

ANALISIS SISTEM KEAMANAN DAN KEBIJAKAN PRIVASI DATA PADA PLATFORM E-COMMERCE : STUDI PERSEPSI KONSUMEN DI KOTA BINJAI

Endri Does, M. fikri Akbar¹; Selfiana Lubis²; Dinda Rahmayani³

Abstrak

Pertumbuhan e-commerce di Indonesia menciptakan kebutuhan mendesak akan sistem keamanan yang handal dan kebijakan privasi data yang transparan untuk melindungi konsumen. Penelitian ini menganalisis implementasi sistem keamanan dan kebijakan privasi data pada lima platform e-commerce terpopuler di Indonesia dengan mengeksplorasi persepsi konsumen di Kota Binjai, Sumatera Utara. Metode penelitian menggunakan pendekatan kualitatif deskriptif dengan teknik analisis dokumen dan observasi sistematis terhadap fitur keamanan serta kebijakan privasi yang diterapkan masing-masing platform, dilengkapi dengan wawancara mendalam terhadap 8 konsumen aktif e-commerce di Kota Binjai. Hasil penelitian menunjukkan bahwa kelima platform (Shopee, Tokopedia, Lazada, Bukalapak, dan Blibli) telah mengimplementasikan protokol keamanan dasar seperti SSL/TLS encryption dan autentikasi multi-faktor, namun terdapat variasi signifikan dalam transparansi kebijakan privasi data dan mekanisme perlindungan informasi konsumen. Temuan dari perspektif konsumen Binjai mengindikasikan awareness yang masih terbatas terhadap fitur keamanan dan kebijakan privasi, dengan kecenderungan mengandalkan reputasi platform sebagai indikator utama keamanan. Penelitian ini menyimpulkan bahwa integrasi antara sistem keamanan teknis, transparansi kebijakan privasi, dan edukasi konsumen menjadi faktor krusial dalam membangun kepercayaan konsumen terhadap ekosistem e-commerce Indonesia.

Kata Kunci: sistem keamanan; kebijakan privasi; e-commerce; perlindungan data; persepsi konsumen

Abstract

The growth of e-commerce in Indonesia creates an urgent need for reliable security systems and transparent data privacy policies to protect consumers. This research analyzes the implementation of security systems and data privacy policies on five most popular e-commerce platforms in Indonesia by exploring consumer perceptions in Binjai City, North Sumatra. The research method uses a descriptive qualitative approach with document analysis techniques and systematic observation of security features and privacy policies applied by each platform, complemented by

¹ M.fikri Akbar, M.fikriakbar135@gmail.com

² Selfiana Lubis, selfianalubis9@gmail.com

³ Dinda Rahmayani, dindarahmayani2006@gmail.com

*Endri Does

in-depth interviews with 8 active e-commerce consumers in Binjai City. Research results show that all five platforms (Shopee, Tokopedia, Lazada, Bukalapak, and Blibli) have implemented basic security protocols such as SSL/TLS encryption and multi-factor authentication, but there are significant variations in the transparency of data privacy policies and consumer information protection mechanisms. Findings from Binjai consumer perspectives indicate limited awareness of security features and privacy policies, with a tendency to rely on platform reputation as the main security indicator. This research concludes that the integration between technical security systems, privacy policy transparency, and consumer education is a crucial factor in building consumer trust in the Indonesian e-commerce ecosystem.

Keywords: security system; privacy policy; e-commerce; data protection; consumer perception

A. PENDAHULUAN

Transformasi digital telah mengubah lanskap bisnis Indonesia secara fundamental, di mana aktivitas perdagangan kini berpindah dari toko fisik menuju platform elektronik yang terkoneksi secara global. E-commerce sebagai representasi bisnis elektronik modern menghadirkan kemudahan akses pasar tanpa batas geografis, efisiensi operasional, dan kenyamanan transaksi bagi konsumen (Turban et al., 2017). Data Kementerian Komunikasi dan Informatika menunjukkan bahwa nilai transaksi e-commerce Indonesia mencapai ratusan triliun rupiah dengan pertumbuhan signifikan setiap tahunnya, menjadikan Indonesia sebagai pasar digital terbesar di Asia Tenggara.

Namun, pertumbuhan eksponensial e-commerce diiringi oleh meningkatnya ancaman keamanan siber yang mengancam kepercayaan konsumen dan keberlanjutan bisnis digital. Simbolon (2025) mengidentifikasi bahwa ancaman cybercrime di Indonesia terus berkembang dalam frekuensi dan tingkat kecanggihan, mencakup serangan malware, phishing, pencurian identitas, dan kebocoran data yang merugikan jutaan pengguna. Ketergantungan total pada infrastruktur digital menjadikan sistem keamanan sebagai fondasi kritis yang menentukan viabilitas platform e-commerce dalam melindungi data sensitif konsumen.

Aspek kebijakan privasi data menjadi dimensi penting yang belum mendapat perhatian memadai dalam penelitian terdahulu. Mansawan et al. (2025) menekankan bahwa perlindungan hukum terhadap data personal konsumen e-commerce di Indonesia masih menghadapi tantangan implementasi meskipun Undang-Undang Perlindungan Data Pribadi telah disahkan. Transparansi dalam kebijakan privasi, mekanisme pengelolaan data, dan hak konsumen atas informasi pribadi mereka menjadi faktor determinan dalam membangun kepercayaan digital.

Penelitian ini difokuskan pada konteks Kota Binjai, Sumatera Utara, sebagai representasi kota menengah di Indonesia yang mengalami pertumbuhan adopsi e-commerce signifikan. Binjai, dengan populasi sekitar 160 ribu jiwa dan posisi strategis di wilayah metropolitan Medan, memiliki karakteristik demografis yang beragam mencakup kalangan mahasiswa, pelaku usaha, dan masyarakat umum yang semakin aktif bertransaksi melalui platform digital. Pemilihan lokasi Binjai memungkinkan eksplorasi mendalam mengenai bagaimana konsumen di kota menengah mempersepsikan dan merespons sistem keamanan serta kebijakan privasi

yang diterapkan platform e-commerce, memberikan perspektif yang berbeda dari studi yang umumnya fokus pada konsumen metropolitan (Wynn & Olayinka, 2021).

Penelitian ini mengisi gap tersebut dengan menganalisis lima platform e-commerce terpopuler di Indonesia melalui dual perspective: evaluasi teknis terhadap sistem keamanan dan kebijakan privasi platform, serta eksplorasi persepsi dan pengalaman konsumen di Kota Binjai untuk memberikan gambaran empiris mengenai praktik keamanan dan kesenjangan antara security features yang tersedia dengan awareness konsumen lokal.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk: (1) menganalisis implementasi sistem keamanan pada platform e-commerce di Indonesia; (2) mengevaluasi transparansi dan kualitas kebijakan privasi data yang diterapkan; (3) mengeksplorasi persepsi dan pengalaman konsumen Binjai terhadap sistem keamanan dan kebijakan privasi platform e-commerce; (4) mengidentifikasi kesenjangan antara security features yang tersedia dengan pemahaman dan pemanfaatan konsumen; serta (5) merumuskan rekomendasi untuk optimalisasi keamanan dan perlindungan data konsumen di ekosistem e-commerce Indonesia.

B. KAJIAN TEORI

Konsep E-Commerce dan Sistem Keamanan Digital

E-commerce merupakan transaksi bisnis yang dilakukan melalui jaringan internet dan platform digital, mencakup aktivitas jual-beli produk atau jasa, pembayaran elektronik, dan distribusi yang difasilitasi oleh teknologi informasi (Turban et al., 2017). Berbeda dengan e-business yang lebih luas mencakup seluruh proses bisnis internal, e-commerce fokus pada transaksi komersial antara organisasi dengan konsumen (B2C), antar organisasi (B2B), atau antar konsumen (C2C). Platform e-commerce modern mengintegrasikan berbagai teknologi seperti mobile applications, payment gateway, logistics tracking, dan customer relationship management untuk menciptakan pengalaman berbelanja yang seamless.

Sistem keamanan digital dalam konteks e-commerce merujuk pada serangkaian mekanisme teknis dan prosedural yang dirancang untuk melindungi integritas data, kerahasiaan informasi, dan ketersediaan layanan dari berbagai ancaman siber (Whitman & Mattord, 2021). Prinsip dasar keamanan informasi yang dikenal sebagai CIA Triad mencakup Confidentiality (memastikan data hanya diakses oleh pihak yang berwenang), Integrity (menjaga akurasi dan kelengkapan data dari modifikasi tidak sah), dan Availability (memastikan sistem dan data dapat diakses saat dibutuhkan). Implementasi sistem keamanan e-commerce memerlukan pendekatan berlapis yang mengintegrasikan teknologi enkripsi, autentikasi, firewall, dan monitoring real-time.

Ancaman Keamanan dalam Ekosistem E-Commerce

Aslan et al. (2023) mengklasifikasikan ancaman keamanan e-commerce ke dalam beberapa kategori utama. Pertama, serangan malware dan ransomware yang menginfeksi sistem untuk mencuri data atau mengenkripsi informasi dengan tujuan memeras korban. Kedua, phishing attack yang memanfaatkan rekayasa sosial untuk menipu pengguna agar memberikan kredensial login atau informasi kartu kredit melalui email atau website palsu. Ketiga, Distributed Denial-of-Service (DDoS) attack yang membanjiri server dengan traffic palsu hingga layanan menjadi tidak dapat diakses oleh pengguna legitimate (Mishra et al., 2024).

Ancaman lain mencakup SQL injection yang mengeksploitasi kerentanan aplikasi web untuk mengakses database backend, man-in-the-middle attack yang menyadap komunikasi antara pengguna dan server, serta pencurian identitas yang menggunakan data personal curian untuk melakukan transaksi fraud. Simbolon (2025) mencatat bahwa konteks Indonesia menghadapi tantangan tambahan berupa literasi keamanan digital yang masih rendah di kalangan konsumen, memudahkan pelaku cybercrime melancarkan serangan berbasis social engineering.

Solusi Keamanan E-Commerce Kontemporer

Evans (2022) menekankan bahwa pendekatan keamanan e-commerce harus bersifat holistik dengan mengintegrasikan teknologi, kebijakan, dan faktor manusia. Enkripsi menggunakan protokol SSL/TLS (Secure Sockets Layer/Transport Layer Security) menjadi standar fundamental untuk melindungi data selama transmisi antara browser pengguna dan server platform. Sertifikat SSL yang valid tidak hanya mengenkripsi komunikasi tetapi juga memberikan verifikasi identitas website, membantu pengguna membedakan platform legitimate dari phishing site.

Autentikasi multi-faktor (MFA) secara signifikan meningkatkan keamanan akun dengan mewajibkan verifikasi menggunakan kombinasi password, one-time password (OTP) yang dikirim via SMS atau email, serta biometric authentication seperti fingerprint atau facial recognition (Whitman & Mattord, 2021). Teknologi emerging seperti artificial intelligence dan machine learning semakin banyak dimanfaatkan untuk fraud detection dengan menganalisis pola transaksi dan perilaku pengguna untuk mengidentifikasi aktivitas mencurigakan secara real-time (Katiyar et al., 2024). Blockchain technology menawarkan potensi untuk meningkatkan transparansi dan immutability transaction records, mengurangi risiko fraud dan meningkatkan accountability (Choo et al., 2020).

Kebijakan Privasi Data dan Perlindungan Konsumen

Kebijakan privasi data merupakan dokumen yang menjelaskan bagaimana organisasi mengumpulkan, menyimpan, menggunakan, dan membagikan informasi personal pengguna. Mansawan et al. (2025) menjelaskan bahwa dalam konteks hukum Indonesia, perlindungan data personal konsumen e-commerce diatur oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengadopsi prinsip-prinsip General Data Protection Regulation (GDPR). Platform e-commerce wajib menerapkan prinsip lawfulness, fairness, transparency dalam pemrosesan data, serta memberikan hak kepada konsumen untuk mengakses, memperbaiki, menghapus, dan memindahkan data personal mereka.

Dewantara et al. (2024) mengidentifikasi bahwa transparansi kebijakan privasi menjadi faktor krusial dalam membangun kepercayaan konsumen terhadap platform marketplace. Kebijakan yang jelas harus mencakup informasi mengenai jenis data yang dikumpulkan, tujuan pengumpulan, pihak ketiga yang menerima akses data, durasi penyimpanan, serta mekanisme keamanan yang diterapkan untuk melindungi data dari akses tidak sah. Aksesibilitas kebijakan privasi, penggunaan bahasa yang mudah dipahami, dan notifikasi perubahan kebijakan merupakan aspek penting yang mencerminkan komitmen platform terhadap hak konsumen.

Governance dan Risk Management Keamanan Digital

Malik (2025) menekankan pentingnya cybersecurity governance sebagai framework strategis yang mengintegrasikan keamanan informasi dengan tujuan bisnis organisasi. Governance yang efektif mencakup penetapan kebijakan keamanan,

alokasi sumber daya, assignment tanggung jawab, serta monitoring dan audit berkala untuk memastikan compliance terhadap standar dan regulasi. Risk management melibatkan identifikasi aset kritis, assessment terhadap ancaman dan kerentanan, evaluasi dampak potensial, serta implementasi kontrol untuk mitigasi risiko hingga tingkat yang acceptable.

Alexander et al. (2020) menjelaskan bahwa information security management principles mencakup pengembangan security policy yang komprehensif, implementasi access control mechanisms, incident response planning, business continuity management, serta continuous improvement melalui lessons learned dari insiden keamanan. Integrasi antara technical controls (enkripsi, firewall, antivirus), administrative controls (kebijakan, prosedur, training), dan physical controls (keamanan data center, backup systems) menciptakan defense in depth yang meminimalkan risiko successful attack.

Peran Analytics dalam E-Commerce Security

Mubarok et al. (2025) mendemonstrasikan bahwa big data analytics dan machine learning memberikan kontribusi signifikan dalam meningkatkan keamanan e-commerce melalui kemampuan mendeteksi anomali dan fraud dalam skala besar. Algoritma machine learning dapat dilatih menggunakan historical transaction data untuk mengidentifikasi pola normal dan mengenali deviasi yang mengindikasikan aktivitas suspicious seperti transaksi fraud, account takeover, atau bot attack. Real-time analytics memungkinkan platform untuk mengambil tindakan preventif segera seperti memblokir transaksi mencurigakan atau meminta verifikasi tambahan sebelum kerugian terjadi.

C. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi dokumen, observasi sistematis, dan wawancara mendalam untuk menganalisis sistem keamanan dan kebijakan privasi data pada platform e-commerce di Indonesia. Desain penelitian ini dipilih karena memungkinkan eksplorasi mendalam terhadap praktik keamanan dan transparansi kebijakan yang diterapkan platform, serta pemahaman komprehensif mengenai persepsi dan pengalaman konsumen tanpa memerlukan intervensi atau manipulasi variabel.

Objek penelitian mencakup lima platform e-commerce terpopuler di Indonesia berdasarkan jumlah pengguna aktif dan volume transaksi, yaitu: (1) Shopee; (2) Tokopedia; (3) Lazada; (4) Bukalapak; dan (5) Blibli. Pemilihan kelima platform ini didasarkan pada market dominance dan representasi model bisnis yang berbeda, dari platform marketplace murni hingga platform dengan model hybrid yang mengintegrasikan seller sendiri dan third-party merchants. Penelitian ini dilaksanakan di Kota Binjai, Sumatera Utara, dengan subjek penelitian konsumen aktif e-commerce yang berdomisili di wilayah Binjai.

Teknik pengumpulan data dilakukan melalui tiga metode utama. Pertama, observasi sistematis terhadap fitur keamanan yang terlihat pada website dan aplikasi mobile masing-masing platform, mencakup: (a) implementasi protokol HTTPS/SSL dengan verifikasi sertifikat keamanan; (b) metode autentikasi yang tersedia (password, OTP, biometric, two-factor authentication); (c) opsi payment gateway dan security features pada proses checkout; (d) badge atau indikator keamanan yang ditampilkan; serta (e) fitur keamanan tambahan seperti secure payment guarantee atau buyer protection program. Observasi dilakukan pada periode September-

Oktober 2025 melalui multiple access points termasuk website desktop, mobile website, dan aplikasi mobile untuk memastikan comprehensiveness data.

Kedua, analisis dokumen kebijakan privasi yang dipublikasikan pada website resmi masing-masing platform. Analisis dilakukan terhadap: (a) aksesibilitas kebijakan privasi (kemudahan menemukan dan membaca dokumen); (b) kelengkapan informasi mengenai jenis data yang dikumpulkan; (c) transparansi tujuan penggunaan data; (d) disclosure mengenai data sharing dengan pihak ketiga; (e) penjelasan tentang security measures untuk melindungi data; (f) informasi tentang hak konsumen atas data personal; serta (g) mekanisme untuk mengajukan pertanyaan atau keluhan terkait privasi. Dokumen kebijakan privasi yang dianalisis merupakan versi yang berlaku pada periode penelitian dengan memperhatikan tanggal pembaruan terakhir untuk memastikan currency informasi.

Ketiga, wawancara mendalam dengan 8 informan yang merupakan konsumen aktif e-commerce di Kota Binjai. Pemilihan informan menggunakan teknik purposive sampling dengan kriteria: (a) berdomisili di Kota Binjai minimal 1 tahun; (b) pengguna aktif e-commerce dengan frekuensi transaksi minimal 2 kali per bulan dalam 6 bulan terakhir; (c) memiliki pengalaman bertransaksi minimal di 2 platform berbeda dari kelima platform yang diteliti; serta (d) bersedia memberikan informasi secara mendalam mengenai pengalaman dan persepsi mereka. Wawancara dilakukan secara semi-terstruktur dengan panduan pertanyaan yang mencakup: awareness terhadap fitur keamanan platform, pemahaman tentang kebijakan privasi data, pengalaman terkait keamanan transaksi, faktor yang mempengaruhi kepercayaan terhadap platform, serta perilaku protective dalam bertransaksi online. Wawancara dilaksanakan selama periode Oktober-November 2025 dengan durasi 30-45 menit per informan, dilakukan secara tatap muka di lokasi yang nyaman bagi informan dengan tetap memperhatikan etika penelitian termasuk informed consent dan confidentiality.

Teknik analisis data menggunakan content analysis dengan pendekatan komparatif untuk data dokumen dan observasi, serta thematic analysis untuk data wawancara. Tahap pertama melakukan coding terhadap fitur keamanan dan elemen kebijakan privasi yang ditemukan pada setiap platform berdasarkan framework yang diadaptasi dari Whitman dan Mattord (2021) serta Tavares, Mishra, Kumar, Zaman, dan Khari (2019). Tahap kedua melakukan kategorisasi tingkat implementasi keamanan dan transparansi privasi menggunakan skala: komprehensif (menerapkan semua aspek dengan detail), memadai (menerapkan sebagian besar aspek esensial), dan terbatas (menerapkan aspek minimum). Tahap ketiga melakukan analisis komparatif untuk mengidentifikasi pola, kesamaan, dan perbedaan antar platform, serta mengeksplorasi hubungan antara sistem keamanan teknis dengan transparansi kebijakan privasi. Data wawancara dianalisis menggunakan thematic analysis dengan tahapan: (1) transkripsi verbatim seluruh hasil wawancara; (2) coding untuk mengidentifikasi tema dan pola yang muncul dari narasi informan; (3) kategorisasi tema berdasarkan dimensi awareness, perception, experience, dan behavior terkait keamanan dan privasi; serta (4) interpretasi untuk memahami kesenjangan antara security features platform dengan pemahaman dan pemanfaatan konsumen (Wynn & Olayinka, 2021).

Validasi data dilakukan melalui triangulasi sumber dengan melakukan observasi pada multiple access points (website desktop, mobile website, dan aplikasi mobile) serta verifikasi silang informasi yang ditemukan dengan dokumentasi resmi platform dan laporan audit keamanan yang tersedia publik. Triangulasi metode

dilakukan dengan membandingkan temuan dari analisis dokumen, observasi fitur, dan hasil wawancara untuk mengidentifikasi konvergensi atau divergensi data. Keterbatasan penelitian terletak pada sifat observasional yang hanya dapat mengakses fitur keamanan yang visible bagi pengguna umum tanpa dapat mengevaluasi infrastruktur backend dan security measures internal yang diterapkan platform, serta generalisasi temuan dari perspektif konsumen Binjai yang mungkin tidak sepenuhnya mewakili konsumen di wilayah lain dengan karakteristik demografis berbeda.

D. HASIL DAN PEMBAHASAN

1. Implementasi Sistem Keamanan pada Platform E-Commerce Indonesia

Hasil observasi menunjukkan bahwa kelima platform e-commerce telah mengimplementasikan protokol keamanan dasar yang menjadi standar industri. Semua platform menerapkan HTTPS dengan sertifikat SSL/TLS yang valid, ditandai dengan ikon gembok pada address bar browser dan penggunaan protokol secure pada seluruh halaman termasuk proses login dan checkout. Implementasi SSL encryption ini memastikan bahwa data yang ditransmisikan antara perangkat pengguna dan server platform terenkripsi, melindungi informasi sensitif seperti kredensial login dan detail pembayaran dari intersepsi pihak ketiga (Whitman & Mattord, 2021).

Tabel 1
Perbandingan Fitur Keamanan Platform E-Commerce

Platform	SSL/HTTPS	Autentikasi MFA	Payment Security	Security Badge	Additional Protection
Shopee	✓	OTP SMS, Email, Biometric	Escrow, Multiple gateway	Shopee Guarantee	Buyer protection
Tokopedia	✓	2FA, OTP, Biometric	Escrow, Certified gateway	Trust badge	Insurance option
Lazada	✓	OTP SMS, Email	Secure payment gateway	Secure badge	Return guarantee
Bukalapak	✓	OTP SMS, PIN	Escrow system	Verified seller	OpenSecurity
Bibli	✓	OTP, 2FA optional	PCI DSS compliant	Security icon	Official guarantee

Sumber: Data observasi platform (2025)

Aspek autentikasi menunjukkan variasi implementasi di antara platform. Tokopedia dan Bibli menyediakan opsi two-factor authentication (2FA) yang dapat diaktifkan pengguna untuk menambah lapisan keamanan pada akun mereka, sementara platform lain mengandalkan one-time password (OTP) yang dikirim via SMS atau email sebagai verifikasi transaksi penting. Shopee dan Tokopedia telah mengintegrasikan biometric authentication menggunakan fingerprint atau facial recognition pada aplikasi mobile mereka, memanfaatkan security features bawaan

smartphone untuk mempermudah sekaligus meningkatkan keamanan akses (Evans, 2022).

Sistem pembayaran pada kelima platform menerapkan mekanisme escrow yang menahan dana transaksi hingga pembeli mengkonfirmasi penerimaan barang sesuai pesanan. Mekanisme ini melindungi kedua belah pihak dari fraud, memastikan seller tidak kehilangan barang tanpa pembayaran dan buyer tidak kehilangan uang tanpa menerima barang yang dipesan. Platform juga berintegrasi dengan payment gateway tersertifikasi yang comply dengan Payment Card Industry Data Security Standard (PCI DSS), memastikan bahwa informasi kartu kredit diproses sesuai standar keamanan internasional tanpa disimpan langsung oleh platform.

Fitur keamanan tambahan seperti buyer protection program yang ditawarkan Shopee Guarantee, buyer insurance Tokopedia, dan BukaPengaman Bukalapak memberikan jaminan pengembalian dana jika terjadi masalah dengan transaksi. Badge atau indikator keamanan seperti "Verified Seller", "Official Store", atau "Trusted Merchant" membantu konsumen mengidentifikasi penjual yang telah melalui verifikasi platform, mengurangi risiko bertransaksi dengan seller fraud (Dewantara et al., 2024).

Namun, hasil observasi juga mengidentifikasi area yang memerlukan perbaikan. Penerapan MFA masih bersifat optional pada sebagian platform dan adoption rate di kalangan pengguna masih rendah karena kurangnya edukasi tentang pentingnya security features tambahan. Monitoring real-time untuk mendeteksi aktivitas mencurigakan belum transparan bagi pengguna, dan mekanisme notifikasi untuk unusual login atau transaction attempts masih inkonsisten antar platform (Aslan et al., 2023).

2. Evaluasi Kebijakan Privasi Data Platform E-Commerce

Analisis dokumen kebijakan privasi menunjukkan bahwa kelima platform telah mempublikasikan privacy policy yang mencakup aspek-aspek utama sebagaimana diwajibkan regulasi. Namun, terdapat variasi signifikan dalam hal transparansi, kelengkapan informasi, dan aksesibilitas dokumen bagi pengguna awam.

Tabel 2
Evaluasi Transparansi Kebijakan Privasi Data

Aspek Kebijakan	Shopee	Tokopedia	Lazada	Bukalapak	Blibli
Aksesibilitas dokumen	Mudah	Sangat mudah	Mudah	Cukup mudah	Mudah
Kelengkapan info data	Lengkap	Sangat lengkap	Lengkap	Cukup lengkap	Lengkap
Transparansi penggunaan	Jelas	Sangat jelas	Jelas	Cukup jelas	Jelas
Disclosure data sharing	Detail	Sangat detail	Detail	Umum	Detail
Penjelasan security measures	Memadai	Komprehensif	Memadai	Terbatas	Memadai
Hak konsumen	Jelas	Sangat jelas	Jelas	Cukup jelas	Jelas

Mekanisme keluhan	Tersedia	Tersedia	Tersedia	Tersedia	Tersedia
-------------------	----------	----------	----------	----------	----------

Sumber: Analisis dokumen privacy policy (2025)

Tokopedia menunjukkan praktik terbaik dalam transparansi kebijakan privasi dengan menyediakan dokumen yang komprehensif namun disajikan dalam bahasa yang accessible bagi pengguna non-teknis. Platform ini secara eksplisit menjelaskan kategori data yang dikumpulkan (informasi akun, data transaksi, device information, location data, browsing behavior), tujuan spesifik pengumpulan setiap jenis data, serta pihak ketiga yang menerima akses data beserta justifikasi business necessity-nya (Mansawan et al., 2025).

Aspek data sharing dengan pihak ketiga menjadi area yang memerlukan perhatian khusus. Shopee, Tokopedia, dan Lazada memberikan disclosure detail mengenai kategori pihak ketiga yang menerima akses data, seperti payment processors, logistics partners, marketing analytics providers, dan affiliated companies. Namun, Bukalapak dan Blibli memberikan informasi yang lebih umum tanpa detail spesifik mengenai jenis data yang dibagikan kepada masing-masing kategori partner.

Kelima platform menjelaskan security measures yang diterapkan untuk melindungi data konsumen, mencakup enkripsi data during transmission dan at rest, access control mechanisms, regular security audits, dan incident response procedures. Tokopedia dan Shopee memberikan penjelasan yang lebih elaboratif mengenai teknologi spesifik yang digunakan seperti AES-256 encryption dan multi-layered firewall systems, sementara platform lain menjelaskan security measures secara konseptual tanpa detail teknis (Tavares et al., 2019; Wynn & Olayinka, 2021).

Informasi tentang hak konsumen atas data personal mereka telah tercakup dalam kebijakan privasi sesuai ketentuan UU Perlindungan Data Pribadi, mencakup hak akses, koreksi, penghapusan (right to be forgotten), portabilitas data, dan hak untuk menarik consent. Tokopedia, Shopee, dan Blibli menyediakan fitur self-service pada setting akun yang memungkinkan pengguna untuk mengunduh data personal mereka atau mengajukan permintaan penghapusan data, sementara platform lain mengharuskan pengguna menghubungi customer service untuk request tersebut (Mansawan et al., 2025).

Mekanisme untuk mengajukan pertanyaan atau keluhan terkait privasi tersedia pada semua platform melalui dedicated email atau contact form, namun response time dan kualitas penanganan keluhan masih menjadi area yang memerlukan improvement berdasarkan review pengguna di berbagai forum.

3. Persepsi dan Pengalaman Konsumen Binjai terhadap Keamanan E-Commerce

Hasil wawancara dengan 8 informan konsumen e-commerce di Kota Binjai mengungkapkan awareness yang masih terbatas terhadap fitur keamanan dan kebijakan privasi platform yang mereka gunakan. Seluruh informan (8 dari 8) mengakui tidak pernah membaca kebijakan privasi secara lengkap sebelum menggunakan platform, dengan alasan utama dokumen terlalu panjang, menggunakan terminologi teknis yang sulit dipahami, dan asumsi bahwa "semua platform punya kebijakan yang sama". Temuan ini mengkonfirmasi observasi sebelumnya bahwa kompleksitas dokumen kebijakan privasi menciptakan barrier signifikan bagi consumer comprehension (Dewantara et al., 2024).

Tabel 3
Profil Informan dan Platform yang Digunakan

Kode	Usia	Pekerjaan	Platform Utama	Frekuensi Transaksi/Bulan	Lama Penggunaan
INF-01	23	Mahasiswa	Shopee, Tokopedia	4-5 kali	3 tahun
INF-02	28	Karyawan Swasta	Tokopedia, Lazada	3-4 kali	4 tahun
INF-03	21	Mahasiswa	Shopee, Bukalapak	2-3 kali	2 tahun
INF-04	35	Wiraswasta	Tokopedia, Blibli	5-6 kali	5 tahun
INF-05	26	Guru	Shopee, Tokopedia	3-4 kali	3 tahun
INF-06	30	Pegawai Negeri	Lazada, Tokopedia	2-3 kali	4 tahun
INF-07	24	Karyawan Swasta	Shopee, Lazada	4-5 kali	3 tahun
INF-08	29	Wiraswasta	Tokopedia, Bukalapak	3-4 kali	4 tahun

Sumber: Data wawancara (2025)

Aspek yang paling diperhatikan informan dalam menilai keamanan platform adalah keberadaan sistem escrow dan program buyer protection. Tujuh dari delapan informan menyatakan bahwa fitur "uang kembali jika barang tidak sesuai" menjadi safety net utama yang membuat mereka merasa aman bertransaksi. Satu informan (INF-04) menjelaskan: *"Saya tidak terlalu paham soal SSL atau enkripsi, tapi yang penting kalau ada masalah uang bisa kembali. Itu yang bikin percaya"*. Temuan ini mengindikasikan bahwa perceived security konsumen lebih banyak dipengaruhi oleh tangible protection mechanisms seperti buyer guarantee dibandingkan technical security features yang bersifat invisible (Wynn & Olayinka, 2021).

Brand recognition dan popularitas platform memainkan peran signifikan dalam pembentukan trust. Enam informan menyatakan bahwa mereka merasa lebih aman bertransaksi melalui platform besar seperti Shopee dan Tokopedia karena "sudah terkenal", "banyak yang pakai", dan "pasti lebih aman karena perusahaan besar". Hanya dua informan (INF-02 dan INF-04) yang secara aktif memverifikasi keberadaan security indicators seperti ikon gembok HTTPS atau badge keamanan sebelum melakukan transaksi. Majority informan mengandalkan heuristic decision-making berdasarkan reputasi platform dan review pengguna lain, tanpa evaluasi mendalam terhadap security infrastructure (Simbolon, 2025).

Terkait fitur autentikasi, seluruh informan menggunakan OTP verification karena bersifat mandatory pada proses login dan transaksi penting. Namun, hanya 2 dari 8 informan (INF-02 dan INF-06) yang mengaktifkan two-factor authentication (2FA) secara proaktif di platform yang menyediakan fitur tersebut. Alasan tidak mengaktifkan 2FA mencakup: kurangnya pemahaman tentang manfaat tambahan yang diberikan (5 informan), persepsi bahwa fitur tersebut memperumit proses login (4 informan), dan ketidaktahuan bahwa fitur tersebut tersedia (3 informan). Satu informan (INF-03) menyatakan: *"OTP saja sudah ribet, apalagi kalau harus pakai aplikasi lain. Lagipula akun saya nggak pernah ada masalah"*. Temuan ini sejalan

dengan observasi Aslan et al. (2023) bahwa adoption rate security features optional masih rendah karena trade-off yang dipersepsikan antara security dan convenience.

Pengalaman negatif terkait keamanan dilaporkan oleh 3 informan. INF-01 pernah menerima SMS phishing yang mengatasnamakan Shopee dan meminta untuk mengklik link verifikasi, namun tidak mengklik karena mencurigakan. INF-05 mengalami kesulitan mendapatkan refund untuk transaksi di mana barang yang diterima palsu, memerlukan waktu 2 minggu untuk penyelesaian. INF-07 pernah mengalami unauthorized login attempt yang terdeteksi sistem dan memerlukan reset password. Ketiga informan menyatakan bahwa meskipun mengalami insiden, kepercayaan mereka terhadap platform tidak menurun drastis selama platform menangani keluhan dengan responsif dan transparan. INF-05 menjelaskan: *"Prosesnya memang lama, tapi akhirnya uang kembali dan customer service tetap update terus. Jadi masih percaya"*. Hal ini menunjukkan bahwa incident response quality menjadi faktor penting dalam maintaining consumer trust bahkan setelah security incident terjadi (Malik, 2025).

Terkait kesadaran tentang privasi data, awareness informan masih sangat terbatas. Ketika ditanyakan tentang bagaimana platform mengelola data personal mereka, majority informan (6 dari 8) menjawab "tidak tahu" atau "sepertinya disimpan di server mereka". Hanya 2 informan (INF-02 dan INF-04) yang menunjukkan concern tentang data sharing dengan pihak ketiga, namun keduanya mengakui tidak pernah mengubah privacy settings default atau mengajukan permintaan akses data. Keseluruhan informan menyatakan bahwa mereka "pasrah" data mereka dikumpulkan platform karena menganggap hal tersebut sebagai "konsekuensi menggunakan layanan gratis". Temuan ini mengindikasikan fatalistic attitude terhadap privasi data, di mana konsumen merasa tidak memiliki control atas informasi personal mereka (Mansawan et al., 2025).

4. Integrasi Sistem Keamanan, Transparansi Privasi, dan Persepsi Konsumen

Analisis komparatif mengidentifikasi korelasi positif antara comprehensiveness sistem keamanan teknis dengan transparansi kebijakan privasi data. Platform yang menerapkan security measures lebih komprehensif cenderung lebih transparan dalam menjelaskan bagaimana data konsumen dilindungi dan dikelola. Tokopedia yang menunjukkan implementasi keamanan paling robust juga menampilkan kebijakan privasi paling transparan dan accessible, mencerminkan organizational commitment terhadap data protection sebagai competitive advantage (Malik, 2025).

Pola ini mengindikasikan bahwa pendekatan keamanan dan privasi tidak bersifat isolated tetapi merupakan bagian integral dari security culture organisasi. Platform yang menginvestasikan sumber daya signifikan pada infrastruktur keamanan teknis juga menunjukkan komitmen pada governance aspects seperti transparency, accountability, dan consumer rights. Sebaliknya, platform dengan implementasi keamanan yang lebih basic cenderung menyediakan kebijakan privasi yang memenuhi requirement minimum regulasi tanpa elaborasi detail yang memberikan assurance tambahan kepada konsumen (Alexander et al., 2020).

Temuan ini sejalan dengan framework cybersecurity governance yang menekankan bahwa keamanan efektif memerlukan integrasi antara technical controls, administrative controls, dan organizational culture (Evans, 2022). Transparansi kebijakan privasi berfungsi sebagai administrative control yang memperkuat technical security measures dengan memberikan clarity kepada

konsumen mengenai bagaimana data mereka dilindungi dan hak apa yang mereka miliki.

Perspektif konsumen Binjai memperkuat argumentasi bahwa technical excellence sistem keamanan harus diimbangi dengan user education dan simplified communication mengenai security features. Kesenjangan antara sophistication teknologi keamanan yang diterapkan platform dengan limited awareness konsumen menciptakan paradox di mana protection mechanisms yang robust tidak memberikan nilai optimal karena tidak dipahami atau dimanfaatkan pengguna. Platform perlu mengembangkan strategi komunikasi yang mentranslate technical security measures ke dalam bahasa yang accessible dan meaningful bagi konsumen awam, menggunakan visual indicators, notifications, atau educational content yang engaging (Mubarak et al., 2025).

Temuan juga mengindikasikan pentingnya behavioral security interventions yang tidak hanya fokus pada teknologi tetapi juga pada human factors. Nudging techniques seperti default-secure settings, progressive disclosure of privacy information, atau gamification dalam security awareness dapat meningkatkan engagement konsumen terhadap security practices. Platform yang berhasil mengintegrasikan usability dengan security, serta menyediakan tangible value proposition untuk security features optional, akan memiliki competitive advantage dalam membangun consumer trust di pasar kota menengah seperti Binjai (Evans, 2022).

5. Tantangan dan Peluang Improvement

Meskipun kelima platform telah menerapkan standar keamanan dasar, beberapa tantangan masih diidentifikasi. Pertama, adoption rate fitur keamanan optional seperti 2FA masih rendah karena lack of awareness di kalangan konsumen tentang pentingnya additional security layers. Education campaign yang sistematis diperlukan untuk meningkatkan security consciousness pengguna (Simbolon, 2025). Temuan dari konsumen Binjai mengkonfirmasi urgency intervensi edukasi, di mana majority pengguna tidak menyadari risks yang mereka hadapi dan security features yang tersedia untuk self-protection.

Kedua, kompleksitas dan panjangnya dokumen kebijakan privasi menciptakan barrier bagi konsumen untuk benar-benar memahami bagaimana data mereka digunakan. Inovasi dalam presentasi informasi privasi seperti layered approach atau visual privacy dashboard dapat meningkatkan comprehension dan engagement konsumen terhadap privacy practices (Dewantara et al., 2024).

Ketiga, pemanfaatan teknologi emerging seperti AI untuk fraud detection dan anomaly detection masih dalam tahap awal implementasi. Mubarak et al. (2025) mendemonstrasikan bahwa machine learning algorithms dapat significantly meningkatkan akurasi deteksi transaksi suspicious, namun implementasi requires significant investment pada infrastructure dan expertise yang mungkin challenging bagi platform dengan resources terbatas.

Keempat, cybersecurity governance belum sepenuhnya terintegrasi dengan business strategy pada beberapa platform, di mana keamanan masih dipandang sebagai cost center rather than value driver. Shift paradigm diperlukan untuk memposisikan security dan privacy sebagai competitive differentiator yang dapat meningkatkan customer trust dan loyalty (Malik, 2025).

Peluang improvement mencakup adoption teknologi blockchain untuk transaction transparency dan immutability (Choo et al., 2020), enhancement pada

incident response capabilities dengan establishment dedicated security operations center, serta collaboration antar platform dalam threat intelligence sharing untuk collective defense terhadap emerging threats (Aslan et al., 2023). Khusus untuk konsumen di kota menengah seperti Binjai, pengembangan program literasi digital yang kontekstual dan accessible melalui kolaborasi dengan institusi pendidikan lokal dan komunitas dapat menjadi strategi efektif untuk meningkatkan security awareness dan protective behavior.

E. KESIMPULAN

Penelitian ini menyimpulkan bahwa platform e-commerce Indonesia telah mengimplementasikan sistem keamanan fundamental yang mencakup SSL/TLS encryption, autentikasi berbasis OTP, sistem pembayaran escrow, dan integration dengan payment gateway tersertifikasi. Namun, terdapat variasi signifikan dalam comprehensiveness security features dan transparansi kebijakan privasi data antar platform. Tokopedia menunjukkan praktik terbaik dengan kombinasi sistem keamanan berlapis dan kebijakan privasi yang sangat transparan, sementara platform lain menerapkan standar yang memadai namun masih dapat ditingkatkan. Eksplorasi persepsi konsumen di Kota Binjai mengungkapkan kesenjangan signifikan antara sophistication sistem keamanan platform dengan awareness dan utilization konsumen, di mana majority pengguna tidak memahami technical security features dan cenderung mengandalkan brand reputation sebagai indikator keamanan.

Hubungan positif teridentifikasi antara robustness sistem keamanan teknis dengan transparansi kebijakan privasi, mengindikasikan bahwa kedua aspek tersebut merupakan manifestasi dari organizational commitment terhadap data protection. Dari perspektif konsumen, perceived security lebih dipengaruhi oleh tangible protection mechanisms seperti buyer guarantee dibandingkan technical features yang invisible, mengindikasikan perlunya simplification dalam komunikasi security benefits kepada end users.

Tantangan utama meliputi rendahnya adoption rate fitur keamanan optional, kesenjangan awareness konsumen terhadap privacy risks dan security features, kompleksitas dokumen kebijakan privasi yang menghambat pemahaman konsumen, serta belum optimalnya pemanfaatan teknologi emerging seperti AI dan blockchain untuk meningkatkan security capabilities. Addressing tantangan-tantangan ini memerlukan integrasi antara technical innovation, regulatory compliance, dan education initiatives yang melibatkan platform, regulator, dan konsumen.

F. SARAN

Berdasarkan temuan penelitian, beberapa rekomendasi strategis perlu diimplementasikan oleh stakeholder ekosistem e-commerce Indonesia untuk meningkatkan keamanan dan perlindungan data konsumen. Platform e-commerce disarankan untuk meningkatkan adoption rate fitur keamanan seperti two-factor authentication melalui kampanye edukasi sistematis dan incentivization program, dengan strategi komunikasi yang mentranslate technical security features ke dalam bahasa accessible bagi konsumen awam menggunakan visual indicators dan educational content yang engaging, menyederhanakan presentasi kebijakan privasi menggunakan pendekatan berlapis atau visual dashboard yang lebih accessible, serta menginvestasikan sumber daya pada teknologi AI-powered fraud detection untuk

pencegahan ancaman secara real-time. Regulator perlu memperkuat enforcement Undang-Undang Perlindungan Data Pribadi dengan menerbitkan guideline implementasi yang jelas dan melakukan audit berkala, mendorong standarisasi minimum security requirements untuk seluruh platform, serta memfasilitasi mekanisme threat intelligence sharing antar platform untuk pertahanan kolektif. Konsumen diharapkan meningkatkan awareness tentang pentingnya mengaktifkan fitur keamanan tambahan, secara proaktif membaca kebijakan privasi platform yang digunakan, dan melaporkan aktivitas mencurigakan kepada platform atau otoritas terkait. Khusus untuk konsumen di kota menengah seperti Binjai, program literasi digital yang disesuaikan dengan konteks lokal dan karakteristik demografis perlu dikembangkan melalui kolaborasi platform, institusi pendidikan, dan komunitas lokal untuk meningkatkan security consciousness dan self-protection behavior. Penelitian lanjutan diperlukan untuk mengukur dampak transparansi kebijakan privasi terhadap trust dan purchase intention konsumen secara kuantitatif, mengeksplorasi implementasi blockchain technology untuk meningkatkan transparansi transaksi, serta menganalisis efektivitas AI-powered security measures dalam konteks platform e-commerce lokal Indonesia.

G. DAFTAR PUSTAKA

- Alexander, D., Finch, A., Sutton, D., & Taylor, A. (2020). *Information Security Management Principles* (3rd ed.). BCS Learning & Development.
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 12(6), 1–31.
<https://doi.org/10.3390/electronics12061333>
- Choo, K.-K. R., Dehghantanha, A., & Parizi, R. M. (2020). *Blockchain Cybersecurity, Trust and Privacy*. Springer International Publishing.
<https://doi.org/10.1007/978-3-030-38181-3>
- Dewantara, R., Bintang, R., & Gatra, R. (2024). Analisis Keamanan Data Pelanggan dalam Menghadapi Tantangan Penggunaan Marketplace. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 9(2), 94–104.
<https://doi.org/10.14421/jiska.2024.9.2.94-104>
- Evans, A. (2022). *Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization*. Routledge.
- Katiyar, S., Tripathi, R., Kumar, A., Verma, P., Sahu, S., & Saxena, A. (2024). AI and Cyber-Security: Enhancing Threat Detection and Response with Machine Learning. *Educational Administration: Theory and Practice*, 30(4), 2377–2385.
<https://doi.org/10.53555/kuey.v30i4.2377>
- Malik, G. (2025). Cybersecurity Governance and Risk Management for Digital Transformation. *International Journal of Applied Mathematics*, 38(10), 2532–2561. <https://doi.org/10.12732/ijam.v38i10s.1139>
- Mansawan, I., Sassan, J., & Bernard, J. (2025). Legal Protection of E-Commerce Consumers' Personal Data Under Indonesian Law. *Jurnal Ilmiah Hukum Dan Keadilan (JIHK)*, 7(1), 538–554. <https://doi.org/10.46924/jihk.v7i1.320>
- Mishra, C., Sindhu, P., Mohanty, P., & Samrat, A. (2024). DDoS Attacks and Analysis of Different Defense Mechanisms. *International Journal of Scientific Research in*

Engineering and Management (IJSREM), 08(06), 1–6.

<https://doi.org/10.55041/IJSREM40061>

Mubarok, D., Adjani, K., Hutama, B. D. R., Mutoffar, M. M., & Indrayani, R. (2025). Big Data Analytics dan Machine Learning untuk Memprediksi Perilaku Konsumen di E-Commerce. *JIRE (Jurnal Informatika & Rekayasa Elektronik)*, 8(1), 159–167.

Simbolon, N. (2025). Ancaman Cybercrime di Indonesia: Tinjauan Sistematis dan Peran Cybersecurity pada E-Commerce dalam Hukum Pidana. *Jurnal Sosial Humaniora Dan Pendidikan*, 4(2), 815–825.

<https://doi.org/10.55606/inovasi.v4i2.4425>

Tavares, J. M. R. S., Mishra, B. K., Kumar, R., Zaman, N., & Khari, M. (Eds.). (2019). *Handbook of E-Business Security*. Auerbach Publications.

Turban, E., Whiteside, J., King, D., & Outland, J. (2017). *Introduction to Electronic Commerce and Social Commerce* (4th ed.). Springer.

<https://doi.org/10.1007/978-3-319-50091-1>

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Wynn, M., & Olayinka, O. (2021). E-Business Strategy in Developing Countries: A Framework and Checklist for the Small Business Sector. *Sustainability*, 13(13), 7356. <https://doi.org/10.3390/su13137356>