Maslahah: Jurnal Manajemen dan Ekonomi Syariah
Volume. 4 Nomor. 3 Juli 2026
e-ISSN: 2988-2230; p-ISSN: 2988-2249, Hal. 18-29
DOI: https://doi.org/10.59059/maslahah.v4i3.3090
Tersedia: https://journal.staiypiqbaubau.ac.id/index.php/Maslahah

Kajian Literatur atas Dinamika Isu Privasi Data dan Kepercayaan pada pengguna E-Commerce di Indonesia

Hotni Pinta Laura Hutabarat[1*], Jonathan Edgarian[2], Catharina Aprilia Hellyani[3]
[1-3]Program Studi Manajemen, Universitas Ma Chung, Indonesia
Penulis Korespondensi: hotnihutabarat303@gmail.com

Abstract. *This literature review analyzes the impact of data privacy issues on consumer usage intention in Indonesian e-commerce platforms. The study aims to map privacy threats and understand the phenomenon of the privacy paradox in the context of digital retail. Using a literature review method, this study synthesized findings from international journals published in the last five years from Scopus, Web of Science, and Google Scholar databases. The results show that excessive data collection, unauthorized secondary use, and data breaches significantly increase consumer privacy concerns. However, the research also confirms a privacy paradox, where consumers willingly share personal data to gain shopping convenience and promotions. The findings highlight that strong brand trust and a seamless user experience can effectively mitigate these privacy fears. Practically, this study recommends that e-commerce companies implement the Privacy by Design framework, utilize dynamic passwords (OTP), and provide transparent privacy settings as a competitive marketing advantage. Future research should explore specific regional demographics and the direct impact of new technologies like AI chatbots on consumer security perceptions.*

Keywords: *Consumer Behavior; Data Privacy; E-Commerce; Privacy Paradox; User Experience.*

Abstrak. Tinjauan literatur ini menganalisis pengaruh isu privasi data terhadap minat penggunaan konsumen pada platform e-commerce di Indonesia. Penelitian ini bertujuan untuk memetakan bentuk ancaman privasi serta memahami fenomena paradoks privasi dalam konteks ritel digital. Menggunakan metode studi literatur, penelitian ini menyintesis temuan dari berbagai jurnal internasional yang terbit dalam lima tahun terakhir dari basis data Scopus, Web of Science, dan Google Scholar. Hasil penelitian menunjukkan bahwa pengumpulan data yang berlebihan, penggunaan data sekunder tanpa izin, dan kasus kebocoran data secara signifikan meningkatkan kekhawatiran privasi konsumen. Namun, riset ini juga mengonfirmasi adanya paradoks privasi, di mana konsumen tetap rela membagikan data pribadi demi mendapatkan kemudahan berbelanja dan promosi. Temuan menyoroti bahwa rasa percaya (*trust*) yang kuat pada merek dan pengalaman pengguna yang lancar secara efektif mampu meredakan ketakutan privasi tersebut. Secara praktis, studi ini menyarankan perusahaan e-commerce untuk menerapkan kerangka kerja *Privacy by Design*, menggunakan kata sandi dinamis (OTP), dan menyediakan pengaturan privasi yang transparan sebagai keunggulan kompetitif dalam pemasaran. Penelitian selanjutnya sebaiknya mengeksplorasi demografi regional yang lebih spesifik serta menguji dampak langsung dari teknologi baru seperti *chatbot* kecerdasan buatan terhadap persepsi keamanan konsumen.

Kata Kunci: E-Commerce; Paradoks Privasi; Pengalaman Pengguna; Perilaku Konsumen; Privasi Data.

1. LATAR BELAKANG

Transformasi digital di Indonesia, didorong oleh penetrasi internet seluler yang masif, telah mengubah lanskap ekonomi secara fundamental dan menjadikan platform e-commerce sebagai tulang punggung transaksi ritel masyarakat modern. Pertumbuhan eksponensial ini secara alamiah membawa konsekuensi langsung berupa pengumpulan, pemrosesan, dan penyimpanan data pribadi konsumen dalam skala yang sangat besar. Sayangnya, akselerasi digitalisasi ini pada kenyataannya diiringi oleh eskalasi kerentanan keamanan siber, di mana isu kebocoran data telah menjadi fenomena kontemporer yang paling mengkhawatirkan (Zafira et al., 2026). Banyaknya kasus nyata di mana jutaan data penting pengguna di e-commerce besar bocor telah membuat masyarakat ragu apakah sistem digital di Indonesia benar-benar mampu menjaga rahasia mereka (Wibowo & Handayani, 2023). Kondisi ini menghadirkan

Naskah Masuk: 30 April 2026; Revisi: 29 Mei 2026; Diterima: 28 Juni 2026; Terbit: 02 Juli 2026

pergeseran paradigma perilaku, di mana kemudahan bertransaksi daring kini secara ketat dibayangi oleh ketakutan kronis terhadap eksploitasi dan penyalahgunaan informasi sensitif tanpa persetujuan eksplisit dari pihak konsumen. Secara konseptual, kekhawatiran terhadap privasi (privacy concern) bertindak sebagai anteseden utama yang mampu mendegradasi tingkat kepercayaan (trust) dan melipatgandakan persepsi risiko (perceived risk) pengguna saat mereka berinteraksi di lingkungan virtual.

Ketika konsumen mulai menyadari adanya celah kerentanan sistemik pada arsitektur perlindungan data di sebuah platform, akan muncul keraguan rasional yang berdampak instan pada penurunan niat beli serta minat penggunaan kembali (repurchase intention) layanan tersebut (Prasetyo & Dewi, 2022). Ancaman kebocoran ini tidak hanya memicu probabilitas kerugian material dan finansial secara langsung, tetapi juga menciptakan potensi kerugian psikologis yang mendalam bagi para korban. Hilangnya kontrol penuh atas identitas pribadi kerap kali memicu respons proaktif berupa perilaku penghindaran (avoidance behavior) dari konsumen, yang pada gilirannya akan sangat merugikan nilai reputasi korporasi serta menekan tingkat retensi pelanggan secara berkelanjutan (Kroll & Stieglitz, 2021; Sari & Rahmawati, 2023). Oleh karenanya, tata kelola isu privasi data pada masa kini telah menjelma menjadi ancaman strategis fundamental terhadap keberlangsungan model bisnis e-commerce itu sendiri. Walaupun dampak destruktif dari isu privasi tampak jelas memengaruhi postur industri niaga elektronik, penelaahan kritis terhadap literatur terdahulu justru memperlihatkan dinamika temuan yang terfragmentasi, bervariasi, dan sering kali saling kontradiktif terkait profil perilaku riil masyarakat digital di Indonesia. Di satu sisi, banyak kajian empiris yang secara konklusif membuktikan bahwa tingginya kekhawatiran privasi berpotensi mengikis kepercayaan konsumen dan secara langsung menghambat niat transaksi mereka (Anaza & Zhao, 2021; Hidayat & Kusuma, 2024). Kegagalan operasional platform dalam meyakinkan validitas sistem keamanannya berujung pada keengganan kolektif pengguna untuk membagikan data, yang berimbas pada stagnasi transaksi (Nuranisa & Lukitasari, 2024)

Namun di sisi lain, berbagai literatur terkini menangkap indikasi kuat munculnya anomali perilaku adaptif yang dalam ranah akademis dikenal sebagai privacy paradox. Dalam fenomena ini, meskipun mayoritas konsumen menyuarakan tuntutan privasi yang tinggi, mereka nyatanya tetap bersedia menyerahkan data pribadinya demi mendapatkan kepraktisan instan dan insentif promosi jangka pendek dari platform e-commerce (Bandara, Fernando, & Akter, 2021; Utomo & Santoso, 2022). Jurang perbedaan kognitif yang tajam antara sikap kesadaran (attitude) dan tindakan kompromistis nyata (actual behavior) inilah yang melahirkan perdebatan akademis intens. Situasi ini dinilai bertambah kompleks pasca pengesahan Undang-

Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang diharapkan mampu memulihkan rasa aman publik, meskipun efektivitas implementasinya di lapangan masih terus diuji dan menjadi subjek evaluasi para peneliti (Ardika, 2025; Prayuti, 2024). Inkonsistensi konklusif dari temuan literatur terkait mekanisme kausalitas antara variabel isu privasi dan minat penggunaan inilah yang memunculkan rumusan permasalahan penelitian (research problem) utama dalam kajian literatur ini. Pemahaman yang masih terpotong-potong terhadap fenomena paradoks privasi yang kompleks ini sangat berisiko menghasilkan kesimpulan empiris dan rekomendasi kebijakan yang bias.

Oleh karena itu, terdapat urgensi akademis dan praktis yang sangat mendesak untuk mengumpulkan, meninjau ulang secara mendalam, dan menyelaraskan berbagai bukti empiris tersebut ke dalam satu kerangka analitis yang komprehensif. Pemetaan ulang atas pola adopsi teknologi dan interaksi pertukaran privasi ini merupakan langkah mitigasi esensial. Hal ini tidak hanya krusial bagi pelaku industri e-commerce sebagai acuan dasar untuk merekonstruksi tata kelola keamanan yang lebih adaptif, tetapi juga bernilai vital bagi institusi negara dalam mengevaluasi tingkat kesiapan dan efektivitas instrumen hukum perlindungan data konsumen di Indonesia (Hidayat & Kusuma, 2024). Berlandaskan pada identifikasi celah penelitian dan urgensi fenomena tersebut, artikel literature review ini diinisiasi dengan tujuan utama untuk menganalisis, mengkritisi secara objektif, serta mensintesis secara holistik pengaruh riil dari isu privasi data terhadap dinamika minat penggunaan platform e-commerce di Indonesia. Demi menjaga standar koherensi dan validitas argumen akademis, alur penulisan ini disusun secara sistematis dengan mengekstraksi desain dan metode riset (research methods) dari setiap literatur utama untuk menguji ketepatan alat ukur metodologisnya. Selanjutnya, kajian literatur ini akan merinci komparasi lintas studi atas ragam temuan lapangan (results/findings) yang membedah secara spesifik relasi kausal variabel psikologis dan perilaku pengguna. Pada tahap pemungkasnya, seluruh telaah kritis ini akan disarikan ke dalam kesimpulan integratif yang diharapkan mampu memecahkan teka-teki privacy paradox, sekaligus memberikan konstruksi kebaruan teoritis serta rekomendasi strategis demi terciptanya ekosistem lokapasar nasional yang tangguh, aman, dan konsisten menjunjung tinggi hak privasi konsumen**.**

2. KAJIAN TEORITIS

Tinjauan literatur ini berlandaskan pada beberapa teori utama yang saling berkaitan untuk menjelaskan perilaku konsumen dan interaksi mereka dengan teknologi e-commerce. Penelitian ini menggunakan kerangka Internet User Information Privacy Concerns (IUIPC) untuk mengukur tingkat kekhawatiran pengguna. Malhotra, Kim, dan Agarwal (2004)

merumuskan teori ini untuk menjelaskan bagaimana pengguna internet merespons praktik pengumpulan data oleh perusahaan. Konsep IUIPC membagi kekhawatiran privasi ke dalam empat dimensi utama. Dimensi tersebut meliputi ketakutan konsumen ketika platform mengambil data secara berlebihan di luar kebutuhan transaksi (pengumpulan data), kekhawatiran bahwa perusahaan akan menjual data kepada pihak lain tanpa persetujuan (penggunaan sekunder tanpa izin), ketakutan bahwa data pribadi diakses oleh pihak yang tidak berwenang (akses tidak tepat), serta kekhawatiran mengenai ketidakakuratan data yang tersimpan di dalam sistem perusahaan (kesalahan data).

Dalam merespons kekhawatiran privasi tersebut, literatur ini menyoroti sebuah keanehan perilaku konsumen yang dikenal sebagai teori paradoks privasi (privacy paradox). Barth dan de Jong (2017) menjelaskan bahwa paradoks privasi terjadi ketika konsumen memiliki tingkat kepedulian yang sangat tinggi terhadap keamanan data secara teori, tetapi mereka tetap membagikan informasi tersebut pada praktiknya. Konsumen secara sadar mengorbankan data pribadi mereka demi mendapatkan fitur kenyamanan, kemudahan berbelanja, atau potongan harga dari platform e-commerce. Untuk menjembatani perbedaan antara niat dan perilaku ini, teori kepercayaan (trust) memainkan peran yang sangat penting. Mayer, Davis, dan Schoorman (1995) mendefinisikan kepercayaan sebagai kesediaan konsumen untuk menerima risiko atas tindakan pihak e-commerce. Tingginya tingkat kepercayaan pada sebuah merek terbukti mampu mengurangi hambatan psikologis akibat ancaman privasi, sehingga konsumen tetap mau melanjutkan transaksi belanja.

Selain faktor kepercayaan, penelitian ini juga bersandar pada Technology Acceptance Model (TAM) yang dikembangkan oleh Davis (1989) untuk menjelaskan keputusan pengguna dalam menggunakan aplikasi. Teori TAM menguraikan bahwa pengguna mau menerima sebuah teknologi baru berdasarkan persepsi kebermanfaatan dan persepsi kemudahan penggunaan. Dalam konteks belanja daring, pengalaman pengguna yang mulus dan antarmuka aplikasi yang mudah digunakan ternyata mampu mengalahkan rasa takut pengguna terhadap risiko keamanan data. Sebagai solusi strategis atas seluruh dinamika tersebut, kajian ini mengangkat urgensi kebijakan privasi yang proaktif. Kurniawan dan Setiawan (2021) menyatakan bahwa perusahaan e-commerce harus mengevaluasi dan mengintegrasikan perlindungan privasi sejak fase awal perancangan sistem informasi, bukan sekadar menjadikannya sebagai tambahan di akhir proses pembuatan aplikasi. Pendekatan ini memastikan pengguna mendapatkan kendali atas data mereka sekaligus meningkatkan keunggulan kompetitif perusahaan.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan mengkaji sejumlah artikel dari jurnal internasional terakreditasi yang secara khusus meneliti isu privasi data konsumen dalam transaksi di platform e-commerce. Peneliti mengumpulkan sumber-sumber ilmiah yang relevan melalui beberapa basis data akademik terkemuka, seperti Google Scholar, Scopus, dan Web of Science, dengan menggunakan kata kunci utama berupa consumer privacy, data privacy, e-commerce, marketplace, dan online transaction. Artikel-artikel yang terpilih kemudian disaring berdasarkan kriteria inklusi, yaitu studi yang diterbitkan dalam sepuluh tahun terakhir, berbahasa Inggris atau Indonesia, serta secara spesifik membahas bagaimana isu privasi data memengaruhi perilaku dan minat konsumen dalam bertransaksi di marketplace daring. Artikel yang tidak memenuhi kriteria tersebut, seperti penelitian yang tidak berkaitan langsung dengan privasi data konsumen di lingkungan e-commerce atau tidak berasal dari jurnal yang terindeks, dikeluarkan dari proses telaah. Setelah seleksi dilakukan, peneliti mengekstrak data penting dari setiap artikel yang mencakup tujuan penelitian, metode yang digunakan, variabel yang dikaji, serta temuan utama yang dihasilkan. Seluruh data tersebut kemudian disintesis secara tematik untuk mengidentifikasi pola, konsensus, maupun perbedaan temuan antar studi, sehingga menghasilkan gambaran yang komprehensif mengenai pengaruh isu privasi data terhadap minat penggunaan platform e-commerce di Indonesia.

4. HASIL DAN PEMBAHASAN

Konstruksi Ancaman dan Kekhawatiran Privasi di Ekosistem Digital

Ekosistem e-commerce saat ini menjadikan data pribadi konsumen sebagai aset strategis yang sangat bernilai. Kondisi ini mendorong konsumen untuk menunjukkan tingkat kekhawatiran yang tinggi terhadap bagaimana platform ritel daring mengelola informasi mereka. Secara konseptual, kekhawatiran privasi mencakup empat dimensi utama: pengumpulan data yang berlebihan, penggunaan data secara sekunder tanpa izin, akses informasi yang tidak tepat, dan kesalahan pengelolaan data (Lutfi et al., 2022; Malhotra, Kim, & Agarwal, 2004). Konsumen merasa terancam ketika platform mengumpulkan data di luar batas kewajaran fungsional untuk keperluan transaksi..

Ancaman privasi ini mengalami eskalasi yang signifikan akibat intervensi teknologi analitik mahadata (big data analytics) dalam taktik pemasaran digital. Penggunaan kecerdasan buatan memungkinkan perusahaan e-commerce untuk merekam jejak data pengguna secara lebih mendalam (Lutfi et al., 2022). Praktik ekstraksi data ini memicu perdebatan akademis antara utilitas komersial dan pengawasan digital. Dalam konteks ini, konsumen sering kali

kehilangan kendali atas informasi pribadi mereka, yang memunculkan ketakutan akan pencurian identitas dan penyalahgunaan profil oleh pihak yang tidak bertanggung jawab (Mutambik et al., 2023; Yao & Tarofder, 2025).

Di Indonesia, ketegangan sistemik terkait keamanan data pribadi semakin nyata di tengah pertumbuhan masif sektor bisnis digital. Eskalasi ancaman siber berhadapan langsung dengan risiko persepsi konsumen (Sari & Rahmawati, 2023). Insiden kebocoran data berskala besar yang pernah menimpa beberapa raksasa e-commerce nasional menjadi preseden buruk yang memvalidasi persepsi ancaman tersebut di mata masyarakat. Dinamika ini diperparah oleh tantangan regulasi, di mana penegakan hukum pelindungan data yang terpadu secara nasional menjadi instrumen esensial yang sangat dibutuhkan (Ardika, 2025).

Dalam menjembatani kesenjangan antara kekhawatiran privasi dan niat transaksi tersebut, kepercayaan memainkan peran yang sangat fundamental. Kepercayaan konsumen terhadap merek e-commerce terbukti secara empiris mampu mengurangi hambatan psikologis yang ditimbulkan oleh ancaman privasi (Wibowo & Handayani, 2023; Yao & Tarofder, 2025). Ketika konsumen memercayai sebuah platform, mereka cenderung menoleransi pertukaran data karena mereka meyakini bahwa entitas ritel tersebut tidak akan menyalahgunakan informasi pribadi mereka. Lebih jauh, literatur mengonfirmasi bahwa kepercayaan berfungsi sebagai variabel mediator yang kuat. Sebuah studi menemukan bahwa persepsi pelanggan yang positif terhadap keamanan secara signifikan mendorong niat konsumen untuk membeli dan membagikan informasi (Prasetyo & Dewi, 2022).

Fenomena *Privacy Paradox* dan Peran Mediasi Kepercayaan (*Trust*)

Diskusi mengenai privasi informasi sering kali memunculkan sebuah anomali perilaku yang dikenal sebagai privacy paradox. Fenomena ini mendeskripsikan kondisi di mana konsumen menunjukkan tingkat kepedulian teoretis yang sangat tinggi terhadap keamanan data pribadi mereka, namun pada praktiknya, mereka tetap bersedia membagikan informasi tersebut (Al-Adwan & Al-Qur'an, 2022; Barth & de Jong, 2017; Yao & Tarofder, 2025). Anomali perilaku ini terjadi karena ketakutan pengguna terhadap pencurian identitas berbenturan secara kognitif dengan dorongan utilitarian (Mutambik et al., 2023). Konsumen cenderung mengorbankan data pribadi mereka demi mengeksploitasi kemudahan berbelanja, mendapatkan fitur kenyamanan, dan menikmati promosi yang ditawarkan oleh platform e-commerce.

Dalam menjembatani kesenjangan antara kekhawatiran privasi dan niat transaksi tersebut, kepercayaan memainkan peran yang sangat fundamental. Kepercayaan konsumen terhadap merek e-commerce terbukti secara empiris mampu mengurangi hambatan psikologis

yang ditimbulkan oleh ancaman privasi (Wibowo & Handayani, 2023; Yao & Tarofder, 2025). Ketika konsumen memercayai sebuah platform, mereka cenderung menoleransi pertukaran data karena mereka meyakini bahwa entitas ritel tersebut tidak akan menyalahgunakan informasi pribadi mereka. Lebih jauh, literatur mengonfirmasi bahwa kepercayaan berfungsi sebagai variabel mediator yang kuat. Sebuah studi menemukan bahwa persepsi pelanggan yang positif terhadap keamanan secara signifikan mendorong niat konsumen untuk membeli dan membagikan informasi (Prasetyo & Dewi, 2022).

Anomali Perilaku: Dampak Pengalaman Pengguna dan Literasi Sistem Informasi

Mayoritas literatur terdahulu mengasumsikan bahwa kekhawatiran privasi selalu menjadi hambatan utama. Namun, penelitian terbaru menemukan anomali empiris yang mematahkan konsensus tersebut. Pada kelompok konsumen tertentu, seperti mereka yang sangat terpengaruh oleh Fear of Missing Out (FOMO), kekhawatiran privasi dapat dikesampingkan demi mengikuti tren belanja (Bright & Logan, 2022). Selain itu, rekam jejak pengalaman pengguna justru mengambil alih peran dominan. Pengalaman pengguna yang positif dan mulus terbukti mampu menganulir ketakutan konsumen terhadap risiko privasi data, di mana kemudahan layanan menutupi kekhawatiran akan keamanan data (Utomo & Santoso, 2022). Fenomena ini sejalan dengan fondasi Technology Acceptance Model (TAM), di mana persepsi kemudahan penggunaan sering kali mengalahkan persepsi risiko (Davis, 1989)..

Lebih lanjut, anomali perilaku ini sangat dipengaruhi oleh tingkat literasi sistem informasi dari pengguna. Konsumen yang memiliki latar belakang literasi teknis yang tinggi, seperti mahasiswa yang mempelajari sistem informasi atau audit, menunjukkan pola perilaku yang unik (Amin, 2021). Demografi yang melek teknologi ini memiliki pemahaman yang lebih rasional terhadap cara kerja arsitektur keamanan digital. Mereka mampu membedakan antara ketakutan privasi yang bersifat teoretis dan ancaman siber yang nyata. Akibatnya, kelompok dengan literasi sistem informasi yang memadai tidak lagi menjadikan privasi sebagai hambatan kaku, melainkan menggunakan pengalaman sistem yang terbukti andal sebagai basis pengambilan keputusan.

Implikasi Strategis bagi Arsitektur Keamanan dan Pemasaran E-Commerce

Dinamika ancaman privasi menuntut perusahaan e-commerce untuk merombak strategi pengelolaan data. Eksekutif ritel digital tidak lagi dapat mengandalkan praktik pengumpulan data yang berlebihan, karena insiden pelanggaran justru akan meruntuhkan kepercayaan institusional secara fatal (Anaza & Zhao, 2021; Lutfi et al., 2022). Sebagai gantinya, platform e-commerce harus mengadopsi inisiatif perlindungan data terintegrasi. Perusahaan didorong untuk menyediakan kebijakan privasi yang jelas untuk menjamin kepercayaan pelanggan (Kurniawan & Setiawan, 2021).

Dari sisi arsitektur teknis, penyedia layanan wajib mengimplementasikan sistem keamanan yang mampu menekan persepsi risiko penggunanya (Sari & Rahmawati, 2023). Selain itu, perancang sistem e-commerce juga perlu menyesuaikan desain panel kontrol privasi agar selaras dengan profil demografis spesifik (Mutambik et al., 2023). Transformasi arsitektur keamanan ini menciptakan implikasi pemasaran yang krusial. Privasi telah berevolusi menjadi instrumen loyalitas pelanggan di industri ritel digital. Entitas korporasi dapat menjadikan jaminan perlindungan data yang kuat sebagai nilai jual utama dalam strategi pemasaran (Hidayat & Kusuma, 2024; Yao & Tarofder, 2025). Tingkat kepercayaan yang solid inilah yang pada akhirnya mendorong transaksi berkelanjutan di tengah lanskap digital.

Tabel 1. Ringkasan Temuan Literatur Review.

Tema / Sub-Bab Pembahasan	Ringkasan Temuan Utama (Key Findings)	Pengelompokan Sumber Artikel
1. Bentuk Ancaman dan Kekhawatiran Privasi	a. Konsumen khawatir akan pengambilan data berlebih, penyalahgunaan, dan akses ilegal sehingga teknologi analitik yang akhirnya meningkatkan ketakutan ini b. Penggunaan teknologi canggih seperti AI membuat ancaman ini makin besar, sehingga pengguna merasa kehilangan kendali atas informasi pribadi mereka. c. Di Indonesia, aturan yang belum jelas di masa lalu dan banyaknya kasus kebocoran data membuat masyarakat semakin takut akan risiko keamanan digital. d. Meskipun rasa takut ini menurunkan niat belanja, platform e-commerce tetap bisa mengatasinya dengan sistem keamanan yang kuat.	Ardika (2025); Kurniawan & Setiawan (2021); Lutfi et al. (2022); Malhotra, Kim, & Agarwal (2004); Mutambik et al. (2023); Sari & Rahmawati (2023); Yao & Tarofder (2025)
2. Fenomena Paradoks Privasi & Peran Kepercayaan	a. Ada sebuah keanehan (paradoks), di mana konsumen sebenarnya sangat khawatir pada privasi, tapi tetap rela membagikan datanya demi kemudahan belanja dan diskon.	Al-Adwan & Al-Qur'an (2022); Barth & de Jong (2017); Mutambik et al. (2023); Prasetyo & Dewi (2022); Wibowo & Handayani (2023); Yao & Tarofder (2025).

Tema / Sub-Bab Pembahasan	Ringkasan Temuan Utama (Key Findings)	Pengelompokan Sumber Artikel
	b. Kepercayaan (trust) berfungsi sebagai mediator inti yang mampu menurunkan resistensi konsumen saat berbelanja. c. Jika konsumen sudah sangat percaya pada sebuah merek e-commerce, mereka akan lebih maklum saat diminta membagikan data dan tetap mau berbelanja.	
3. Pengaruh Pengalaman Pengguna dan Pemahaman Teknologi	a. Pengalaman menggunakan aplikasi yang lancar, cepat, dan mudah ternyata bisa membuat konsumen mengabaikan ketakutan privasi b. Tingkat pemahaman teknologi sangat berpengaruh; pengguna yang melek teknologi bisa membedakan mana ketakutan yang berlebihan dan mana ancaman siber yang benar-benar nyata. c. Faktor kemudahan penggunaan aplikasi dan dorongan sosial (seperti FOMO) mampu mengalahkan kecemasan privas	Al-Adwan & Al-Qur'an (2022); Bright & Logan (2022); Davis (1989); Utomo & Santoso (2022).
4. Saran Strategi untuk Keamanan dan Pemasaran	a. E-commerce tidak boleh lagi mengambil data secara berlebihan atau memaksa. Mereka harus merancang sistem yang aman sejak awal dan membiarkan pengguna mengatur privasinya sendiri. b. Dari sisi teknis, e-commerce wajib memakai pengaman seperti sandi sekali pakai (OTP) dan membuat menu pengaturan privasi yang mudah digunakan oleh semua kalangan. c. Aturan privasi yang jelas dan bukti bahwa platform tersebut aman kini bisa dijadikan bahan promosi untuk menarik lebih banyak pelanggan.	Anaza & Zhao (2021); Hidayat & Kusuma (2024); Kurniawan & Setiawan (2021); Lutfi et al. (2022); Mutambik et al. (2023); Sari & Rahmawati (2023); Yao & Tarofder (2025).

Sumber : Penulis (2026)

5. KESIMPULAN DAN SARAN

Artikel tinjauan literatur ini merangkum dan menganalisis berbagai studi terdahulu untuk melihat bagaimana masalah privasi memengaruhi pengguna e-commerce. Berdasarkan hasil analisis, konsumen merasa sangat khawatir jika aplikasi mengambil data terlalu banyak, menyebarkannya tanpa izin, membiarkan pihak lain mengaksesnya, atau melakukan kesalahan sistem. Rasa takut ini semakin besar karena munculnya teknologi canggih seperti kecerdasan buatan dan maraknya kasus kebocoran data masa lalu di Indonesia. Dengan demikian, temuan mengonfirmasi adanya keanehan perilaku yang disebut paradoks privasi. Konsumen yang tadinya takut ternyata tetap rela menyerahkan data pribadi mereka demi mendapatkan diskon dan kemudahan saat berbelanja. Rasa percaya (*trust*) pada merek dan pengalaman menggunakan aplikasi yang lancar secara konsisten terbukti bisa mengalahkan ketakutan

pengguna terhadap risiko keamanan. Namun, tinjauan ini memiliki keterbatasan karena sebagian besar literatur terdahulu masih berfokus pada demografi konsumen secara umum di wilayah tertentu dan belum banyak membandingkan perilaku konsumen di berbagai latar belakang budaya yang berbeda secara lintas negara.

Bagi peneliti selanjutnya, terbuka peluang besar untuk memperluas area penelitian dengan menyebarkan kuesioner langsung pada target masyarakat di skala regional yang lebih spesifik, seperti kota-kota yang sedang berkembang pesat ekosistem digitalnya. Pengambilan data lokal ini akan memberikan sudut pandang perilaku konsumen yang lebih akurat dan sangat cocok untuk diangkat sebagai topik tugas akhir atau penelitian lanjutan tingkat sarjana. Selain itu, riset mendatang sebaiknya mulai menguji dampak langsung dari fitur-fitur baru, seperti interaksi pelanggan dengan *chatbot* otomatis, terhadap rasa aman pengguna.

Saran untuk Perusahaan E-Commerce sebaiknya tidak lagi hanya memikirkan keuntungan dari mengambil data pengguna. Perusahaan harus membangun sistem aplikasi yang melindungi privasi pelanggan sejak tahap perancangan awal. Pemilik aplikasi wajib memakai sistem pengaman tambahan seperti sandi sekali pakai (OTP) dan memberikan menu pengaturan yang memungkinkan pengguna mengontrol datanya sendiri. Pada akhirnya, perusahaan dapat menggunakan transparansi kebijakan privasi dan sistem yang terbukti aman ini sebagai nilai jual utama dalam materi promosi mereka untuk memenangkan kepercayaan pasar.

UCAPAN TERIMA KASIH

Artikel ini merupakan bagian dari hasil penelitian tugas akhir di Program Studi Manajemen, Universitas Ma Chung. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada Catharina Aprilia Hellyani, S.E., M.M., selaku dosen pembimbing, yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan arahan serta tinjauan kritis selama proses penulisan naskah ini. Penulis juga berterima kasih kepada pihak fakultas dan universitas yang telah memfasilitasi akses ke berbagai basis data literatur internasional

DAFTAR REFERENSI

Al-Adwan, A. S., & Al-Qur'an, H. (2022). E-commerce and consumer privacy: An empirical study of the privacy paradox. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(1), 120–135. https://doi.org/10.3390/jtaer17010008

Anaza, N. A., & Zhao, J. (2021). The impact of data privacy breaches on consumer trust in e-commerce. *International Journal of Information Management*, *57*, Article 102292. https://doi.org/10.1016/j.ijinfomgt.2020.102292

Ardika, I. W. C. (2025). Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce. *Indonesian Journal of Law and Justice, 2*(3), 11. https://doi.org/10.47134/ijlj.v2i3.3601

Bandara, R., Fernando, M., & Akter, S. (2021). Exposing the privacy paradox in the context of e-commerce: A grounded theory approach. *Electronic Markets, 31*(3), 629–647. https://doi.org/10.1007/s12525-020-00405-w

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bright, L. F., & Logan, K. (2022). Is my fear of missing out (FOMO) higher than my privacy concerns? A study of the privacy paradox in the e-commerce context. *Journal of Consumer Behaviour, 21*(5), 1032–1044. https://doi.org/10.1002/cb.2052

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Hidayat, M., & Kusuma, D. (2024). Perlindungan privasi konsumen dalam ekosistem bisnis digital dan pengaruhnya terhadap loyalitas. *Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship, 13*(2), 234–248. https://doi.org/10.30588/jmp.v13i2.1154

Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behaviour & Information Technology, 40*(1), 1–19. https://doi.org/10.1080/0144929X.2019.1584644

Kurniawan, B., & Setiawan, A. (2021). Evaluasi kebijakan privasi data pada aplikasi e-commerce terhadap kepercayaan konsumen. *Jurnal Sistem Informasi Bisnis, 11*(2), 150–158. https://doi.org/10.21456/vol11iss2pp150-158

Lutfi, A., Al-Okaily, M., Alsyouf, A., Alrawad, M., & Suryanto, T. (2022). Evaluating the big data analytics adoption in the e-commerce sector. *Sustainability, 14*(7), Article 4035. https://doi.org/10.3390/su14074035

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Mutambik, I., Lee, J., Almuqrin, A., Zhang, J. Z., Baihan, M., & Alkhanifer, A. (2023). Privacy concerns in social commerce: The impact of gender. *Sustainability, 15*(17), Article 12771. https://doi.org/10.3390/su151712771

Nuranisa, A., & Lukitasari, D. (2024). Tindak pidana pencurian data dan privasi pengguna dalam transaksi e-commerce (Studi kasus pada aplikasi Tokopedia). *Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, 1*(2), 115–126. https://doi.org/10.62383/amandemen.v1i2.145

Prasetyo, Y. T., & Dewi, A. (2022). Pengaruh kepercayaan, kualitas informasi, dan privasi terhadap niat beli konsumen pada platform e-commerce di Indonesia. *Jurnal Manajemen dan Pemasaran Jasa, 15*(1), 45–60. https://doi.org/10.25105/jmpj.v15i1.9213

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. https://doi.org/10.22225/juinhum.5.1.8482.903-913

Sari, N. P., & Rahmawati, E. (2023). Analisis persepsi risiko dan privasi data terhadap minat penggunaan dompet digital dan e-commerce. *Jurnal Ilmiah Ekonomi Bisnis*, *28*(2), 210–225.

Utomo, P., & Santoso, B. (2022). Mengurai paradoks privasi pengguna aplikasi e-commerce: Antara kenyamanan berbelanja dan risiko keamanan data. *Jurnal Ilmu Komunikasi, 20*(1), 77–92. https://doi.org/10.31315/jik.v20i1.4121

Wibowo, A., & Handayani, P. W. (2023). Dampak kebocoran data pengguna terhadap loyalitas pelanggan e-commerce: Peran mediasi kepercayaan merek. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 12*(1), 12–20. https://doi.org/10.22146/jnteti.v12i1.5642

Yao, H., & Tarofder, A. K. (2025). Impact of consumer self-efficacy on online purchase intention in Henan Province, China. *International Journal of Innovative Research and Scientific Studies*, *8*(1), 481–489. https://doi.org/10.53894/ijirss.v8i1.4181

Zafira, N., Aisyahara, N., Safriana, C. A., Rofli, & Hafizatunnisa. (2026). Analisis keamanan data pengguna pada platform e-commerce: Studi kasus kebocoran data Tokopedia 2020. *JIKUM: Jurnal Ilmu Komputer*, *2*(1), 117–123. https://doi.org/10.62671/jikum.v2i1.174