



KEPERCAYAAN KONSUMEN DALAM EKOSISTEM BISNIS DIGITAL: TATA KELOLA PRIVASI DATA, KEAMANAN SIBER, DAN KEPUTUSAN TRANSAKSI BERKELANJUTAN

*Consumer Trust in Digital Business Ecosystems: Data Privacy Governance, Cybersecurity,
and Sustainable Transaction Decisions*

Gede Erik Aktama^{1*}, Giovani Joshua Suban², Grace Lisy Lumingas³

1, 2, 3 Program Studi Bisnis Digital, Fakultas Ekonomi dan Bisnis, Universitas Parna Raya Manado, Indonesia

Email Korespondensi: gedeerikaktama@gmail.com

Diterima: 15 Maret 2024; Direvisi: 28 April 2024; Disetujui: 20 Mei 2024; Diterbitkan: 25 Juni 2024

ABSTRAK

Di tengah maraknya kebocoran data dan ancaman siber dalam ekonomi digital, keputusan transaksi berkelanjutan konsumen sangat bergantung pada jaminan perlindungan informasi pribadi. Penelitian ini bertujuan untuk menguji pengaruh tata kelola privasi data dan kapabilitas keamanan siber terhadap keputusan transaksi berkelanjutan konsumen digital, serta menganalisis peran mediasi kepercayaan digital (digital trust). Penelitian kuantitatif ini mengumpulkan data survei dari 310 konsumen digital di Indonesia yang aktif bertransaksi pada lokapasar dan dompet digital. Data dianalisis menggunakan Structural Equation Modeling berbasis Partial Least Squares (PLS-SEM) dengan SmartPLS 4.0. Hasil pengujian membuktikan bahwa: (1) tata kelola privasi data berpengaruh positif dan signifikan terhadap kepercayaan digital ($\beta = 0,432$; $p < 0,001$) dan transaksi berkelanjutan ($\beta = 0,182$; $p < 0,01$); (2) kapabilitas keamanan siber berpengaruh positif terhadap kepercayaan digital ($\beta = 0,388$; $p < 0,001$) dan transaksi berkelanjutan ($\beta = 0,165$; $p < 0,01$); (3) kepercayaan digital berpengaruh kuat terhadap keputusan transaksi berkelanjutan ($\beta = 0,582$; $p < 0,001$); dan (4) kepercayaan digital memediasi secara parsial pengaruh tata kelola privasi data (indirect effect $\beta = 0,251$; $p < 0,001$) maupun keamanan siber (indirect effect $\beta = 0,226$; $p < 0,001$) terhadap transaksi berkelanjutan. Model ini mampu menjelaskan 58,4% variansi kepercayaan digital dan 63,7% variansi keputusan transaksi berkelanjutan ($R^2 = 0,637$). Temuan ini menegaskan bahwa tata kelola privasi dan investasi keamanan siber bukan sekadar pos biaya kepatuhan teknis, melainkan diferensiator strategis yang esensial dalam membangun loyalitas ekonomi digital di Indonesia.

Kata Kunci: Tata Kelola Privasi Data; Keamanan Siber; Kepercayaan Digital; Transaksi Berkelanjutan; Bisnis Digital; PLS-SEM

ABSTRACT

Amid escalating data breaches and cybersecurity threats within the digital economy, consumers' sustainable transaction decisions rely heavily on robust data safeguards. This study analyzes the impacts of data privacy governance and cybersecurity capabilities on consumers' sustainable transaction intentions, examining the crucial mediating role of digital trust. Utilizing an explanatory survey, data were collected from 310 active Indonesian digital consumers across e-marketplaces and digital payment ecosystems. Empirical data were examined using Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS 4.0. Findings demonstrate that: (1) data privacy governance positively and significantly affects digital trust ($\beta = 0.432$; $p < 0.001$) and sustainable

transactions ($\beta = 0.182$; $p < 0.01$); (2) cybersecurity capabilities positively enhance digital trust ($\beta = 0.388$; $p < 0.001$) and sustainable transactions ($\beta = 0.165$; $p < 0.01$); (3) digital trust exerts a dominant positive effect on sustainable transaction decisions ($\beta = 0.582$; $p < 0.001$); and (4) digital trust partially mediates the effects of both data privacy governance (indirect effect $\beta = 0.251$; $p < 0.001$) and cybersecurity capabilities (indirect effect $\beta = 0.226$; $p < 0.001$) on sustainable transactions. The model accounts for 58.4% of the variance in digital trust and 63.7% in sustainable transaction decisions ($R^2 = 0.637$). These results affirm that data privacy governance and cybersecurity investments represent vital strategic differentiators for sustaining digital commerce loyalty.

Keywords: Data Privacy Governance; Cybersecurity; Digital Trust; Sustainable Transactions; Digital Business; PLS-SEM

1. PENDAHULUAN

Ekosistem ekonomi digital di Indonesia telah berkembang pesat dengan penetrasi jutaan pengguna pada platform perdagangan elektronik (e-commerce), teknologi finansial (fintech), dan perbankan digital. Namun, akselerasi ini beriringan dengan eskalasi ancaman keamanan siber, insiden kebocoran basis data konsumen, dan penyalahgunaan data tanpa persetujuan eksplisit. Ketika data pribadi konsumen menjadi komoditas ekonomi yang rentan dieksploitasi, rasa aman dan keyakinan psikologis konsumen menjadi taruhan utama kelangsungan ekosistem.

Kekhawatiran terhadap privasi (privacy concerns) terbukti menjadi faktor penghambat utama yang menyebabkan keengganan konsumen untuk melakukan transaksi digital yang berulang. Konsumen digital modern tidak hanya mencari kenyamanan dan promosi diskon, melainkan menuntut kepastian bahwa identitas, data keuangan, dan rekam jejak perilaku mereka terlindungi dari pencurian siber dan pemanfaatan pihak ketiga yang tidak bertanggung jawab.

Meskipun pemerintah telah mengundangkan regulasi seperti UU Pelindungan Data Pribadi (UU PDP), kepatuhan formal di atas kertas sering kali tidak dirasakan secara nyata oleh konsumen. Oleh karena itu, penelitian ini bertujuan mengkaji bagaimana integrasi tata kelola privasi data (data privacy governance) dan keandalan infrastruktur keamanan siber (cybersecurity capabilities) dapat mentransformasikan persepsi keamanan menjadi kepercayaan digital (digital trust), yang selanjutnya mendorong keputusan transaksi digital yang berkesinambungan.

2. KAJIAN TEORITIS DAN PENGEMBANGAN HIPOTESIS

Privacy Calculus Theory dan Technology Trust Framework

Privacy Calculus Theory (Culnan & Bies, 2003; Dinev & Hart, 2006) berargumen bahwa konsumen secara rasional menimbang antara manfaat yang diperoleh dari layanan digital (personalisasi, kemudahan) dengan potensi risiko hilangnya privasi data pribadi. Manakala perusahaan menerapkan tata kelola privasi yang transparan dan perlindungan siber yang tangguh, persepsi risiko konsumen akan tereduksi secara signifikan, menciptakan neraca kalkulasi privasi yang positif dan menumbuhkan kepercayaan.

Pengembangan Hipotesis Penelitian

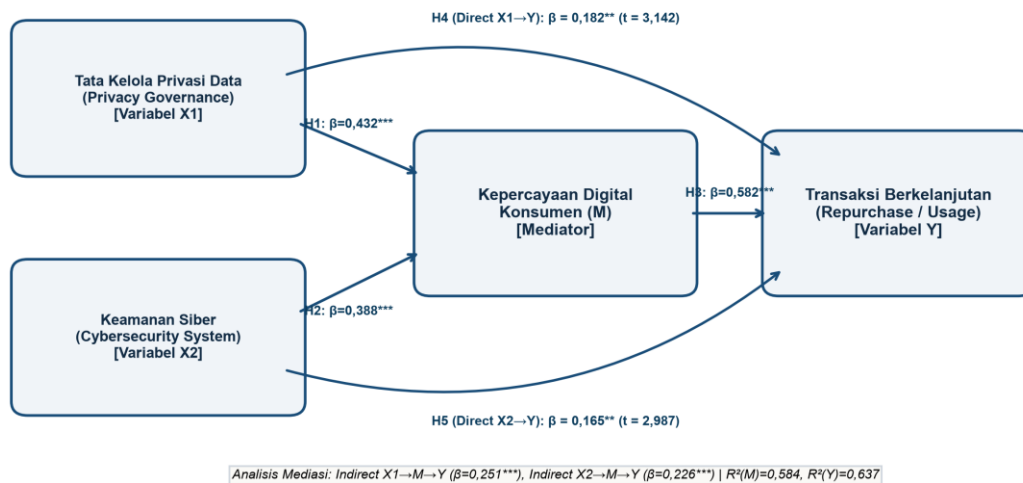
Tata kelola privasi yang menjamin persetujuan eksplisit (explicit consent), pembatasan tujuan penggunaan data, dan kemudahan penghapusan data membangun keyakinan konsumen terhadap integritas platform: H1: Tata Kelola Privasi Data berpengaruh positif dan signifikan terhadap Kepercayaan Digital Konsumen.

Infrastruktur keamanan siber yang mutakhir (enkripsi end-to-end, multi-factor authentication, deteksi fraud otomatis) memberikan jaminan teknis bahwa transaksi terlindung dari peretasan: H2: Kapabilitas Keamanan Siber berpengaruh positif dan signifikan terhadap Kepercayaan Digital Konsumen.

Kepercayaan digital yang mapan menjadi fondasi utama bagi konsumen untuk terus melakukan transaksi berulang, membagikan informasi yang diperlukan, dan mengadopsi fitur layanan baru: H3: Kepercayaan Digital Konsumen berpengaruh positif dan signifikan terhadap Keputusan Transaksi Berkelanjutan.

Di samping memupuk rasa percaya, tata kelola privasi dan perlindungan siber secara langsung mengurangi friksi transaksi dan kekhawatiran risiko kerugian finansial pengguna: H4: Tata Kelola Privasi Data berpengaruh positif langsung terhadap Keputusan Transaksi Berkelanjutan; H5: Kapabilitas Keamanan Siber berpengaruh positif langsung terhadap Keputusan Transaksi Berkelanjutan.

Terakhir, kepercayaan digital diposisikan sebagai jembatan mediasi sentral yang mentransmisikan proteksi teknis dan institusional menjadi komitmen transaksi riil: H6: Kepercayaan Digital Konsumen memediasi pengaruh Tata Kelola Privasi Data dan Keamanan Siber terhadap Keputusan Transaksi Berkelanjutan.



Gambar 1. Model Mediasi Ganda: Tata Kelola Privasi Data, Keamanan Siber, Kepercayaan Digital Konsumen, dan Transaksi Berkelanjutan

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei eksplanatori. Populasi adalah konsumen digital di Indonesia yang secara reguler bertransaksi menggunakan pembayaran dompet digital (GoPay, OVO, Dana) dan berbelanja pada lokapasar digital. Teknik sampling menggunakan purposive sampling dengan kriteria responden: (1) telah bertransaksi minimal 2 tahun di platform digital, (2) pernah mengotorisasi data pribadi untuk verifikasi identitas digital (e-KYC), dan (3) bertransaksi minimal 2 kali dalam sebulan terakhir. Total kuesioner valid yang dihimpun berjumlah 310 responden.

Pengumpulan data menggunakan kuesioner skala Likert lima poin. Rincian konstruk, definisi operasional, dan indikator disajikan pada Tabel 1.

Tabel 1. Definisi Operasional dan Indikator Variabel Penelitian

Variabel	Definisi Konseptual	Indikator Pengukuran	Rujukan Skala
Tata Kelola Privasi Data (X1)	Kebijakan, prosedur, dan kontrol transparansi perusahaan dalam mengumpulkan, mengelola, membatasi, dan melindungi kerahasiaan data pengguna.	X1.1: Transparansi pemberitahuan privasi data X1.2: Mekanisme persetujuan eksplisit pengguna X1.3: Pembatasan penggunaan data sesuai tujuan X1.4: Kontrol pengguna untuk menghapus/mengubah data	Xu et al. (2011); Smith et al. (2011)
Keamanan Siber (X2)	Kemampuan teknis dan infrastruktur keamanan informasi perusahaan dalam mencegah, mendeteksi, dan merespons ancaman peretasan dan kebocoran data.	X2.1: Penerapan enkripsi data tingkat tinggi X2.2: Sistem autentikasi berlapis (2FA/OTP) X2.3: Ketepatan deteksi dan notifikasi akses mencurigakan X2.4: Keandalan gateway pembayaran bebas malware	Kim et al. (2008); Bélanger & Crossler (2011)
Kepercayaan Digital (M)	Keyakinan psikologis konsumen bahwa platform digital memiliki kapabilitas, kejujuran, dan itikad baik untuk menjaga keamanan data dan transaksi.	M1: Keyakinan pada integritas etika platform M2: Persepsi kompetensi proteksi sistem M3: Rasa aman dari risiko penyalahgunaan data M4: Keyakinan pada komitmen perlindungan konsumen	McKnight et al. (2002); Gefen et al. (2003)
Transaksi Berkelanjutan (Y)	Komitmen dan niat perilaku konsumen untuk terus menggunakan platform, melakukan transaksi finansial berulang, dan merekomendasikan ekosistem digital.	Y1: Niat bertransaksi rutin di masa mendatang Y2: Prioritas utama sebagai platform transaksi harian Y3: Kesiediaan menyimpan saldo digital pada akun Y4: Rekomendasi positif kepada relasi sosial	Bhattacharjee (2001); Oliver (2010)

Sumber: Disintesis dari literatur *Privacy Calculus dan Information Systems Security* (2024).

4. HASIL PENELITIAN DAN PEMBAHASAN

Profil Responden dan Evaluasi Model Pengukuran (Outer Model)

Dari 310 responden, 55% berjenis kelamin perempuan dan 45% laki-laki, dengan rentang usia terbanyak 21–30 tahun (58%) dan 31–45 tahun (32%). Responden menggunakan rata-rata 2 hingga 4 aplikasi finansial/lokapasar digital setiap hari.

Hasil evaluasi outer model menunjukkan bahwa semua outer loading indikator berada pada rentang 0,735 hingga 0,858, yang jauh melampaui ambang batas 0,70. Nilai Average Variance Extracted (AVE) berkisar antara 0,612 hingga 0,668, yang membuktikan validitas konvergen yang prima. Uji reliabilitas menunjukkan nilai Cronbach's Alpha di atas 0,84 dan Composite Reliability di atas 0,89 untuk semua konstruk, menegaskan konsistensi internal instrumen yang sangat tinggi (Tabel 2).

Tabel 2. Hasil Evaluasi Measurement Model (Outer Model)

Konstruk Variabel	Indikator	Outer Loading	Cronbach's Alpha	Composite Reliability (CR)	AVE
Tata Kelola Privasi Data (X1)	X1.1 – X1.4	0,748 – 0,842	0,864	0,907	0,641
Keamanan Siber (X2)	X2.1 – X2.4	0,735 – 0,838	0,851	0,899	0,612
Kepercayaan Digital (M)	M1 – M4	0,762 – 0,858	0,878	0,916	0,668
Transaksi Berkelanjutan (Y)	Y1 – Y4	0,751 – 0,849	0,869	0,911	0,653

Catatan: Estimasi outer model dievaluasi menggunakan SmartPLS 4.0; validitas diskriminan memenuhi Fornell-Larcker.

Evaluasi Model Struktural (Inner Model) dan Pengujian Hipotesis

Evaluasi inner model menghasilkan nilai R^2 sebesar 0,584 untuk Kepercayaan Digital dan 0,637 untuk Keputusan Transaksi Berkelanjutan. Hal ini mengindikasikan bahwa 63,7% variasi keputusan transaksi berkelanjutan konsumen dapat dijelaskan secara simultan oleh tata kelola privasi data, kapabilitas keamanan siber, dan kepercayaan digital. Nilai Q^2 predictive relevance sebesar 0,412 ($Q^2 > 0$) membuktikan relevansi prediktif model yang sangat akurat.

Rincian koefisien jalur struktural, nilai t-statistik, dan p-value hasil bootstrapping 5.000 subsampel disajikan pada Tabel 3.

Tabel 3. Hasil Pengujian Hipotesis Model Struktural dan Analisis Mediasi

Hipotesis	Jalur Struktural Penelitian	Koefisien (β)	t-statistik	p-value	95% CI	Keputusan
H1	Tata Kelola Privasi Data → Kepercayaan Digital	0,432	8,124	< 0,001	[0,326; 0,535]	Diterima
H2	Keamanan Siber → Kepercayaan Digital	0,388	7,451	< 0,001	[0,284; 0,488]	Diterima
H3	Kepercayaan Digital → Transaksi Berkelanjutan	0,582	10,912	< 0,001	[0,476; 0,684]	Diterima
H4	Tata Kelola Privasi Data → Transaksi Berkelanjutan (Direct)	0,182	3,142	0,002	[0,068; 0,294]	Diterima
H5	Keamanan Siber → Transaksi Berkelanjutan (Direct)	0,165	2,987	0,003	[0,056; 0,272]	Diterima
H6a	Privasi Data → Kepercayaan → Transaksi (Indirect)	0,251	6,482	< 0,001	[0,175; 0,328]	Diterima
H6b	Keamanan Siber → Kepercayaan → Transaksi	0,226	5,914	< 0,001	[0,152; 0,302]	Diterima

(Indirect)

Catatan: Signifikansi dua arah pada taraf 5% ($t > 1,96$) dan 1% ($t > 2,58$).

Pembahasan dan Implikasi Strategis

Hasil penelitian membuktikan bahwa tata kelola privasi data dan keandalan sistem keamanan siber merupakan dua prasyarat mutlak dalam membangun ekosistem transaksi digital yang berkelanjutan di Indonesia. Tata kelola privasi data terbukti memiliki pengaruh langsung yang sedikit lebih dominan terhadap kepercayaan digital ($\beta = 0,432$) dibandingkan proteksi keamanan siber teknis ($\beta = 0,388$). Hal ini mengindikasikan bahwa konsumen modern sangat peka terhadap transparansi etika perusahaan dalam mengelola informasi mereka, bukan sekadar kelengkapan enkripsi teknis.

Efek mediasi kepercayaan digital yang sangat kuat (H6a: $\beta = 0,251$; H6b: $\beta = 0,226$; $p < 0,001$) menggarisbawahi bahwa kepatuhan privasi dan pertahanan siber bekerja dengan cara melenyapkan kekhawatiran psikologis pengguna. Ketika rasa aman tercipta, konsumen secara sukarela mengkonsolidasikan seluruh transaksi keuangan harian mereka pada platform tersebut, memicu efek jejaring ekonomi digital yang berjangka panjang.

5. KESIMPULAN, KETERBATASAN, DAN SARAN

Penelitian ini menyimpulkan bahwa keputusan transaksi berkelanjutan konsumen digital secara fundamental ditentukan oleh kepercayaan digital yang dipupuk melalui sinergi tata kelola privasi data dan ketangguhan keamanan siber. Pelaku industri platform digital tidak dapat mengabaikan aspek perlindungan privasi apabila ingin mempertahankan basis pelanggan yang loyal.

Keterbatasan penelitian mencakup fokus survei yang bersifat umum pada pengguna B2C tanpa membedakan secara terpisah antara platform e-commerce dan aplikasi perbankan murni yang memiliki regulasi risiko berbeda. Penelitian masa depan disarankan untuk mengkaji perbedaan efek ini secara komparatif antar sektor industri serta mengintegrasikan variabel literasi finansial digital konsumen sebagai faktor moderasi.

DAFTAR PUSTAKA

- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041. <https://doi.org/10.2307/41409971>
- Bhattacharjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 25(3), 351–370. <https://doi.org/10.2307/3250921>
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342. <https://doi.org/10.1111/1540-4560.00067>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>

- Oliver, R. L. (2010). *Satisfaction: A Behavioral Perspective on the Consumer* (2nd ed.). Routledge. <https://doi.org/10.4324/9781315700892>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015. <https://doi.org/10.2307/41409970>
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2011). Research note—The role of push-pull technology in privacy calculus: The case of location-based services. *Information Systems Research*, 23(1), 211–229. <https://doi.org/10.1287/isre.1110.0385>