

IMPLEMENTASI UU PELINDUNGAN DATA PRIBADI DALAM MENJAMIN KEAMANAN TRANSAKSI ELEKTRONIK PADA E-COMMERCE DI INDONESIA

Author:

Pandapotan
Tampubolon¹
Samuel Revaldo
Jeverson Siboro²
Ryam Chandra
Dalimunthe³

Affiliation:

Universitas Negeri
Medan^{1,2,3}

Corresponding email

[pandapotantampubolon13@
gmail.com](mailto:pandapotantampubolon13@gmail.com),
Samuelsioro91@gmail.com
[yanchandradalimunthe97@g
mail.com](mailto:yanchandradalimunthe97@gmail.com)

Histori Naskah:

Submit: 28-05-2026
Accepted: 15-06-2026
Published: 13-07-2026



*This is an Creative Commons
License This work is licensed
under a Creative Commons
Attribution-NonCommercial
4.0 International License*

Abstrak:

Pesatnya perkembangan ekonomi digital telah menempatkan electronic commerce (e-commerce) sebagai sektor utama dalam transaksi nasional. Namun, akselerasi aktivitas digital ini berbanding lurus dengan risiko kebocoran data pribadi. Meskipun berbagai penelitian telah membahas perlindungan konsumen digital dan keamanan transaksi elektronik secara terpisah, masih terbatas kajian yang mengintegrasikan analisis keamanan transaksi elektronik dengan implementasi UU Pelindungan Data Pribadi (UU PDP) dalam konteks e-commerce Indonesia. Oleh karena itu, penelitian ini menawarkan perspektif yang lebih komprehensif mengenai hubungan antara aspek teknis keamanan informasi dan kerangka hukum perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis pengaruh sistem keamanan transaksi elektronik terhadap efektivitas perlindungan data pribadi konsumen. Menggunakan metode penelitian yuridis normatif dengan pendekatan studi literatur, penelitian ini mensintesis temuan dari 27 sumber primer yang mencakup e-book dan jurnal ilmiah terkini. Hasil analisis menunjukkan bahwa keamanan teknis, seperti enkripsi, tanda tangan digital, dan Dynamic Application Security Testing (DAST), berperan sebagai benteng pertahanan pertama. Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan UU ITE memberikan kepastian hukum dan kerangka tanggung jawab bagi pihak marketplace. Penelitian ini menemukan bahwa meskipun kerangka hukum telah kuat, tantangan implementasi masih terletak pada lembaga pengawas dan kesadaran hukum masyarakat. Penelitian menunjukkan bahwa sinergi antara infrastruktur keamanan yang canggih dan penegakan hukum yang konsisten sangat krusial untuk membangun kepercayaan konsumen dan menjamin pertumbuhan ekonomi digital yang berkelanjutan. Secara akademik, penelitian ini memperkaya kajian hukum bisnis digital melalui sintesis antara pendekatan keamanan siber dan perlindungan data pribadi. Secara praktis, hasil penelitian dapat menjadi rujukan bagi regulator dan penyelenggara e-commerce dalam memperkuat tata kelola keamanan data konsumen.

Kata kunci: Keamanan Transaksi Elektronik, Perlindungan Data Pribadi, E-Commerce, UU PDP, Kepercayaan Konsumen.

Pendahuluan

Transformasi ekonomi digital di Indonesia telah menempatkan sektor perdagangan elektronik atau *e-commerce* sebagai katalisator utama pertumbuhan ekonomi nasional yang mengubah paradigma interaksi antara pelaku usaha dan konsumen. Pesatnya

perkembangan ini memungkinkan konsumen untuk melakukan transaksi tanpa batasan waktu dan geografis, yang didorong oleh kemudahan akses serta efisiensi biaya operasional bagi para penyedia layanan (Menarianti et al., 2024). Penggunaan sistem pembayaran digital seperti *Quick Response Code Indonesian Standard* (QRIS) menjadi salah satu tren utama yang mempercepat inklusi keuangan dan revitalisasi sektor usaha mikro, kecil, dan menengah (UMKM) dalam ekosistem digital (Handayani & Soeparan, 2022; Kristanty, 2024). Namun, akselerasi digitalisasi ini membawa tantangan besar terkait ketergantungan pada pengumpulan dan analisis data konsumen secara masif sebagai aset strategis dalam aktivitas ekonomi (Prayuti, 2024). Keamanan informasi dan jaringan komputer akhirnya menjadi fondasi yang tidak terpisahkan dalam menjamin keberlangsungan layanan *e-commerce* yang memproses data sensitif setiap harinya (Putra & Toresa, 2021).

Urgensi penelitian ini didasarkan pada fenomena meningkatnya risiko keamanan dalam transaksi elektronik yang berbanding lurus dengan intensitas aktivitas digital masyarakat. Kerentanan pada aplikasi *web* di berbagai platform besar seperti Shopee, TikTok Shop, dan Facebook Marketplace menunjukkan bahwa serangan siber tetap menjadi ancaman nyata yang dapat mengganggu integritas transaksi (Lubis et al., 2025). Keamanan informasi bukan sekadar masalah teknis, melainkan aspek krusial dalam membangun kepercayaan (*trust*) pelanggan yang menjadi kunci keberhasilan platform digital seperti Lazada (Handayani et al., 2024). Tanpa sistem keamanan yang andal, pelaku usaha berisiko menghadapi kerugian finansial sekaligus degradasi reputasi akibat kegagalan dalam menjaga kerahasiaan data pengguna (Wibowo, 2024). Oleh karena itu, implementasi manajemen sekuriti yang efektif sangat diperlukan untuk memitigasi ancaman kecurangan transaksi yang kian kompleks di ruang siber (Rahmat Irawan et al., dalam Handayani et al., 2024).

Masalah perlindungan data pribadi konsumen dalam *e-commerce* telah mencapai titik kritis dengan seringnya terjadi kasus kebocoran data yang melibatkan jutaan akun pengguna di Indonesia (Priliasari, 2023). Kebocoran informasi sensitif seperti nomor kartu kredit, alamat, dan identitas pribadi lainnya telah menimbulkan risiko hukum dan sosial yang serius, mulai dari pencurian identitas hingga penyalahgunaan data untuk aktivitas ilegal (Budiandru & Hidayat, 2025). Sektor teknologi finansial (*fintech*) yang terintegrasi dengan *e-commerce* juga tidak luput dari ancaman ini, di mana kebocoran data pada platform pinjaman *online* dapat mengakibatkan kerugian materiil bagi konsumen (Sari, 2025; Kim et al., 2025). Meskipun data pribadi merupakan bagian dari hak asasi manusia atas perlindungan diri yang dijamin konstitusi, namun dalam praktiknya, pemenuhan hak privasi ini masih sering terabaikan oleh penyelenggara sistem elektronik (Jurnal Analisis Hukum, 2023; Maharani & Prakoso, 2024).

Penelitian terdahulu telah banyak mengeksplorasi perlindungan konsumen dari perspektif Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (Izazi et al., 2024). Dinamika perlindungan hukum di era digital juga mulai bergeser dengan lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan

Data Pribadi (UU PDP) yang diharapkan memberikan standar pengikatan yang lebih kuat bagi pengendali data (Budhijanto, 2024). Beberapa studi juga menyoroti keabsahan tanda tangan digital sebagai instrumen kepastian hukum dalam memperkuat validasi transaksi elektronik (Susilowati et al., 2025). Meskipun demikian, terdapat *research gap* yang signifikan di mana meskipun instrumen hukum seperti UU PDP dan perubahan UU ITE telah tersedia, implementasinya masih terkendala oleh absennya lembaga pengawas data yang independen dan efektif (Matheus & Gunadi, 2024; Gustryan & Hoessein, 2025). Selain itu, tingkat kesadaran hukum masyarakat terhadap hak atas datanya masih tergolong rendah, yang pada akhirnya melemahkan efektivitas perlindungan yang diberikan oleh regulasi (Putra et al., 2023; Zahwani & Nasution, 2023).

Penelitian terdahulu cenderung mengkaji perlindungan data pribadi dari perspektif hukum semata atau menelaah keamanan transaksi elektronik dari aspek teknis keamanan informasi. Studi Izazi et al. (2024) berfokus pada perlindungan konsumen dalam transaksi elektronik, sedangkan Lubis et al. (2025) menitikberatkan pada aspek keamanan aplikasi e-commerce melalui pendekatan DAST. Di sisi lain, Budhijanto (2024) mengkaji implementasi UU PDP sebagai instrumen perlindungan data pribadi. Namun demikian, belum banyak penelitian yang mengintegrasikan dimensi keamanan transaksi elektronik, perlindungan data pribadi, dan implementasi UU PDP dalam satu kerangka analisis hukum bisnis digital. Kesenjangan inilah yang menjadi dasar penelitian ini.

Tujuan dari penelitian ini adalah untuk menganalisis secara mendalam pengaruh sistem keamanan transaksi elektronik terhadap efektivitas perlindungan data pribadi konsumen dalam ekosistem *e-commerce* di Indonesia. Analisis ini tidak hanya fokus pada aspek yuridis perlindungan konsumen melalui tanggung jawab pelaku usaha, tetapi juga mengkaji bagaimana keandalan teknologi keamanan dapat membangun kepercayaan digital (Purwito, 2023). Selain itu, penelitian ini bertujuan mengevaluasi sejauh mana penerapan prinsip-prinsip etika bisnis dan transparansi tata kelola data oleh pihak *marketplace* mampu memitigasi risiko kebocoran data (Pernando et al., 2024). Dengan memahami korelasi antara keamanan teknis dan kepastian hukum, diharapkan penelitian ini dapat memberikan rekomendasi strategis bagi penguatan regulasi dan praktik industri. Keberhasilan dalam menjamin keamanan transaksi dan privasi data pada akhirnya akan mendorong keputusan pembelian konsumen secara berkelanjutan di platform digital (Siallagan & Wasiman, 2025). Kebaruan penelitian ini terletak pada pengintegrasian analisis keamanan transaksi elektronik, implementasi UU PDP, dan perlindungan data pribadi konsumen dalam satu kerangka hukum bisnis digital. Berbeda dengan penelitian terdahulu yang cenderung mengkaji aspek hukum atau aspek teknis secara terpisah, penelitian ini menawarkan sintesis multidisipliner yang menjelaskan bagaimana keamanan teknologi dan regulasi perlindungan data saling memperkuat dalam membangun kepercayaan konsumen pada ekosistem e-commerce.

Studi Literatur

Dinamika *E-Commerce* dan Ekosistem Ekonomi Digital

Perdagangan elektronik atau *e-commerce* telah berkembang menjadi pilar fundamental dalam ekonomi global yang menawarkan efisiensi operasional melalui integrasi teknologi informasi dan komunikasi dalam setiap rantai bisnis. Secara konseptual, *e-commerce* bukan sekadar media jual beli daring, melainkan sebuah ekosistem kompleks yang melibatkan transaksi keuangan, pertukaran data elektronik, dan sistem manajemen inventaris yang terotomatisasi (Menarianti et al., 2024). Keberadaan *e-commerce* memberikan keunggulan kompetitif bagi pelaku usaha, khususnya dalam menjangkau pasar yang lebih luas tanpa kendala fisik, sementara bagi konsumen, platform ini menyediakan transparansi harga dan kenyamanan bertransaksi (Priliasari, 2023). Di Indonesia, revitalisasi sektor UMKM sangat bergantung pada adopsi sistem pembayaran digital yang memungkinkan proses transaksi menjadi lebih cepat dan tercatat secara akurat (Handayani & Soeparan, 2022). Namun, ketergantungan yang tinggi pada infrastruktur digital ini menuntut adanya standar keamanan yang mumpuni untuk melindungi seluruh pemangku kepentingan dalam ekosistem tersebut. Perkembangan *e-commerce* menunjukkan bahwa keberhasilan ekonomi digital tidak hanya ditentukan oleh kemudahan transaksi dan inovasi teknologi, tetapi juga oleh kemampuan platform dalam menjamin keamanan informasi pengguna. Semakin tinggi ketergantungan aktivitas perdagangan pada sistem elektronik, semakin besar pula kebutuhan terhadap perlindungan data pribadi sebagai instrumen untuk menjaga keberlangsungan ekosistem digital. Dengan demikian, keamanan transaksi dan perlindungan data menjadi elemen yang tidak terpisahkan dari perkembangan *e-commerce* modern.

Keamanan Transaksi Elektronik dan *Cyber Security*

Keamanan transaksi elektronik merupakan proteksi menyeluruh terhadap integritas, ketersediaan, dan kerahasiaan data selama proses pertukaran informasi secara daring. Dalam perspektif teknis, keamanan ini melibatkan penggunaan kriptografi, protokol enkripsi data, serta mekanisme autentikasi yang canggih untuk mencegah akses tidak sah (Putra & Toresa, 2021). Pengujian keamanan aplikasi secara berkala menggunakan metode seperti *Dynamic Application Security Testing* (DAST) menjadi sangat krusial, mengingat platform besar seperti Shopee dan TikTok Shop tetap memiliki potensi kerentanan terhadap serangan siber yang dapat memanipulasi integritas transaksi (Lubis et al., 2025). Selain itu, penggunaan instrumen seperti tanda tangan digital memberikan lapisan kepastian hukum tambahan yang menjamin bahwa transaksi dilakukan oleh pihak yang sah dan tidak dapat disangkal di kemudian hari (Susilowati et al., 2025). Keamanan informasi dalam hal ini bukan hanya sekadar kebutuhan teknis, melainkan sebuah standar manajemen sekuriti yang menentukan reputasi dan keberlangsungan sebuah platform digital (Wibowo, 2024). Dalam konteks *e-commerce*, keamanan transaksi elektronik tidak dapat dipandang semata-mata sebagai persoalan teknis. Efektivitas sistem keamanan akan menentukan sejauh mana data pribadi konsumen dapat dilindungi dari akses yang tidak sah. Oleh karena itu, aspek keamanan siber memiliki keterkaitan erat dengan implementasi kewajiban perlindungan data pribadi sebagaimana diatur dalam UU PDP.

Perlindungan Data Pribadi dan Hak Privasi Konsumen

Perlindungan data pribadi merupakan manifestasi dari hak privasi yang dijamin oleh konstitusi sebagai bagian dari hak asasi manusia untuk mendapatkan perlindungan atas diri pribadi dan martabatnya (Jurnal Analisis Hukum, 2023). Dalam konteks digital, data pribadi bertransformasi menjadi aset strategis yang memiliki nilai ekonomi tinggi, sehingga pengelolaannya harus didasarkan pada prinsip transparansi dan akuntabilitas (Gustryan & Hoesein, 2025). Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) di Indonesia menandai babak baru dalam pengaturan tanggung jawab pengendali data, yang mengharuskan adanya jaminan keamanan fisik maupun elektronik terhadap data yang dikelola (Budhijanto, 2024). Tantangan utama dalam perlindungan ini sering kali muncul dari lemahnya pengawasan dan belum terbentuknya lembaga pengawas independen yang mampu memberikan sanksi tegas terhadap kegagalan sistem elektronik (Matheus & Gunadi, 2024). Dialog ilmiah menunjukkan bahwa tanpa perlindungan data yang efektif, hak-hak privasi konsumen akan terus terancam oleh praktik komersialisasi data tanpa izin dan risiko kebocoran informasi sensitif (Maharani & Prakoso, 2024). Kehadiran UU PDP memperluas paradigma perlindungan konsumen digital dari sekadar perlindungan terhadap kerugian transaksi menjadi perlindungan terhadap hak atas data pribadi. Dengan demikian, keamanan transaksi elektronik berfungsi sebagai instrumen teknis, sedangkan UU PDP berfungsi sebagai instrumen yuridis yang secara bersama-sama menjamin perlindungan hak privasi konsumen.

Perlindungan Konsumen Digital dan Tanggung Jawab Pelaku Usaha

Perlindungan konsumen dalam era digital menghadapi tantangan kebijakan yang lebih kompleks dibandingkan transaksi konvensional karena adanya asimetri informasi dan batasan yurisdiksi. Pelaku usaha di platform *e-commerce* memiliki kewajiban hukum untuk menyediakan sistem yang aman dan bertanggung jawab atas setiap kerugian yang timbul akibat cacat sistem atau kebocoran data (Prabowo & Sulistianingsih, 2026). Tanggung jawab ini mencakup pemenuhan standar pelayanan purna jual dan penyelesaian sengketa, baik melalui jalur litigasi maupun non-litigasi (Purwito, 2023). Namun, penegakan hukum terhadap perusahaan yang gagal menjaga keamanan transaksi sering kali terkendala oleh interpretasi regulasi yang reaktif dan kurang adaptif terhadap inovasi teknologi (Halim et al., 2024). Oleh karena itu, sinergi antara UU ITE, UU Perlindungan Konsumen, dan UU PDP menjadi instrumen krusial dalam menciptakan keadilan bagi pengguna jasa digital di tengah dinamika ekonomi yang agresif (Izazi et al., 2024). Dengan berkembangnya model bisnis berbasis data, tanggung jawab pelaku usaha tidak lagi terbatas pada penyediaan barang dan jasa yang aman, tetapi juga mencakup kewajiban menjaga keamanan data pribadi konsumen. Oleh karena itu, perlindungan konsumen digital pada era ekonomi digital harus dipahami sebagai kombinasi antara perlindungan transaksi dan perlindungan data pribadi.

Kepercayaan Konsumen (*Consumer Trust*) dan Etika Bisnis

Kepercayaan konsumen merupakan faktor psikologis utama yang menentukan keputusan pembelian dan loyalitas pelanggan dalam transaksi elektronik. Kepercayaan ini dibangun melalui persepsi konsumen terhadap keamanan sistem, kejujuran pelaku usaha, dan penerapan prinsip-prinsip etika bisnis yang konsisten (Pernando et al., 2024). Hasil penelitian terdahulu mengonfirmasi bahwa jaminan keamanan transaksi secara langsung berkorelasi positif dengan tingkat kepercayaan masyarakat terhadap platform seperti Lazada atau TikTok Shop (Handayani et al., 2024; Siallagan & Wasiman, 2025). Di sisi lain, rendahnya kesadaran hukum masyarakat dan kurangnya pemahaman teknis mengenai hak-hak datanya menjadi hambatan dalam membangun lingkungan digital yang terpercaya (Zahwani & Nasution, 2023; Putra et al., 2023). Kepercayaan digital tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada bagaimana platform mampu menunjukkan transparansi dalam pengelolaan data pribadi pengguna secara etis (Kim et al., 2025).

Penelitian Terdahulu

Untuk memperjelas posisi penelitian ini dalam khazanah hukum bisnis digital, diperlukan telaah terhadap beberapa penelitian terdahulu yang relevan mengenai keamanan transaksi elektronik, perlindungan data pribadi, dan perlindungan konsumen dalam ekosistem e-commerce.

Tabel 1. Penelitian Terdahulu yang Relevan

Peneliti	Fokus Penelitian	Temuan Utama	Keterbatasan
Priliasari (2023)	Perlindungan data pribadi konsumen dalam transaksi e-commerce	Perlindungan data pribadi telah diatur dalam berbagai peraturan perundang-undangan, namun implementasinya masih menghadapi berbagai tantangan.	Belum mengkaji hubungan antara keamanan transaksi elektronik dan efektivitas perlindungan data pribadi.
Budhijanto (2024)	Hukum perlindungan data pribadi dan data nasional	UU PDP memberikan dasar hukum yang lebih komprehensif dalam tata kelola data pribadi.	Fokus pada aspek regulasi tanpa mengaitkan dengan keamanan transaksi elektronik.
Lubis et al. (2025)	Analisis keamanan aplikasi e-commerce menggunakan DAST	Keamanan aplikasi sangat menentukan tingkat kerentanan terhadap serangan siber and kebocoran data.	Berorientasi pada aspek teknis dan belum membahas implikasi hukum.

Maharani dan Prakoso (2024)	Perlindungan data pribadi oleh penyelenggara sistem elektronik	Penyelenggara sistem elektronik memiliki tanggung jawab menjaga keamanan data pengguna.	Tidak membahas keterkaitan dengan kepercayaan konsumen dan keberlanjutan ekonomi digital.
Handayani et al. (2024)	Manajemen sekuriti dan kepercayaan pelanggan e-commerce	Keamanan sistem berpengaruh terhadap peningkatan kepercayaan pelanggan.	Tidak mengintegrasikan aspek perlindungan data pribadi dan regulasi UU PDP.

Berdasarkan tabel di atas, dapat dilihat bahwa penelitian terdahulu cenderung membahas keamanan transaksi elektronik, perlindungan data pribadi, maupun kepercayaan konsumen secara terpisah. Sebagian penelitian berfokus pada aspek teknis keamanan sistem, sedangkan penelitian lainnya menitikberatkan pada aspek regulasi perlindungan data pribadi. Hingga saat ini masih terbatas penelitian yang mengintegrasikan keamanan transaksi elektronik dengan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dalam konteks perlindungan data pribadi konsumen e-commerce. Oleh karena itu, penelitian ini berupaya mengisi kesenjangan tersebut melalui analisis yang menghubungkan aspek teknologi keamanan informasi dengan instrumen hukum perlindungan data pribadi dalam kerangka hukum bisnis digital.

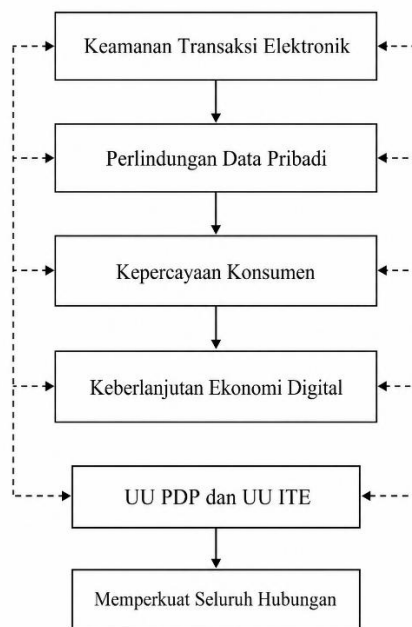
Kerangka Konseptual Penelitian

Kajian literatur menunjukkan bahwa keamanan transaksi elektronik merupakan fondasi utama dalam perlindungan data pribadi konsumen. Sistem keamanan yang andal melalui enkripsi, autentikasi, tanda tangan digital, serta pengujian keamanan aplikasi secara berkala mampu meminimalkan risiko kebocoran data dan penyalahgunaan informasi pribadi pengguna. Dalam konteks ini, keamanan transaksi elektronik berperan sebagai instrumen preventif yang mendukung terlindunginya hak-hak privasi konsumen. Di sisi lain, perlindungan data pribadi yang efektif tidak hanya bergantung pada aspek teknis, tetapi juga memerlukan dukungan regulasi yang kuat. Kehadiran UU PDP dan UU ITE memberikan dasar hukum bagi pengendali data dan penyelenggara sistem elektronik untuk menjalankan kewajiban perlindungan data secara bertanggung jawab. Dengan demikian, regulasi berfungsi sebagai instrumen penguatan terhadap implementasi keamanan transaksi elektronik.

Perlindungan data pribadi yang terjamin selanjutnya akan meningkatkan kepercayaan konsumen terhadap platform e-commerce. Kepercayaan tersebut menjadi faktor penting dalam mendorong loyalitas pelanggan, meningkatkan partisipasi masyarakat dalam transaksi digital, serta memperkuat keberlanjutan ekonomi digital nasional. Oleh karena itu, hubungan antara keamanan transaksi elektronik, perlindungan data pribadi, dan

kepercayaan konsumen membentuk suatu kerangka konseptual yang saling terintegrasi.

Model konseptual penelitian ini dapat digambarkan sebagai berikut:



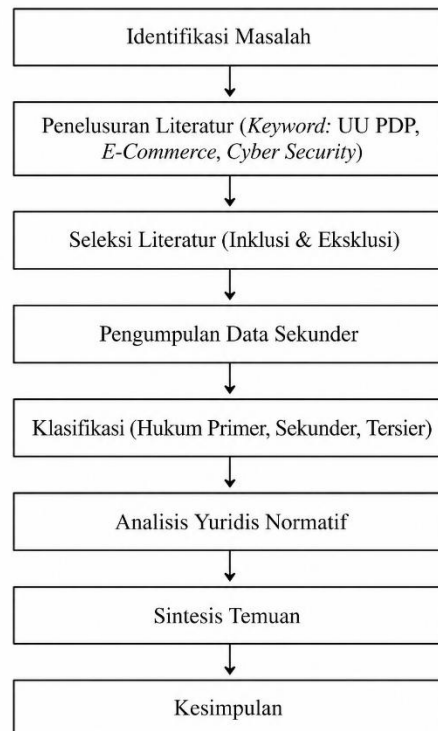
Gambar 1. Kerangka Konseptual

Metode Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif yang berfokus pada analisis terhadap norma-norma hukum positif, asas-asas hukum, serta sinkronisasi peraturan perundang-undangan yang berlaku di Indonesia terkait ekonomi digital. Jenis penelitian yang diterapkan adalah deskriptif-analitis dengan metode studi literatur (*library research*) untuk menggambarkan secara sistematis fakta-fakta hukum mengenai keamanan transaksi elektronik dan perlindungan data pribadi konsumen (Priliasari, 2023). Objek penelitian ini difokuskan pada pengaruh mekanisme keamanan teknis dan kerangka regulasi terhadap pemenuhan hak privasi pengguna dalam platform *e-commerce*. Pendekatan ini dipilih karena permasalahan yang dikaji memerlukan interpretasi mendalam terhadap teks undang-undang serta sintesis dari berbagai hasil penelitian terdahulu yang relevan dengan dinamika keamanan siber (Matheus & Gunadi, 2024).

Prosedur seleksi literatur dalam penelitian ini dilakukan melalui beberapa tahapan sistematis untuk memastikan relevansi dan validitas sumber yang digunakan. Tahap pertama adalah identifikasi literatur menggunakan kata kunci seperti “keamanan transaksi elektronik”, “perlindungan data pribadi”, “e-commerce”, dan “UU PDP” pada basis data jurnal ilmiah dan buku elektronik. Tahap kedua adalah penyaringan (*screening*) berdasarkan kriteria inklusi, yaitu publikasi dalam rentang waktu 2021–2025, relevansi langsung dengan topik penelitian, serta sumber berasal dari jurnal ilmiah terakreditasi,

buku akademik, dan regulasi resmi. Tahap ketiga adalah seleksi akhir (eligibility) dengan mempertimbangkan kualitas metodologis, keterkaitan substansi dengan fokus penelitian, serta ketersediaan teks lengkap. Dari proses tersebut diperoleh sebanyak sumber yang terdiri atas e-book dan artikel jurnal ilmiah yang digunakan dalam analisis.



Gambar 2. Diagram Alur Penelitian

Sumber data yang digunakan dalam artikel ini sepenuhnya berasal dari data sekunder yang dikategorikan ke dalam bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup regulasi otoritatif seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 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 (Izazi et al., 2024). Bahan hukum sekunder diperoleh melalui penelusuran terhadap 27 sumber literatur terpilih yang terdiri dari 5 *e-book* bertema hukum siber, keamanan informasi, dan perlindungan konsumen, serta 22 artikel jurnal ilmiah yang diterbitkan dalam rentang waktu lima tahun terakhir untuk menjaga kebaruan data (Budhijanto, 2024; Wibowo, 2024). Sementara itu, bahan hukum tersier mencakup kamus hukum dan materi referensi lainnya yang berfungsi memberikan penjelasan tambahan terhadap istilah teknis dan yuridis dalam penelitian.

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis kualitatif dengan pendekatan yuridis normatif melalui metode penalaran hukum deduktif. Analisis

dilakukan dengan mengkaji norma-norma hukum yang berlaku, kemudian menghubungkannya dengan fenomena implementasi keamanan transaksi elektronik dalam praktik e-commerce. Proses analisis mencakup interpretasi hukum, sinkronisasi peraturan perundang-undangan, serta penarikan kesimpulan dari norma umum menuju penerapan khusus dalam perlindungan data pribadi konsumen. Pendekatan ini memungkinkan peneliti untuk menilai sejauh mana efektivitas regulasi seperti UU PDP dan UU ITE dalam menjawab tantangan keamanan data di era digital.

Hasil

Berdasarkan sintesis terhadap 27 sumber literatur yang dianalisis, penelitian ini mengidentifikasi tiga temuan utama terkait keterkaitan antara keamanan transaksi elektronik, implementasi UU Pelindungan Data Pribadi (UU PDP), dan kepercayaan konsumen dalam ekosistem *e-commerce* di Indonesia.

Pertama, dari aspek infrastruktur keamanan teknis, hasil kajian menunjukkan bahwa penerapan enkripsi data, tanda tangan digital, *Intrusion Detection System* (IDS), dan pengujian keamanan aplikasi melalui *Dynamic Application Security Testing* (DAST) merupakan lapisan pertahanan pertama yang paling banyak digunakan platform *e-commerce* besar seperti Shopee, TikTok Shop, dan Facebook Marketplace untuk mencegah kebocoran data. Ditemukan pula bahwa keamanan sistem pembayaran digital seperti QRIS turut bergantung pada infrastruktur pembayaran nasional, bukan semata pada sistem internal platform, dan bahwa faktor literasi digital pengguna memengaruhi efektivitas lapisan keamanan tersebut.

Kedua, dari aspek regulasi, hasil analisis normatif menunjukkan bahwa UU PDP dan UU ITE bersama-sama membentuk kerangka akuntabilitas ganda bagi penyelenggara sistem elektronik, dengan UU PDP menetapkan prinsip akuntabilitas ketat (*strict accountability*) yang mewajibkan pengendali data bertanggung jawab atas kebocoran data tanpa perlu membuktikan kesalahan pihak ketiga. Namun demikian, ditemukan bahwa efektivitas kedua regulasi tersebut masih dibatasi oleh belum terbentuknya lembaga pengawas independen yang memiliki kewenangan otoritatif untuk mengawasi sirkulasi data pribadi di sektor ekonomi digital.

Ketiga, dari aspek kepercayaan konsumen, hasil sintesis literatur menunjukkan adanya korelasi antara kekuatan sistem keamanan transaksi dengan tingkat loyalitas konsumen pada platform digital seperti Lazada dan TikTok Shop, sementara insiden kebocoran data secara konsisten berasosiasi dengan penurunan kepercayaan dan reputasi platform. Selain itu, ditemukan bahwa transparansi tata kelola data dan penerapan prinsip etika bisnis oleh pelaku usaha menjadi variabel pendukung yang memperkuat persepsi keamanan di mata konsumen, meskipun rendahnya kesadaran hukum masyarakat terhadap hak atas data pribadi tetap menjadi kendala yang berulang ditemukan di berbagai sumber yang dikaji.

Secara keseluruhan, temuan-temuan tersebut menegaskan adanya tiga pilar yang saling terhubung dalam ekosistem *e-commerce* Indonesia, yaitu kekuatan infrastruktur

keamanan teknis, kepastian kerangka regulasi perlindungan data, dan tingkat kepercayaan konsumen yang selanjutnya akan diuraikan keterkaitan dan implikasinya pada bagian Pembahasan.

Pembahasan

Infrastruktur Keamanan Transaksi Elektronik sebagai Preventif Kebocoran Data

Keamanan transaksi elektronik dalam ekosistem *e-commerce* merupakan determinan utama yang tidak hanya berfungsi sebagai aspek teknis, tetapi juga sebagai fondasi normatif dalam menjamin perlindungan data pribadi konsumen. Implementasi sistem keamanan berlapis seperti enkripsi data, *digital signature*, serta *Intrusion Detection System* (IDS) menunjukkan bahwa perlindungan data tidak dapat dilepaskan dari kualitas arsitektur keamanan sistem elektronik. Hal ini sejalan dengan pandangan Putra & Toresa (2021) yang menegaskan bahwa keamanan informasi merupakan elemen fundamental dalam menjaga integritas sistem digital.

Temuan dalam penelitian ini memperkuat studi Wibowo (2024) yang menyatakan bahwa keamanan informasi bukan sekadar elemen teknis pendukung, melainkan instrumen utama dalam menjamin keberlangsungan aktivitas ekonomi digital. Namun demikian, berbeda dengan pendekatan tersebut yang cenderung bersifat teknis, penelitian ini menegaskan bahwa keamanan transaksi elektronik juga memiliki dimensi yuridis karena berkaitan langsung dengan tanggung jawab hukum penyelenggara sistem elektronik berdasarkan UU ITE dan UU PDP. Kebaruan analisis dalam bagian ini terletak pada penggunaan metode *Dynamic Application Security Testing* (DAST) sebagai pendekatan evaluasi keamanan yang bersifat preventif dan berkelanjutan. Studi Lubis et al. (2025) menunjukkan bahwa platform dengan pengujian keamanan yang konsisten memiliki tingkat kerentanan lebih rendah dibandingkan platform yang tidak melakukan pengujian berkala. Dalam konteks ini, penelitian ini memperluas temuan tersebut dengan menegaskan bahwa kegagalan dalam menerapkan pengujian keamanan tidak hanya berdampak pada aspek teknis, tetapi juga berimplikasi pada pelanggaran kewajiban hukum perlindungan data pribadi.

Selain itu, sistem pembayaran digital seperti QRIS memperlihatkan bahwa keamanan transaksi tidak hanya bergantung pada sistem platform *e-commerce*, tetapi juga pada infrastruktur pembayaran nasional. Meskipun teknologi enkripsi dan autentikasi telah meningkatkan keamanan transaksi, Kristanty (2024) menunjukkan bahwa faktor manusia seperti rendahnya literasi digital tetap menjadi titik lemah dalam sistem perlindungan data. Dengan demikian, keamanan transaksi elektronik tidak dapat dipahami secara parsial, melainkan harus dilihat sebagai sistem yang melibatkan teknologi, manusia, dan regulasi secara simultan. Selanjutnya, keberadaan *digital signature* memberikan legitimasi hukum terhadap keabsahan transaksi elektronik sebagaimana ditegaskan oleh Susilowati et al. (2025). Hal ini menunjukkan adanya integrasi antara aspek teknologi dan kepastian hukum, di mana validitas data tidak hanya ditentukan oleh sistem teknis, tetapi juga oleh pengakuan hukum negara. Oleh karena itu, sinkronisasi antara keamanan teknis dan kepastian hukum

menjadi elemen penting dalam mencegah kebocoran data pribadi secara sistemik.

Secara konseptual, temuan ini menunjukkan bahwa keamanan transaksi elektronik tidak hanya berfungsi sebagai lapisan perlindungan teknis, tetapi juga sebagai prasyarat hukum dalam menjamin efektivitas perlindungan data pribadi. Dengan demikian, kegagalan sistem keamanan tidak hanya bersifat teknis, tetapi juga dapat dikategorikan sebagai bentuk kelalaian hukum (*legal negligence*) dalam penyelenggaraan sistem elektronik.

Urgensi Regulasi dan Tanggung Jawab Marketplace dalam Pelindungan Data Pribadi

Pelindungan data pribadi konsumen di Indonesia memasuki era baru dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Regulasi ini memberikan kerangka hukum yang lebih tegas mengenai hak-hak subjek data dan kewajiban bagi pengendali data dalam mengelola informasi konsumen secara bertanggung jawab (Budhijanto, 2024). Analisis menunjukkan bahwa UU PDP, bersama dengan UU ITE, menciptakan standar akuntabilitas bagi pihak *marketplace* untuk menjamin keamanan sistem elektroniknya (Gustryan & Hoesein, 2025). Namun, efektivitas regulasi ini masih sangat bergantung pada pembentukan lembaga pengawas independen yang memiliki kewenangan otoritatif untuk memantau sirkulasi data pribadi di sektor ekonomi digital (Matheus & Gunadi, 2024).

Penguatan perlindungan data pribadi di Indonesia semakin memperoleh dasar hukum yang kuat dengan disahkannya UU PDP. Regulasi ini menegaskan hak subjek data serta kewajiban pengendali data dalam menjaga keamanan informasi pribadi konsumen (Budhijanto, 2024). Dalam kerangka hukum digital, UU PDP bersama UU ITE membentuk sistem akuntabilitas ganda yang mewajibkan penyelenggara sistem elektronik untuk menjamin keamanan data secara menyeluruh (Gustryan & Hoesein, 2025).

Namun demikian, jika dibandingkan dengan praktik implementasi di lapangan, efektivitas regulasi masih menghadapi tantangan serius, terutama terkait lemahnya mekanisme pengawasan independen. Matheus & Gunadi (2024) menekankan bahwa tanpa lembaga pengawas yang memiliki otoritas kuat, UU PDP berpotensi tidak berjalan optimal dalam penegakan hukum. Kondisi ini menunjukkan adanya kesenjangan antara *law in the books* dan *law in action* dalam perlindungan data pribadi di sektor e-commerce.

Dari perspektif tanggung jawab hukum, marketplace memiliki kewajiban untuk menjamin keamanan data pengguna secara menyeluruh. Dalam kerangka UU PDP, pendekatan tanggung jawab cenderung mengarah pada prinsip akuntabilitas ketat (*strict accountability*), yang menuntut pengendali data bertanggung jawab atas setiap kebocoran data tanpa harus membuktikan kesalahan pihak ketiga (Budiandru & Hidayat, 2025). Namun, dalam praktiknya, posisi konsumen masih lemah akibat asimetri informasi dan kesulitan pembuktian kerugian digital (Purwito, 2023).

Jika dibandingkan dengan penelitian Maharani & Prakoso (2024), perlindungan data konsumen masih sering dipandang sebagai kewajiban administratif, bukan sebagai

kewajiban hukum yang bersifat preventif dan melekat pada desain sistem. Oleh karena itu, prinsip *privacy by design* menjadi relevan untuk memastikan bahwa perlindungan data sudah diintegrasikan sejak tahap awal pengembangan sistem, bukan hanya sebagai respons setelah terjadinya pelanggaran.

Tabel berikut menunjukkan perbandingan instrumen hukum yang mengatur perlindungan data dan konsumen di Indonesia:

Tabel 2. Perbandingan Fokus Regulasi Perlindungan Data dan Konsumen di Indonesia

Instrumen Hukum	Fokus Utama Perlindungan	Sifat Tanggung Jawab
UU Perlindungan Konsumen (No. 8/1999)	Hak atas keamanan, kenyamanan, dan ganti rugi produk/jasa.	Tanggung jawab pelaku usaha atas cacat produk/layanan.
UU ITE (No. 11/2008 jo. UU No. 1/2024)	Integritas transaksi elektronik dan keamanan sistem informasi.	Penyelenggara sistem elektronik wajib menjaga keamanan data.
UU PDP (No. 27/2022)	Tata kelola, hak subjek data, dan kerahasiaan data pribadi.	Akuntabilitas pengendali data dan kewajiban pengamanan.
PP No. 80/2019	Standar perdagangan melalui sistem elektronik (e-commerce).	Efektivitas perlindungan konsumen dalam transaksi digital.

Sumber: Analisis Peneliti (2026), diolah dari berbagai sumber (Budhijanto, 2024; Izazi et al., 2024; Priliasari, 2023).

Secara normatif, tabel tersebut menunjukkan bahwa meskipun regulasi telah tersedia secara komprehensif, tantangan utama terletak pada sinkronisasi implementasi antarinstrumen hukum. Hal ini diperkuat oleh Halim et al. (2024) yang menyatakan bahwa lemahnya penegakan hukum dapat mengurangi efektivitas perlindungan konsumen dalam ekosistem digital. Dengan demikian, regulasi yang kuat harus diiringi dengan mekanisme pengawasan yang efektif agar tidak menjadi *law without enforcement*.

Dampak Keamanan dan Pelindungan Data terhadap Kepercayaan Konsumen

Keamanan transaksi elektronik dan perlindungan data pribadi memiliki peran signifikan dalam membentuk *consumer trust* sebagai variabel kunci dalam keberlanjutan ekosistem e-commerce. Kepercayaan konsumen tidak hanya dibentuk oleh kualitas layanan, tetapi juga oleh persepsi keamanan dalam pengelolaan data pribadi (Siallagan & Wasiman, 2025). Hasil analisis menunjukkan bahwa sistem keamanan yang kuat berkorelasi dengan meningkatnya loyalitas konsumen, sedangkan kebocoran data berdampak langsung pada penurunan kepercayaan dan reputasi platform (Handayani et al., 2024). Jika dibandingkan dengan Sari (2025), fenomena kebocoran data yang berulang tidak hanya menimbulkan kerugian ekonomi, tetapi juga menciptakan krisis kepercayaan

jangka panjang terhadap ekosistem digital.

Selain itu, etika bisnis menjadi faktor penting dalam memperkuat hubungan antara teknologi dan kepercayaan konsumen. Implementasi transparansi dalam pengelolaan data menunjukkan bahwa perusahaan yang mematuhi prinsip etika cenderung lebih dipercaya oleh pengguna dibandingkan perusahaan yang hanya berorientasi pada keuntungan jangka pendek (Pernando et al., 2024). Dalam konteks ini, pelanggaran terhadap prinsip etika dapat dianggap sebagai pelanggaran terhadap ekspektasi normatif masyarakat digital. Namun, rendahnya literasi digital masyarakat menjadi faktor penghambat dalam optimalisasi perlindungan data pribadi. Banyak pengguna yang menyetujui penggunaan data tanpa memahami konsekuensi hukumnya (Putra et al., 2023). Hal ini menunjukkan adanya kesenjangan antara keberadaan regulasi dan pemahaman praktis masyarakat terhadap hak-hak digital mereka (Zahwani & Nasution, 2023).

Dengan demikian, dapat disintesis bahwa keberlanjutan ekosistem e-commerce sangat bergantung pada tiga faktor utama yang saling terkait, yaitu keamanan teknologi, kepastian hukum, dan etika bisnis. Ketiga faktor tersebut secara kolektif membentuk fondasi kepercayaan digital yang menentukan keberhasilan ekonomi digital di Indonesia.

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa keamanan transaksi elektronik berfungsi sebagai benteng pertahanan teknis utama dalam mencegah kebocoran data pribadi konsumen pada ekosistem perdagangan elektronik di Indonesia. Penerapan teknologi keamanan yang kredibel seperti enkripsi data, tanda tangan digital, hingga pengujian kerentanan berkala berbasis pengujian keamanan aplikasi secara dinamis bukan sekadar kebutuhan operasional internal pasar digital, melainkan prasyarat teknis preventif yang menjamin integritas, kerahasiaan, dan validitas transaksi secara menyeluruh.

Secara yuridis, Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang bersinergi dengan Undang Undang Informasi dan Transaksi Elektronik serta Undang Undang Perlindungan Konsumen telah memberikan landasan kepastian hukum yang kokoh. Kerangka regulasi ini secara tegas menetapkan standar akuntabilitas ketat bagi penyelenggara sistem elektronik dan pengendali data, di mana kegagalan dalam menjaga keamanan data pribadi konsumen dapat dikategorikan sebagai kelalaian hukum dalam penyelenggaraan sistem elektronik.

Meskipun demikian, efektivitas penegakan regulasi tersebut dalam praktik di lapangan masih menghadapi berbagai tantangan nyata. Hambatan utama yang ditemukan meliputi durasi transisi pembentukan lembaga pengawas data pribadi independen yang belum optimal, kendala asimetri informasi antara pelaku usaha dan konsumen, serta masih rendahnya tingkat kesadaran dan literasi hukum masyarakat terhadap hak atas perlindungan data pribadinya.

Penelitian ini juga mengonfirmasi adanya korelasi positif dan hubungan kausalitas yang kuat antara keandalan sistem keamanan transaksi, perlindungan data pribadi, dan

pembentukan kepercayaan konsumen. Kegagalan sistemik dalam menjaga keamanan data terbukti berimplikasi langsung pada degradasi reputasi platform dan penurunan tingkat partisipasi masyarakat dalam ekonomi digital, sedangkan transparansi tata kelola data serta penerapan etika bisnis terbukti mampu memperkuat loyalitas konsumen secara berkelanjutan.

Secara akademis, penelitian ini berhasil mengisi kesenjangan kajian dengan mensintesis dimensi keamanan siber dan instrumen hukum bisnis digital ke dalam satu kerangka analisis yang komprehensif. Secara praktis, temuan ini memberikan rekomendasi strategis bagi pemerintah untuk segera mengakselerasi operasionalisasi lembaga pengawas data pribadi, serta mendorong para penyelenggara perdagangan elektronik untuk menyelaraskan arsitektur teknologi keamanannya dengan prinsip tata kelola data yang akuntabel demi menyokong pertumbuhan ekonomi digital nasional.

Referensi

- Budiandru, & Hidayat, R. S. (2025). Tanggung jawab hukum marketplace terhadap kebocoran data pribadi pengguna dalam perspektif UU ITE dan UU Perlindungan Data Pribadi. *Journal of Artificial Intelligence and Digital Business (RIGGS)*, 4(3), 7738–7743.
- Budhijanto, D. (2024). *Hukum perlindungan data pribadi dan data nasional*. Logoz Publishing.
- Gustryan, M., & Hoesein, Z. A. (2025). Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam perlindungan data dan privasi di era ekonomi digital. *Jurnal Minfo Polgan*, 14(2).
- Halim, S., Franciska, W., & Noor, Z. Z. (2024). Penegakan hukum bagi perusahaan yang melakukan transaksi elektronik melalui e-commerce sebagai perlindungan hukum terhadap pengguna. *Sinergi: Jurnal Riset Ilmiah*, 1(8), 599–609.
- Handayani, A., Eprianto, I., Fauzi, A., Al Gifari, M. F. A., Wicaksono, H. D., Nyngrum, K. W., et al. (2024). Manajemen sekuriti yang efektif untuk meningkatkan kepercayaan pelanggan platform e-commerce Lazada. *Orbit: Jurnal Ilmu Multidisiplin*, 1(2).
- Handayani, N. L. P., & Soeparan, P. F. (2022). Peran sistem pembayaran digital dalam revitalisasi UMKM. *Jurnal Mahasiswa*, 4(3), 238–250.
- Izazi, F. S., Sajena, P., Kirana, R. S., & Marsaulina, K. (2024). Perlindungan hukum terhadap konsumen dalam transaksi e-commerce melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Peraturan Pemerintah (PP) Nomor 80 Tahun 2019 tentang Perdagangan melalui Sistem Elektronik. *Leuser: Jurnal Hukum Nusantara*, 1(2), 8–14.
- Kim, M. T., Jacob, Y. M. Y., & Dju Bire, C. M. (2025). Perlindungan data pribadi pada

platform digital pinjaman online ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Studi kasus di Kota Kupang, NTT). *Artemis Law Journal*, 2(2).

Kristanty, D. N. (2024). Tren dan tantangan keamanan bertransaksi dengan QRIS dalam era transformasi sistem pembayaran digital. *Jurnal Syntax Admiration*, 5(10), 3922–3932.

Lubis, D. L., Nisa, F., & Ulya, A. (2025). Analisis perbandingan keamanan aplikasi web pada platform e-commerce studi kasus: Shopee, TikTok Shop dan Facebook Marketplace menggunakan Dynamic Application Security Testing (DAST). *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(6).

Maharani, R., & Prakoso, A. L. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *Jurnal Hukum*.

Matheus, J., & Gunadi, A. (2024). Pembentukan lembaga pengawas perlindungan data pribadi di era ekonomi digital: Kajian perbandingan dengan KPPU. *Justisi*, 10(1).

Menarianti, I., Rahmanto, B. T., Wijayanti, A., Sungkawati, E., Bintari, W. C., Komariyah, E. F., et al. (2024). *E-commerce*. PT Media Penerbit Indonesia.

Pernando, O. R., Berliandes, W., & Juliyani, E. (2024). Penerapan prinsip-prinsip etika bisnis dalam transaksi e-commerce: Membangun kepercayaan konsumen. *Ebisnis Manajemen*, 2(4), 51–59.

Prabowo, M. S., & Sulistianingsih, D. (2026). *Buku ajar perlindungan konsumen dalam era digital: Tantangan dan kebijakan*. PT Media Penerbit Indonesia.

Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, 5(1), 903–913.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce menurut peraturan perundang-undangan di Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).

Purwito, E. (2023). Konsep perlindungan hukum konsumen dan tanggung jawab hukum pelaku usaha terhadap produk gula pasir kadaluarsa di Kota Surabaya. *Dekrit: Jurnal Magister Ilmu Hukum*, 13(1).

Putra, C. A. G., Budiarta, I. N. P., & Ujianti, N. M. P. (2023). Perlindungan hukum terhadap konsumen dalam perspektif kesadaran hukum masyarakat. *Jurnal Konstruksi Hukum*, 4(1), 13–19.

Putra, P. P., & Toresa, D. (2021). *Buku ajar keamanan informasi dan jaringan komputer*. LPPM Universitas Lancang Kuning.

Sari, A. K. (2025). Kebijakan hukum perlindungan konsumen terhadap kebocoran data di platform fintech. *Judge: Jurnal Hukum*, 6(2), 353–360.

Siallagan, D. N. A., & Wasiman. (2025). Pengaruh word of mouth, kualitas produk dan

kepercayaan konsumen terhadap keputusan pembelian pada e-commerce TikTok Shop di Kota Batam. *Akademik: Jurnal Mahasiswa Ekonomi & Bisnis*, 5(3), 1545–1555.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–146.

Susilowati, D. E., Muhtarom, M., & Junaidi, A. (2025). Analisis yuridis keabsahan tanda tangan digital dalam transaksi e-commerce di Indonesia. *Jurnal Serambi Hukum*, 18(1).

Wibowo, A. (2024). *Hukum siber dan keamanan informasi*. Yayasan Prima Agus Teknik.

Zahwani, S. T., & Nasution, M. I. P. (2023). Analisis kesadaran masyarakat terhadap perlindungan data pribadi di era digital. *JOSES: Journal of Sharia Economics Scholar*, 2(2), 105–109.