangi tingkat kepercayaan konsumen terhadap keamanan informasi pribadi mereka. Di sisi lain, pengawasan internal dari pelaku usaha terhadap pihak ketiga, seperti penyedia layanan pembayaran, jasa logistik, dan penyedia iklan, masih kurang kuat. Padahal, hubungan bisnis dengan pihak ketiga bisa membuka akses lebih luas terhadap data pribadi pelanggan.

Selain itu, dalam aspek penegakan hukum, penelitian ini menunjukkan bahwa mekanisme pengawasan terhadap pelaku e-commerce belum berjalan dengan baik. Meskipun Undang-Undang Perlindungan Data Pribadi telah menetapkan kewajiban pelaku usaha dalam melindungi data pribadi, implementasinya menghadapi kendala akibat kurangnya kapasitas pada lembaga pengawas. Pengawasan siber membutuhkan teknologi canggih dan sumber daya manusia yang memadai, namun kenyataannya lembaga pengawas masih terbatas dalam hal kemampuan teknis dan jumlah personel. Akibatnya, banyak insiden kebocoran data tidak diatasi dengan serius, bahkan sebagian tidak dilaporkan kepada publik maupun otoritas yang berwenang. Pelaku e-commerce sering kali menyimpan informasi mengenai insiden keamanan untuk melindungi reputasi bisnis mereka, sehingga konsumen tidak mendapatkan informasi yang cukup untuk melindungi diri dari risiko lanjutan seperti penyalahgunaan data oleh pihak lain.

Penelitian ini menemukan adanya ketidakjelasan dalam pembagian tanggung jawab hukum dalam ekosistem e-commerce. Dalam rantai bisnis digital, terdapat berbagai pihak seperti penyelenggara marketplace, penyedia jasa pembayaran, perusahaan pengiriman, serta pihak ketiga yang terlibat dalam periklanan atau analisis data. Namun, regulasi yang ada saat ini belum mengatur dengan jelas mengenai batas tanggung jawab tiap pihak jika terjadi pelanggaran data pribadi. Hal ini mengakibatkan tumpang tindih kewajiban hukum yang menyulitkan konsumen saat mengajukan tuntutan ganti rugi. Banyak kasus kebocoran data yang tidak menemukan penyelesaian yang baik karena sulitnya menentukan siapa yang bertanggung jawab atas kelalaian dalam menjaga data pribadi. Ketidakpastian dalam hukum ini mengurangi efektivitas perlindungan privasi yang seharusnya dijamin oleh peraturan yang berlaku.

Ketiga, temuan penelitian menunjukkan bahwa masyarakat yang menggunakan e-commerce masih memiliki tingkat pemahaman digital yang rendah, terutama dalam mengetahui hak-hak mereka berkaitan dengan data pribadi. Sebagian besar konsumen cenderung memberikan persetujuan secara otomatis tanpa membaca syarat privasi yang disediakan oleh platform. Selain itu, masih banyak konsumen yang belum paham cara mengatur perlindungan privasi pada akun mereka, seperti penerapan autentikasi dua faktor, manajemen akses aplikasi, atau pembaruan kata sandi secara berkala. Situasi ini membuat konsumen menjadi salah satu faktor yang melemahkan sistem perlindungan data pribadi secara keseluruhan. Tanpa partisipasi aktif dari pengguna, usaha hukum untuk menjaga privasi menjadi kurang efektif meskipun regulasinya sudah cukup baik.

Keempat, penelitian ini mengungkapkan perlunya keselarasan kebijakan antara berbagai lembaga pemerintah serta di antara peraturan yang ada. Meskipun UU PDP telah berfungsi sebagai kerangka hukum utama untuk pengelolaan data pribadi, berbagai peraturan sekunder dari sektor lain seperti keuangan, komunikasi, dan perdagangan tetap memiliki standar yang bervariasi. Ketidakcocokan ini dapat menyebabkan kebingungan bagi pelaku e-commerce dalam menerapkan standar keamanan yang sesuai. Di samping itu, juga diperlukan panduan operasional yang lebih teknis dan spesifik agar para pelaku usaha dapat lebih memahami langkah-langkah yang perlu dilakukan untuk memastikan kepatuhan terhadap hukum. Tanpa adanya standar keamanan yang konsisten, pelaksanaan perlindungan data pribadi sulit mencapai hasil yang optimal.

Kelima, hasil diskusi dalam penelitian ini menunjukkan bahwa tanggung jawab dan keterbukaan pelaku usaha harus menjadi fokus utama dalam membangun lingkungan e-commerce yang aman. Pelaku e-commerce perlu memberikan informasi yang rinci dan mudah dipahami oleh konsumen berkaitan dengan pengelolaan data pribadi. Laporan mengenai insiden kebocoran data seharusnya dikomunikasikan dengan jelas dan segera, sehingga konsumen dapat mengambil langkah pencegahan. Di sisi lain, pelaku usaha juga harus mengadopsi prinsip privasi sejak awal dalam setiap pengembangan sistem dan fitur baru, agar aspek perlindungan data sudah diperhitungkan dari tahap awal.

Secara keseluruhan, hasil dan analisis dari penelitian ini menunjukkan bahwa isu hukum dalam menjamin keamanan data dan privasi konsumen dalam bisnis e-commerce bersifat kompleks. Masalah ini tidak hanya berkaitan dengan aspek regulasi, tetapi juga meliputi penerapan teknis, budaya kepatuhan pelaku usaha, kapasitas pengawasan pemerintah, serta tingkat pemahaman digital di kalangan konsumen. Untuk menciptakan lingkungan e-commerce yang lebih aman dan terpercaya, diperlukan kerja sama antara pemerintah, pelaku usaha, dan

masyarakat. Penguatan regulasi, peningkatan penegakan hukum, pendidikan publik, dan komitmen teknologi dari pelaku usaha merupakan kunci dalam menghadapi tantangan ini secara berkelanjutan.

Selain temuan yang telah disebutkan, penelitian ini juga menekankan bahwa tantangan hukum yang dihadapi oleh sektor e-commerce tidak hanya berkaitan dengan perlindungan data pribadi, tetapi juga dengan perkembangan teknologi yang sangat pesat. Munculnya teknologi analisis big data, kecerdasan buatan, dan pembelajaran mesin semakin memperluas cara penggunaan data pribadi oleh para pelaku usaha. Sebagai contoh, banyak platform e-commerce yang memanfaatkan data perilaku pelanggan untuk meramalkan kebutuhan, mengatur tampilan produk, serta menetapkan harga secara dinamis. Kegiatan ini masih berada dalam area yang tidak jelas secara hukum, karena belum ada aturan yang mengatur secara mendetail dalam UU PDP. Di sisi lain, penerapan teknologi ini tanpa pengawasan yang baik menimbulkan risiko pelanggaran privasi dan potensi penyalahgunaan data pelanggan. Hasil penelitian ini mengisyaratkan bahwa kemajuan teknologi digital perlu diimbangi dengan regulasi yang fleksibel dan responsif agar perlindungan data pribadi bisa tetap terjaga dengan baik.

Penelitian juga mengindikasikan bahwa sebagian besar pelaku e-commerce kecil dan menengah belum sepenuhnya memahami kewajiban hukum yang berkaitan dengan perlindungan data pribadi. Kurangnya pemahaman ini sering kali mengarah pada pelanggaran yang tidak disengaja, seperti penyimpanan data pelanggan tanpa enkripsi atau pembagian data dengan pihak ketiga tanpa landasan hukum yang jelas. Situasi ini menggarisbawahi perlunya peningkatan pembinaan dan sosialisasi dari pemerintah. Pelaku UMKM digital, yang merupakan pilar ekonomi Indonesia, memerlukan dukungan berupa pedoman yang sederhana dan mudah untuk dipraktikkan demi memastikan mereka mematuhi ketentuan hukum. Tanpa adanya upaya pembinaan yang luas, potensi pelanggaran hukum akan terus tinggi meskipun regulasi sudah diterapkan dengan lengkap.

Selain itu, penelitian menunjukkan bahwa secara umum konsumen tidak memiliki saluran pengaduan yang memadai saat privasi mereka dilanggar oleh platform e-commerce. Beberapa platform masih belum menyediakan mekanisme pengaduan yang khusus untuk pelanggaran privasi, atau jika sudah ada, respons yang diberikan sering kali tidak memadai. Konsumen yang mengalami kebocoran data kerap kali merasa bingung dalam menentukan langkah hukum yang harus dilakukan dan sering kali merasa putus asa karena proses penyelesaian sengketa yang rumit dan memakan waktu. Hal ini menunjukkan bahwa perlindungan hukum terhadap privasi konsumen tidak hanya bergantung pada regulasi formal, tetapi juga pada adanya mekanisme penyelesaian sengketa yang efektif dan berfokus pada perlindungan konsumen.

Dalam diskusi yang lebih luas, penelitian menunjukkan bahwa perlindungan data pribadi dalam e-commerce harus dipandang sebagai bagian dari budaya hukum di masyarakat digital. Ini berarti keberhasilan perlindungan data tidak hanya ditentukan oleh hukum dan lembaga penegak hukum, tetapi juga oleh kepatuhan sosial dari semua pihak yang terlibat. Jika masyarakat tidak memiliki pemahaman yang tinggi mengenai pentingnya melindungi data pribadi dan pelaku bisnis hanya menganggap perlindungan data sebagai kewajiban administratif saja, maka perlindungan data tidak akan terwujud secara substansial. Budaya hukum yang kuat akan muncul jika masyarakat menyadari hak dan kewajibannya, pelaku bisnis berkomitmen secara etis, dan pemerintah memberikan regulasi serta pengawasan yang tepat.

Diskusi lebih lanjut juga menunjukkan bahwa tantangan hukum di bidang e-commerce yang berkaitan dengan privasi dan keamanan data memiliki aspek internasional. Banyak platform e-commerce besar beroperasi di berbagai negara, sehingga data pelanggan Indonesia bisa diproses atau disimpan di luar negeri. Situasi ini memunculkan berbagai masalah hukum, seperti yurisdiksi, standar keamanan antarnegara, dan mekanisme penegakan hukum lintas batas. Tanpa adanya kerja sama global dan harmonisasi standar, perlindungan data pribadi pelanggan Indonesia akan terus menghadapi tantangan yang signifikan. Ini menunjukkan bahwa perlindungan data pribadi tidak dapat dipisahkan dari dinamika ekonomi digital global.

Akhirnya, penelitian ini menekankan pentingnya reformasi hukum dalam perlindungan data pribadi yang bersifat menyeluruh dan berkelanjutan. Pemerintah perlu tidak hanya memperbarui regulasi sesuai dengan perkembangan zaman, tetapi juga memastikan pelaksanaannya secara konsisten. Penguatan lembaga pengawas data pribadi merupakan hal yang mendesak agar mampu mengawasi pelaku e-commerce dengan efektif dan memberikan sanksi yang tegas kepada yang melanggar. Selain itu, edukasi masyarakat tentang keamanan data pribadi harus dilakukan secara terus-menerus, baik melalui kampanye nasional, pendidikan di kurikulum, maupun pelatihan untuk pelaku usaha. Dengan cara ini, perlindungan privasi dan keamanan data pelanggan dalam bisnis e-commerce dapat terwujud secara holistik.

### 3.1 Efektivitas Kerangka Hukum Perlindungan Data dalam E-Commerce

Dalam perspektif yuridis normatif, keberadaan Undang-Undang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta peraturan mengenai penyelenggaraan sistem dan transaksi elektronik telah membentuk dasar hukum yang relatif memadai untuk mengatur aktivitas e-commerce. Kerangka tersebut menempatkan data pribadi sebagai kepentingan hukum yang wajib dilindungi dan tidak boleh diproses secara sewenang-wenang. Pelaku usaha tidak cukup hanya menyediakan layanan transaksi, tetapi juga harus mampu menunjukkan dasar pemrosesan data, tujuan penggunaan, jangka waktu penyimpanan, mekanisme pengamanan, serta bentuk pertanggungjawaban apabila terjadi pelanggaran. Dengan demikian, kewajiban perlindungan data seharusnya dipahami sebagai bagian yang melekat pada seluruh siklus layanan, mulai dari pembuatan akun, pencarian produk, pembayaran, pengiriman, layanan purnajual, sampai penghapusan akun pelanggan.

Meskipun demikian, efektivitas hukum tidak hanya ditentukan oleh kelengkapan norma tertulis. Hukum baru dapat memberikan perlindungan nyata apabila dapat diterjemahkan ke dalam prosedur operasional yang jelas, terukur, dan konsisten. Persoalan yang ditemukan pada banyak platform adalah adanya jarak antara kebijakan privasi yang tertulis dan praktik pengelolaan data sehari-hari. Kebijakan dapat terlihat lengkap, tetapi tidak selalu diikuti pemetaan arus data, pembatasan akses, dokumentasi persetujuan, dan evaluasi terhadap risiko pemrosesan. Oleh sebab itu, penilaian kepatuhan perlu diarahkan pada bukti pelaksanaan, bukan hanya pada keberadaan dokumen. Audit kepatuhan, pencatatan aktivitas pemrosesan, evaluasi berkala, dan pengawasan terhadap perubahan sistem perlu menjadi bagian dari budaya organisasi agar kerangka hukum dapat bekerja secara substantif.

### 3.2 Persetujuan, Transparansi, dan Pembatasan Tujuan Pemrosesan

Persetujuan pelanggan merupakan salah satu unsur penting dalam pengelolaan data pribadi, tetapi persetujuan tidak boleh diperlakukan sekadar sebagai tombol yang harus ditekan sebelum konsumen dapat menggunakan layanan. Dalam praktik e-commerce, konsumen sering dihadapkan pada kebijakan privasi yang panjang, menggunakan istilah teknis, dan sulit dipahami. Kondisi tersebut dapat menghasilkan persetujuan yang bersifat formal, tetapi tidak mencerminkan pemahaman yang sebenarnya. Transparansi harus diwujudkan melalui penjelasan yang ringkas dan mudah ditemukan mengenai jenis data yang dikumpulkan, alasan pengumpulan, pihak yang menerima data, risiko yang mungkin timbul, serta cara konsumen menggunakan haknya. Informasi penting seharusnya tidak disembunyikan dalam ketentuan yang rumit atau digabungkan dengan persetujuan yang tidak berkaitan langsung dengan transaksi utama.

Prinsip pembatasan tujuan juga menjadi penting karena data yang awalnya dikumpulkan untuk menyelesaikan transaksi dapat digunakan kembali untuk pemasaran, analisis perilaku, pengembangan algoritma, atau dibagikan kepada mitra bisnis. Penggunaan lanjutan semacam itu memerlukan dasar yang jelas dan harus tetap selaras dengan tujuan yang telah diberitahukan kepada konsumen. Pelaku e-commerce perlu membedakan data yang benar-benar diperlukan untuk transaksi dengan data tambahan yang hanya mendukung kepentingan komersial. Konsumen seharusnya tetap dapat memperoleh layanan dasar tanpa dipaksa menyetujui seluruh kegiatan pemrosesan tambahan. Pendekatan ini akan memperkuat kebebasan memilih, mencegah pengumpulan data berlebihan, dan mengurangi risiko penyalahgunaan informasi pribadi.

### 3.3 Keamanan Data sebagai Kewajiban Hukum dan Tata Kelola Perusahaan

Keamanan data tidak dapat dibatasi pada penggunaan perangkat lunak keamanan atau pemasangan sistem enkripsi. Dalam konteks hukum, keamanan merupakan kewajiban tata kelola yang mencakup kebijakan, pembagian tanggung jawab, pengendalian akses, pelatihan sumber daya manusia, pemantauan sistem, dan penanganan risiko. Sebagian besar insiden tidak selalu terjadi karena kelemahan teknologi yang sangat rumit, tetapi dapat muncul akibat kata sandi yang lemah, akses pegawai yang tidak dibatasi, perangkat yang tidak diperbarui, atau kesalahan dalam mengirimkan informasi. Oleh karena itu, pelaku usaha perlu mengembangkan sistem pengamanan berlapis yang sesuai dengan skala bisnis, sensitivitas data, dan kemungkinan dampak yang timbul bagi pelanggan.

Penerapan prinsip privasi sejak perancangan perlu ditempatkan sebagai bagian dari proses pengembangan layanan. Setiap fitur baru, integrasi aplikasi, atau perubahan metode pembayaran seharusnya dinilai sejak awal dari sisi kebutuhan data dan risiko terhadap pelanggan. Pengumpulan data harus diminimalkan, akses dibatasi berdasarkan fungsi kerja, dan penyimpanan dilakukan hanya selama masih diperlukan. Selain itu, perusahaan perlu memiliki penanggung jawab yang mampu menghubungkan aspek hukum, teknologi, dan manajemen. Dengan model

tersebut, perlindungan data tidak menjadi tugas satu unit semata, melainkan tanggung jawab seluruh organisasi. Penguatan tata kelola juga membantu perusahaan membuktikan bahwa langkah pencegahan telah dilakukan secara wajar apabila terjadi sengketa atau pemeriksaan oleh otoritas.

### **3.4 Akuntabilitas Pihak Ketiga dalam Rantai Layanan Digital**

Transaksi e-commerce melibatkan lebih dari satu pelaku. Marketplace bekerja sama dengan penyedia pembayaran, perusahaan logistik, layanan komputasi awan, penyedia analitik, jaringan periklanan, dan berbagai mitra lain. Setiap hubungan tersebut dapat menimbulkan perpindahan atau akses terhadap data pelanggan. Karena itu, perlindungan tidak akan efektif apabila standar keamanan hanya diterapkan pada platform utama, sementara pihak ketiga memiliki pengamanan yang lebih lemah. Pelaku e-commerce perlu melakukan pemeriksaan sebelum menunjuk mitra, menetapkan kewajiban perlindungan data dalam perjanjian, membatasi tujuan penggunaan, serta menyediakan mekanisme pengawasan selama kerja sama berlangsung.

Pembagian tanggung jawab harus dijelaskan secara tegas agar tidak terjadi saling melepaskan kewajiban ketika insiden muncul. Perjanjian perlu mengatur siapa yang menentukan tujuan pemrosesan, siapa yang melaksanakan pemrosesan, siapa yang menangani permintaan pelanggan, dan siapa yang bertanggung jawab memberikan pemberitahuan apabila terjadi kebocoran. Ketentuan mengenai penghapusan atau pengembalian data setelah kerja sama berakhir juga perlu diperhatikan. Dari sudut perlindungan konsumen, kompleksitas hubungan bisnis tidak boleh menjadi alasan bagi pelanggan untuk kehilangan hak memperoleh penjelasan dan pemulihan. Platform yang berhubungan langsung dengan pelanggan tetap perlu menyediakan saluran pengaduan yang jelas dan membantu menentukan pihak yang bertanggung jawab berdasarkan alur pemrosesan data yang dapat dibuktikan.

### **3.5 Penanganan Insiden, Pemberitahuan, dan Pemulihan Kerugian**

Tidak ada sistem elektronik yang sepenuhnya bebas dari ancaman, sehingga kesiapan menghadapi insiden menjadi ukuran penting dari kepatuhan. Pelaku e-commerce perlu memiliki prosedur yang menjelaskan cara mendeteksi, mengendalikan, menyelidiki, dan mendokumentasikan kejadian keamanan. Ketika insiden terjadi, langkah pertama bukan hanya memperbaiki gangguan teknis, tetapi juga menilai jenis data yang terdampak, jumlah pengguna yang terlibat, kemungkinan penyalahgunaan, dan tindakan yang harus dilakukan untuk mengurangi kerugian. Proses tersebut harus melibatkan tim teknologi, hukum, komunikasi, dan layanan pelanggan agar respons tidak berjalan secara terpisah.

Pemberitahuan kepada pelanggan harus disampaikan secara jujur, jelas, dan tepat waktu. Informasi yang diberikan perlu menjelaskan apa yang terjadi, data apa yang mungkin terdampak, risiko yang dapat muncul, serta langkah yang dapat dilakukan pelanggan, misalnya mengganti kata sandi, mengaktifkan autentikasi tambahan, atau mengawasi aktivitas transaksi. Pemberitahuan yang terlambat atau terlalu umum dapat memperbesar kerugian karena pelanggan tidak memiliki kesempatan melindungi dirinya. Selain pemberitahuan, pemulihan juga harus mencakup dukungan nyata, penanganan pengaduan, dan mekanisme kompensasi apabila kelalaian pelaku usaha menimbulkan kerugian. Kesiapan pemulihan menunjukkan bahwa perlindungan data tidak berhenti pada pencegahan, tetapi mencakup tanggung jawab setelah risiko benar-benar terjadi.

### **3.6 Hak Konsumen dan Mekanisme Penyelesaian Sengketa**

Perlindungan data dalam e-commerce berkaitan langsung dengan hak konsumen untuk memperoleh informasi, keamanan, dan perlakuan yang adil. Konsumen perlu memiliki akses yang mudah untuk mengetahui data yang dikelola, memperbaiki informasi yang tidak akurat, menarik persetujuan untuk pemrosesan tertentu, serta meminta penghapusan ketika dasar penyimpanan tidak lagi tersedia. Saluran untuk menggunakan hak tersebut harus dipisahkan dari layanan pengaduan umum agar permintaan tidak terabaikan. Prosedur juga harus sederhana dan tidak mensyaratkan dokumen berlebihan yang justru menghambat konsumen.

Apabila terjadi sengketa, penyelesaian harus mempertimbangkan karakter transaksi digital yang cepat dan melibatkan pengguna dalam jumlah besar. Proses pengadilan tetap penting, tetapi tidak selalu menjadi pilihan yang praktis untuk setiap kasus. Karena itu, mekanisme internal yang transparan, mediasi, penyelesaian sengketa konsumen, dan sarana pengaduan elektronik perlu diperkuat. Platform perlu menyediakan nomor laporan, batas waktu penanganan, serta alasan tertulis atas keputusan yang diberikan. Kejelasan proses akan membantu konsumen memahami posisi hukumnya dan mencegah pengaduan berhenti tanpa penyelesaian. Dari sisi pelaku

usaha, dokumentasi pengaduan dapat digunakan untuk mengidentifikasi pola masalah, memperbaiki sistem, dan mencegah pelanggaran serupa. Dengan demikian, mekanisme sengketa tidak hanya berfungsi menyelesaikan kasus, tetapi juga menjadi bagian dari evaluasi kepatuhan.

### **3.7 Transfer Data Lintas Negara dan Persoalan Yurisdiksi**

Karakter e-commerce memungkinkan data pelanggan disimpan atau diproses melalui infrastruktur yang berada di negara lain. Penggunaan layanan komputasi awan, pusat data regional, dan penyedia analitik internasional dapat meningkatkan efisiensi, tetapi sekaligus menimbulkan persoalan yurisdiksi dan perbedaan standar perlindungan. Pelanggan sering tidak mengetahui lokasi data mereka diproses dan hukum mana yang berlaku ketika terjadi pelanggaran. Oleh karena itu, pelaku usaha perlu memiliki pemetaan yang jelas mengenai lokasi penyimpanan, pihak penerima, serta dasar perlindungan yang digunakan dalam pemindahan data.

Transfer lintas negara tidak seharusnya mengurangi tingkat perlindungan yang diterima pelanggan di Indonesia. Perusahaan harus memastikan bahwa penerima data menerapkan standar keamanan yang sepadan, tunduk pada kewajiban kontraktual, dan dapat diawasi. Ketentuan mengenai akses oleh pihak asing, penggunaan kembali data, serta penghapusan setelah tujuan selesai perlu diatur secara rinci. Dalam hal sengketa, platform juga harus memberikan titik kontak yang dapat dijangkau pelanggan di Indonesia. Kerja sama antarotoritas dan harmonisasi prinsip perlindungan data menjadi penting karena penegakan hukum nasional memiliki keterbatasan ketika pelaku atau infrastruktur berada di luar wilayah negara. Pendekatan tersebut dapat mengurangi ketidakpastian hukum tanpa menghambat perdagangan digital lintas batas.

### **3.8 Kecerdasan Buatan, Profiling, dan Keputusan Otomatis**

Pemanfaatan kecerdasan buatan dalam e-commerce memberi manfaat berupa rekomendasi produk, deteksi penipuan, pengelolaan persediaan, dan pelayanan pelanggan yang lebih cepat. Namun, teknologi ini juga memperluas penggunaan data perilaku dan dapat menghasilkan profiling yang sangat rinci. Riwayat pencarian, pola pembelian, lokasi, waktu transaksi, dan respons terhadap promosi dapat digabungkan untuk memperkirakan minat atau kemampuan konsumen. Jika tidak diawasi, pemrosesan tersebut dapat menimbulkan praktik yang tidak transparan, diskriminasi harga, manipulasi pilihan, atau pembatasan akses terhadap layanan tertentu.

Dari sudut hukum, penggunaan algoritma harus tetap tunduk pada prinsip tujuan yang sah, proporsionalitas, akurasi, dan akuntabilitas. Pelaku usaha perlu menjelaskan ketika keputusan yang berdampak penting terhadap konsumen dibuat secara otomatis. Konsumen juga perlu memiliki kesempatan untuk meminta peninjauan manusia apabila hasil sistem dianggap tidak tepat atau merugikan. Data yang digunakan untuk melatih atau menguji algoritma harus diperiksa agar tidak mengandung informasi yang diperoleh tanpa dasar atau menghasilkan bias yang berulang. Evaluasi dampak sebelum penerapan teknologi dapat membantu mengenali risiko dan menentukan langkah pengamanan. Dengan demikian, inovasi tetap dapat berkembang tanpa mengorbankan hak privasi dan kedudukan konsumen sebagai pihak yang harus dilindungi.

### **3.9 Kepatuhan Proporsional bagi Usaha Kecil dan Menengah Digital**

Kewajiban perlindungan data berlaku bagi seluruh pelaku usaha, tetapi kemampuan setiap perusahaan tidak sama. Platform besar memiliki sumber daya untuk membentuk tim keamanan dan hukum, sedangkan usaha kecil sering dikelola oleh sedikit orang dengan sistem sederhana. Pendekatan kepatuhan perlu mempertimbangkan skala dan risiko tanpa mengurangi hak pelanggan. Pemerintah dan asosiasi industri dapat menyediakan pedoman praktis, contoh kebijakan, daftar pemeriksaan, dan pelatihan yang mudah digunakan. Standar minimum dapat dimulai dari inventarisasi data, penggunaan kata sandi yang kuat, pembatasan akses, pencadangan, pembaruan perangkat, dan prosedur penghapusan data.

Pelaku usaha kecil juga perlu didorong memilih penyedia teknologi yang memiliki pengamanan memadai. Penggunaan layanan pihak ketiga bukan berarti seluruh tanggung jawab berpindah kepada penyedia tersebut. Pemilik usaha tetap perlu memahami data apa yang dikumpulkan, siapa yang dapat mengakses, dan bagaimana pelanggan dapat mengajukan permintaan. Pendampingan kepatuhan dapat dilakukan secara bertahap berdasarkan prioritas risiko. Data identitas, pembayaran, dan autentikasi harus memperoleh pengamanan lebih tinggi dibandingkan informasi yang bersifat umum. Model proporsional akan membantu UMKM digital memenuhi

kewajiban secara realistis, sekaligus mencegah anggapan bahwa perlindungan data hanya dapat dilakukan oleh perusahaan besar.

### 3.10 Penguatan Pengawasan dan Model Evaluasi Berkelanjutan

Pengawasan yang efektif memerlukan koordinasi antara lembaga yang menangani perlindungan data, perdagangan, komunikasi, keamanan siber, dan perlindungan konsumen. Koordinasi diperlukan agar pelaku usaha tidak menghadapi standar yang saling bertentangan dan konsumen tidak kebingungan menentukan tempat pengaduan. Pembagian kewenangan harus disertai pertukaran informasi, prosedur pemeriksaan, dan mekanisme tindak lanjut yang jelas. Pengawasan juga perlu bersifat berbasis risiko, sehingga perhatian lebih besar diberikan kepada platform yang memproses data dalam jumlah besar, menggunakan teknologi profiling, atau memiliki riwayat insiden keamanan.

Evaluasi kepatuhan sebaiknya tidak hanya dilakukan setelah pelanggaran terjadi. Pemeriksaan berkala, pelaporan internal, pengujian keamanan, dan evaluasi dampak dapat digunakan sebagai langkah pencegahan. Indikator evaluasi dapat mencakup waktu respons terhadap permintaan konsumen, jumlah akses yang tidak sah, kepatuhan pihak ketiga, hasil audit, dan efektivitas pelatihan pegawai. Hasil evaluasi kemudian menjadi dasar perbaikan kebijakan dan sistem. Transparansi mengenai upaya perlindungan juga dapat meningkatkan kepercayaan publik, selama tidak membuka informasi teknis yang dapat dimanfaatkan oleh pelaku kejahatan. Pada akhirnya, perlindungan data dalam e-commerce harus dipahami sebagai proses berkelanjutan yang menyesuaikan perkembangan teknologi, pola ancaman, dan kebutuhan konsumen. Pendekatan tersebut akan membuat regulasi lebih hidup dan mendorong terciptanya ekosistem digital yang aman, adil, dan dapat dipercaya.

## 4. Kesimpulan

Penelitian tentang tantangan hukum dalam bisnis e-commerce untuk melindungi data dan privasi pengguna menunjukkan bahwa kemajuan teknologi digital telah menyebabkan perubahan besar dalam cara transaksi ekonomi dan sistem bisnis saat ini. Meskipun kemudahan dan efisiensi yang ditawarkan, ada risiko signifikan terkait dengan pengelolaan dan perlindungan data pribadi pengguna. Risiko tersebut timbul dari tingginya volume pengumpulan data, meningkatnya kemungkinan kebocoran informasi, serta ketidakmampuan sebagian pelaku usaha untuk menerapkan standar keamanan siber yang memadai. Dalam hal ini, masalah keamanan data bukan sekadar isu teknis, tetapi juga merupakan isu hukum yang memerlukan kepastian regulasi dan kepatuhan dari pelaku usaha. Temuan penelitian menunjukkan bahwa sistem regulasi di Indonesia sebenarnya telah berkembang, terutama dengan adanya Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini memberikan dasar hukum yang lebih solid untuk melindungi hak-hak pemilik data sekaligus menambahkan kewajiban bagi pengendali dan pemroses data. Namun, penegakan hukum dan mekanisme pengawasan masih memiliki banyak kekurangan, terutama karena masih ada tumpang tindih regulasi sektoral, kurangnya pemahaman di kalangan pelaku usaha, dan terbatasnya kapasitas lembaga pengawas dalam melakukan audit serta investigasi. Dengan demikian, meskipun kerangka hukum relatif kuat, penerapannya belum optimal dan masih menyisakan celah untuk potensi pelanggaran privasi. Di sisi lain, penelitian ini juga menemukan bahwa pelaku usaha e-commerce menghadapi tantangan internal, termasuk keterbatasan sumber daya, fokus pada keuntungan jangka pendek, serta kurangnya perhatian terhadap aspek keamanan informasi. Banyak platform, terutama yang berasal dari usaha kecil dan menengah, belum menerapkan teknologi perlindungan data yang cukup seperti enkripsi, pengujian kerentanan, atau sistem manajemen keamanan informasi yang baik. Hal ini membuat data konsumen rentan disalahgunakan oleh pihak ketiga, baik untuk tujuan komersial maupun kejahatan siber. Keadaan ini menegaskan perlunya perubahan pemikiran bahwa keamanan data adalah aset bisnis yang harus dikelola secara serius, tidak hanya sebagai tambahan dalam operasional. Dari perspektif konsumen, masih ada masalah kurangnya kesadaran tentang hak terkait data pribadi. Banyak pelanggan memberikan izin akses data tanpa memahami atau membaca syarat dan ketentuan layanan yang ada. Konsumen juga cenderung tidak melaporkan pelanggaran privasi, sehingga pelaku usaha kurang terdorong untuk meningkatkan standar perlindungan data. Rendahnya pemahaman tentang privasi ini memperburuk risiko penyalahgunaan data, terutama di platform yang tidak transparan mengenai kebijakan privasinya. Oleh karena itu, peran masyarakat juga sangat penting dalam menciptakan ekosistem perlindungan data pribadi yang aman. Kesimpulan utama dari penelitian ini adalah bahwa tantangan hukum dalam bisnis e-commerce berkaitan dengan keamanan data dan privasi pengguna merupakan masalah yang kompleks dan melibatkan berbagai aspek regulasi, teknologi, tata kelola perusahaan, serta perilaku konsumen. Kerangka hukum yang kuat tidak akan efektif tanpa penerapan yang konsisten dari pelaku usaha, pengawasan yang ketat dari pemerintah, serta kesadaran yang tinggi dari masyarakat. Oleh karena itu, perlindungan data pribadi harus dianggap sebagai tanggung jawab bersama yang memerlukan kolaborasi antara negara, pelaku usaha, dan

konsumen. Tanpa upaya bersama, risiko pelanggaran privasi akan semakin meningkat seiring dengan pertumbuhan ekosistem digital. Secara keseluruhan, studi ini menyoroti pentingnya penguatan pengelolaan data pribadi dalam dunia e-commerce sebagai bagian dari upaya untuk menciptakan transaksi digital yang aman, dapat dipercaya, dan berkelanjutan. Perlindungan data tidak hanya bersifat kewajiban hukum, tetapi juga merupakan investasi strategis bagi pelaku usaha dalam mempertahankan loyalitas pelanggan, citra bisnis, dan kelangsungan usaha. Dengan demikian, tantangan hukum dalam sektor e-commerce perlu diatasi melalui penguatan regulasi, peningkatan kepatuhan, dan transformasi budaya digital yang mengutamakan keamanan serta privasi sebagai prioritas utama.

## Referensi

1. Asshiddiqie, Jimly. Pengantar Ilmu Hukum Tata Negara. Jakarta: Rajawali Pers, 2020.
2. Bakhri, Syaiful. Keamanan Siber dan Tantangan Regulasi di Indonesia. Yogyakarta: Deepublish, 2021.
3. Chaffey, Dave. E-Business and E-Commerce Management. New York: Pearson, 2019.
4. Elly Erawati. Hukum Perlindungan Konsumen. Bandung: Refika Aditama, 2020.
5. Friedman, Lawrence. Legal System: A Social Science Perspective. New York: Russel Sage Foundation, 2021.
6. Gunawan, Hendra. Hukum Siber dan Perlindungan Data. Jakarta: Kencana, 2022.
7. Laudon, Kenneth dan Laudon, Jane. Management Information Systems. London: Pearson, 2020.
8. McQuade, Samuel. Understanding Cybercrime. Oxford: Oxford University Press, 2019.
9. O'Brien, James. Management Information System for Business Decisions. New York: McGraw-Hill, 2020.
10. Sumanjuntak, R. H. Hukum Digital dan Perlindungan Data Pribadi. Jakarta: Sinar Grafika, 2023.
11. Adi, Naufal. "Implikasi UU Perlindungan Data Pribadi terhadap Model Bisnis E-Commerce di Indonesia." *Jurnal Hukum dan Teknologi*, 11(2), 2023.
12. Ahsan, R. "Kebijakan Regulasi Data Pribadi dalam Transformasi Digital." *Jurnal Legislasi Indonesia*, 20(1), 2023.
13. Anggraeni, M. "Keamanan Transaksi Digital pada Platform Marketplace." *Jurnal Teknologi Informasi*, 15(1), 2022.
14. Dewi, Ayu. "Privasi Pengguna dalam Ekosistem Digital." *Jurnal Komunikasi Hukum*, 9(3), 2021.
15. Fadilah, Hanif. "Analisis Kerangka Hukum E-Commerce dalam Perspektif Perlindungan Konsumen." *Jurnal Ilmu Hukum Prima*, 18(2), 2022.
16. Fitriani, Nurul. "Cybersecurity Readiness in Indonesian SMEs." *Jurnal Bisnis Digital Indonesia*, 5(2), 2022.
17. Gunawan, D. "Urgensi Penegakan UU ITE dalam Kejahatan Siber." *Jurnal Hukum Pidana Kontemporer*, 8(1), 2021.
18. Hidayat, R. "Perlindungan Privasi pada Platform Marketplace." *Jurnal Ekonomi dan Bisnis Digital*, 12(2), 2023.
19. Iskandar, B. "Implementasi Sistem Keamanan Informasi di UMKM Digital." *Jurnal Sistem Informasi*, 14(4), 2021.
20. Lestari, Shinta. "Regulasi Perlindungan Data Pribadi di Indonesia: Analisis Normatif." *Jurnal Rechtsvinding*, 10(3), 2022.
21. Kementerian Komunikasi dan Informatika. Laporan Keamanan Siber Nasional 2023. Jakarta: Kominfo, 2023.
22. Badan Siber dan Sandi Negara. Indonesia Cyber Security Monitoring Report 2024. Jakarta: BSSN, 2024.
23. Otoritas Jasa Keuangan. Survei Literasi dan Inklusi Digital. Jakarta: OJK, 2022.
24. World Bank. Digital Economy Report: Southeast Asia Outlook. Washington DC: World Bank, 2023.
25. OECD. Data Governance and Digital Privacy Guidelines. Paris: OECD Publishing, 2022.
26. UNCTAD. Digital Economy Report 2022: Cross-Border Data Flows and Development. Geneva: UNCTAD, 2022.
27. McKinsey and Company. The Rise of Online Commerce in Asia. Hong Kong: McKinsey, 2023.
28. Google, Temasek, Bain and Company. E-Conomy SEA Report 2023. Singapore, 2023.
29. PwC Indonesia. Cybersecurity Risk in Indonesian E-Commerce. Jakarta: PwC, 2022.
30. Deloitte. Digital Consumer Insights 2023. Singapore: Deloitte Southeast Asia, 2023.
31. European Data Protection Board. Guidelines on Data Protection Impact Assessment.
32. International Association of Privacy Professionals (IAPP). Global Legislative Update on Data Privacy Regulations.
33. Asia-Pacific Economic Cooperation (APEC). Privacy Framework and Cross-Border Privacy Rules.
34. ISO/IEC 27001 Documentation on Information Security Management Systems (ISMS).
35. Cybersecurity and Infrastructure Security Agency (CISA). Cyber Threat Analysis Report, 2023.
36. Harvard Business Review Digital Resources on E-Commerce Privacy Frameworks.
37. Stanford Cyber Policy Center. Data Governance and Digital Surveillance Insights, 2023.