Jurnal Siber Multi Disiplin (JSMD)
E-ISSN: 2987-0380
P-ISSN: 2987-0402
+62 822 1012 3600 https://research.e-siber.org siberpublisher.info@gmail.com
DOI: https://doi.org/10.38035/jsmd.v3i3

Keamanan E-Commerce: Cara Menjaga Data Pribadi Tetap Aman

Reny Ernitasari[1], Suci Ramdhani[2], Yuliusman[3], Muhammad Gowon[4]
[1]Magister Ilmu Akuntansi, Pascasarjana Universitas Jambi, Indonesia, renyernita@gmail.com
[2]Magister Ilmu Akuntansi, Pascasarjana Universitas Jambi, Indonesia, ramadhanisuci2022@gmail.com
[3]Magister Ilmu Akuntansi, Pascasarjana Universitas Jambi, Indonesia, yuliusman@unja.ac.id
[4]Magister Ilmu Akuntansi, Pascasarjana Universitas Jambi, Indonesia, gowon@unja.ac.id

Corresponding Author: renyernita@gmail.com[1]

Abstract: *This study, titled "E-Commerce Security: How to Keep Personal Data Safe," aims to analyze personal data protection efforts in digital transactions and to describe various threats that arise in the use of e-commerce platforms. The research object consists of scientific articles discussing data security within e-commerce services. This study employs the Systematic Literature Review method to identify, evaluate, and synthesize findings from relevant publications. The results show that threats to personal data, including data breaches, identity theft, and manipulative online activities, remain prevalent and are influenced by both technical weaknesses and user behavior. Several protection strategies, such as layered authentication, data encryption, system monitoring, and improved user awareness, are found to be effective in enhancing security. Based on the analysis, this research concludes that personal data protection in e-commerce requires a comprehensive approach that integrates technological strengthening, improved digital literacy, proper risk management, and effective regulatory support.*

Keyword: *E-commerce security, Personal data protection, Digital security, Cyber risk, Information security management.*

Abstrak: Penelitian berjudul "Keamanan E-Commerce: Cara Menjaga Data Pribadi Tetap Aman" ini bertujuan menganalisis upaya perlindungan data pribadi dalam transaksi digital serta menggambarkan berbagai ancaman yang muncul dalam penggunaan layanan e-commerce. Objek penelitian adalah artikel ilmiah yang membahas keamanan data pada platform e-commerce. Penelitian menggunakan metode Systematic Literature Review untuk mengidentifikasi, menilai, dan mensintesis temuan dari berbagai publikasi yang relevan. Hasil penelitian menunjukkan bahwa ancaman terhadap data pribadi, seperti kebocoran data, pencurian identitas, dan aktivitas manipulatif pada transaksi digital, masih sering terjadi dan dipengaruhi oleh faktor teknis serta perilaku pengguna. Berbagai strategi perlindungan, seperti autentikasi berlapis, enkripsi data, pengawasan sistem, dan peningkatan pemahaman pengguna, terbukti berperan penting dalam meningkatkan keamanan. Berdasarkan hasil analisis, penelitian ini menyimpulkan bahwa perlindungan data pribadi dalam e-commerce memerlukan

pendekatan menyeluruh yang mencakup penguatan teknologi, peningkatan literasi digital, manajemen risiko yang baik, serta dukungan regulasi yang efektif.

Kata Kunci: Keamanan E-Commerce, Perlindungan data Pribadi, Keamanan Digital, Risiko siber, Manajemen keamanan informasi.

PENDAHULUAN

Perkembangan teknologi digital telah mendorong peningkatan signifikan dalam penggunaan *e-commerce* sebagai media transaksi modern. Masyarakat semakin mengandalkan platform digital untuk memenuhi kebutuhan sehari-hari karena kemudahan akses, kecepatan layanan, dan efisiensi waktu. Namun, kemajuan ini juga memunculkan tantangan baru terkait keamanan data pribadi pengguna. Berbagai insiden seperti pencurian identitas, kebocoran informasi pelanggan, dan penipuan transaksi menunjukkan bahwa aktivitas di *e-commerce* tidak terlepas dari risiko kejahatan siber (Suryanto, 2021). Kondisi tersebut menuntut penerapan mekanisme keamanan yang kuat agar data pribadi tetap terlindungi.

Dalam konteks keamanan informasi, konsep *cybersecurity* berfokus pada perlindungan sistem, jaringan, dan data digital dari akses ilegal, gangguan, atau serangan berbahaya (Stallings, 2019). Model keamanan klasik menekankan tiga komponen utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), yang dikenal sebagai prinsip CIA Triad (Whitman & Mattord, 2020). Pada *e-commerce*, perlindungan ini sangat penting karena platform digital mengumpulkan dan memproses data sensitif seperti informasi identitas, alamat, histori transaksi, hingga data pembayaran pengguna.

Selain aspek teknis, perilaku pengguna juga memengaruhi tingkat keamanan. Rendahnya kesadaran terhadap ancaman siber seperti *phishing*, *malware*, dan rekayasa sosial (*social engineering*) dapat meningkatkan kerentanan akun pengguna terhadap serangan (Pangestu, 2022). Dengan demikian, keamanan *e-commerce* bukan hanya bergantung pada teknologi yang digunakan, tetapi juga pada pemahaman dan perilaku pengguna dalam menjaga kerahasiaan data pribadinya.

Penelitian mengenai keamanan *e-commerce* telah dilakukan dalam berbagai pendekatan, namun hasil-hasil penelitian tersebut masih tersebar dan memiliki fokus yang berbeda-beda. Oleh karena itu, diperlukan sebuah kajian sistematis untuk merangkum temuan ilmiah terkini, memetakan risiko yang paling sering terjadi, serta mengidentifikasi strategi perlindungan data yang terbukti efektif. Pendekatan *Systematic Literature Review* atau SLR dipilih untuk memberikan pemahaman komprehensif mengenai bagaimana data pribadi dapat dijaga dalam konteks *e-commerce* melalui analisis literatur secara terstruktur dan terstandar (Kitchenham, 2004).

Tujuan penelitian ini adalah untuk menjawab pertanyaan penelitian berikut: bagaimana bentuk ancaman keamanan terhadap data pribadi dalam *e-commerce*, strategi apa saja yang digunakan untuk melindungi data pribadi pengguna, dan bagaimana efektivitas pendekatan keamanan yang telah dikembangkan dalam penelitian-penelitian sebelumnya. Hasil penelitian ini diharapkan mampu memberikan gambaran menyeluruh mengenai kondisi keamanan *e-commerce* dan memberikan arah bagi penelitian selanjutnya sehingga perlindungan data pribadi dapat ditingkatkan secara optimal.

METODE

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengidentifikasi, menilai, dan menginterpretasikan berbagai penelitian yang relevan terkait keamanan *e-commerce* dan upaya menjaga data pribadi tetap aman dalam transaksi digital. Pendekatan SLR dipilih untuk memberikan gambaran yang komprehensif mengenai

perkembangan penelitian, strategi perlindungan data pribadi, serta risiko-risiko keamanan yang sering dibahas dalam literatur, sehingga hasil yang diperoleh memiliki tingkat keandalan dan validitas yang tinggi. Seluruh proses peninjauan dilakukan secara sistematis melalui tahapan pencarian, seleksi, ekstraksi, dan analisis literatur yang memenuhi kriteria inklusi.

Data dikumpulkan dari berbagai sumber literatur yang kredibel dan relevan. Informasi yang diekstraksi dari setiap artikel meliputi judul penelitian, nama penulis, tahun publikasi, tujuan penelitian, metode penelitian yang digunakan, jenis ancaman keamanan yang dibahas, teknik atau pendekatan perlindungan data pribadi yang diterapkan, serta temuan utama terkait efektivitas upaya keamanan dalam *e-commerce*. Ekstraksi data dilakukan untuk memastikan bahwa setiap artikel memberikan kontribusi terhadap pemahaman mengenai bagaimana data pribadi dapat dilindungi dalam lingkungan digital.

Kata kunci yang digunakan dalam proses pencarian literatur meliputi *cybersecurity*, *e-commerce security*, *data privacy*, *personal data protection*, *online security threats*, *information security*, dan *consumer data protection*. Variasi kombinasi kata kunci tersebut digunakan untuk menjangkau literatur yang relevan di berbagai basis data seperti *Google Scholar*, dan portal jurnal nasional. Artikel yang disertakan adalah artikel ilmiah yang dipublikasikan dalam jurnal bereputasi dari tahun 2020 hingga 2025, sesuai dengan rentang waktu perkembangan isu keamanan *e-commerce* yang paling signifikan.

Data yang telah diekstraksi dianalisis secara deskriptif dan tematik. Analisis deskriptif digunakan untuk menggambarkan karakteristik umum dari studi yang termasuk dalam tinjauan, seperti distribusi tahun publikasi, metode penelitian yang digunakan, fokus penelitian, dan jenis ancaman keamanan yang paling banyak dibahas. Selanjutnya, analisis tematik dilakukan untuk mengidentifikasi tema-tema utama yang muncul dari literatur, terutama terkait bentuk ancaman keamanan, teknik perlindungan data pribadi, serta efektivitas strategi *cybersecurity* dalam mencegah penyalahgunaan data pengguna. Analisis tematik juga digunakan untuk memetakan hubungan antara ancaman yang muncul dan strategi perlindungan yang diusulkan dalam berbagai penelitian.

HASIL DAN PEMBAHASAN

Hasil

Tabel 1. Ringkasan Jurnal yang di Review

Judul	Penulis dan Tahun	Temuan
Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia	(Priliasari 2023)	Indonesia kini memiliki dasar hukum kuat untuk melindungi data pribadi melalui UU PDP 2022. Marketplace wajib menjaga keamanan data konsumen dan memberi pemberitahuan jika terjadi kebocoran. Banyak kasus kebocoran terjadi karena lemahnya sistem keamanan, sehingga marketplace dapat dikenai sanksi dan digugat secara perdata. Konsumen memiliki hak atas keamanan data dan dapat mengajukan pengaduan. Artikel juga menekankan perlunya lembaga pengawas data pribadi serta peningkatan literasi digital masyarakat.
Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce	(Nafi'ah 2020)	Artikel ini menemukan bahwa pelanggaran data dan pencurian identitas di e-commerce semakin meningkat karena lemahnya keamanan dan minimnya perlindungan data pribadi. Kasus

		kebocoran pada Tokopedia, Bukalapak, dan Bhinneka menunjukkan data pengguna tidak diamankan dengan baik. Regulasi sebenarnya sudah ada, tetapi penegakannya lemah. E-commerce perlu memperkuat enkripsi, protokol keamanan, dan pengelolaan internal karena selama data mudah diakses, ancaman pencurian identitas akan terus terjadi.
Algoritma Autentikasi Multi Factor Sebagai Solusi Untuk Meningkatkan Keamanan Sistem Pembayaran E-Commerce	(Melyana, Darmawan, and Syah 2024)	Artikel ini menemukan bahwa Autentikasi Multi-Faktor (AMF) efektif meningkatkan keamanan pembayaran e-commerce dengan menambah lapisan verifikasi seperti OTP atau biometrik. AMF mampu secara signifikan menurunkan risiko phishing, peretasan, dan pencurian identitas, sehingga mencegah akses ilegal dan meningkatkan kepercayaan konsumen.
Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi	(Cahyaaty, Wijaya, and Dafin Al Dzky 2024)	Artikel ini menemukan bahwa Shopee telah menerapkan langkah keamanan seperti enkripsi data dan autentikasi dua faktor (2FA), namun pemahaman pengguna terhadap kebijakan keamanan masih rendah—sebanyak 28,26% tidak mengetahui kebijakan tersebut. Meski 68,84% pengguna merasa data mereka aman, lebih dari 30% tetap merasa terancam dan 52,90% ragu membagikan data pribadinya. Hal ini menunjukkan bahwa meskipun sistem keamanan Shopee cukup baik, edukasi, transparansi, dan komunikasi mengenai perlindungan data perlu ditingkatkan untuk memperkuat kepercayaan pengguna.
Perlindungan Data Identitas Konsumen Dalam Transaksi E-Commerce Berdasarkan Undang Undang No. 27 Tahun 2022 Perlindungan Data Pribadi	(Kurniastuti and Prastyanti 2025)	Artikel ini menemukan bahwa UU No. 27 Tahun 2022 memberikan dasar hukum kuat untuk melindungi data identitas konsumen dalam e-commerce, tetapi kasus kebocoran data yang terus meningkat menunjukkan bahwa regulasi saja tidak cukup. Perlindungan data tetap membutuhkan kesadaran digital konsumen, seperti penggunaan 2FA, password kuat, dan memilih platform yang aman.
Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Pembayaran E-Commerce Titin	(Sumarni et al. 2024)	Artikel ini menemukan bahwa ancaman siber terhadap sistem pembayaran e-commerce semakin meningkat dan berdampak pada keamanan data serta kepercayaan pengguna. Penipuan digital banyak terjadi karena rendahnya literasi pengguna, kebocoran data, iming-iming hadiah palsu, dan lemahnya pengawasan keamanan. Bentuk penipuan yang sering terjadi termasuk phishing, pharming, pretexting, quid pro quo, serta penipuan melalui

		kontak langsung. Untuk mengatasi hal tersebut, diperlukan strategi keamanan yang mencakup manajemen risiko, penerapan cybersecurity, edukasi pengguna, dan pelatihan sumber daya manusia. Pemerintah juga telah menetapkan regulasi seperti UU ITE dan UU Perlindungan Konsumen, meskipun pelaksanaannya perlu diperkuat. Secara umum, artikel ini menegaskan bahwa keamanan e-commerce memerlukan kolaborasi antara teknologi, pengguna, pemerintah, dan pelaku industri agar transaksi tetap aman dan terpercaya.
Pengaruh Citra Merek dan Keamanan Data Terhadap Minat Beli Pada E-Commerce Shopee (Studi Literature Review)	(Saputra et al. 2024)	Artikel ini menemukan bahwa minat beli konsumen pada platform e-commerce Shopee dipengaruhi oleh dua faktor utama, yaitu citra merek dan keamanan data. Citra merek yang positif dapat meningkatkan kepercayaan, preferensi, dan ketertarikan konsumen terhadap Shopee sehingga mendorong niat membeli. Selain itu, keamanan data juga terbukti berpengaruh karena konsumen semakin peduli terhadap perlindungan informasi pribadi saat bertransaksi secara online. Dengan demikian, semakin baik citra merek dan semakin tinggi tingkat keamanan data yang diberikan, maka semakin besar pula minat beli konsumen dalam menggunakan Shopee sebagai platform belanja.
The Importance of Protecting E-Commerce Consumer Personal Data	(Kurniawan 2024)	Artikel ini menemukan bahwa perlindungan data pribadi konsumen dalam e-commerce memiliki peran penting dalam meningkatkan rasa aman dan kepuasan pengguna saat bertransaksi secara online. Keamanan informasi seperti identitas, alamat, dan data pembayaran menjadi faktor yang menentukan tingkat kepercayaan konsumen kepada penyedia layanan e-commerce. Ketika data pribadi terlindungi dengan baik, konsumen cenderung merasa percaya dan lebih loyal dalam menggunakan layanan e-commerce dibandingkan dengan metode belanja konvensional. Artikel ini juga menekankan bahwa keamanan data tidak hanya bergantung pada penyedia platform, tetapi juga pada kesadaran pengguna untuk menjaga kerahasiaan informasi pribadinya. Selain itu, regulasi hukum seperti UU ITE dan aturan terkait lainnya menjadi penting untuk memberikan perlindungan dan kepastian hukum bagi konsumen dalam transaksi digital.

Legal Analysis of Consumer Protection in E-Commerce Transactions in Indonesia Post Personal Data Protection Law	(Sinaga, Pane, and Awira 2025)	Artikel ini menemukan bahwa meskipun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang lebih kuat bagi perlindungan konsumen dalam transaksi e-commerce, implementasinya di lapangan masih menghadapi berbagai hambatan serius. Tantangan utama meliputi rendahnya literasi digital konsumen, kurangnya kesadaran hukum pelaku usaha, serta lemahnya mekanisme pengawasan dan penegakan hukum atas pelanggaran data pribadi. Selain itu, terdapat kesenjangan antara perkembangan teknologi dan regulasi, sehingga aturan yang ada belum sepenuhnya mampu menjawab dinamika pesat di sektor e-commerce. Penelitian ini menegaskan perlunya peningkatan edukasi hukum, penguatan pengawasan, serta penyusunan regulasi turunan yang lebih adaptif agar ekosistem e-commerce dapat berjalan secara lebih aman, adil, dan berkelanjutan.
Protection of Personal Data in the Context of E-Commerce	(Mori, Dakic, and Regvart 2024)	Artikel ini menemukan bahwa kepuasan pelanggan dalam penggunaan e-commerce sangat dipengaruhi oleh faktor keamanan digital. Elemen seperti perlindungan data pribadi, keamanan transaksi, regulasi hukum yang jelas, serta penerapan sistem keamanan siber yang memadai menjadi faktor kunci yang menentukan tingkat kepercayaan dan kenyamanan pengguna saat berbelanja online. Semakin baik aspek-aspek keamanan tersebut diterapkan, semakin tinggi tingkat kepuasan konsumen dalam melakukan transaksi melalui platform e-commerce.

Dari tabel 1. Dapat dilihat beberapa temuan utama terkait keamanan e-commerce dan cara menjaga data pribadi tetap aman, aitu sebagai berikut:

Jenis Ancaman Keamanan dalam E-Commerce

Hasil SLR menunjukkan bahwa ancaman keamanan dalam e-commerce semakin beragam dan kompleks seiring meningkatnya penggunaan platform digital untuk transaksi. Nafi'ah (2020) mengungkapkan bahwa kebocoran data berskala besar yang terjadi pada Tokopedia dan Bukalapak menjadi bukti bahwa sistem keamanan e-commerce di Indonesia masih rentan terhadap serangan eksternal. Kasus tersebut tidak hanya memperlihatkan kelemahan pada perlindungan basis data, tetapi juga menunjukkan bahwa kemampuan pelaku serangan dalam mengeksploitasi celah keamanan semakin meningkat. Selain kebocoran data, serangan rekayasa sosial seperti *phishing*, *smishing*, dan *pretexting* juga menjadi ancaman utama. Sumarni, Rahayu, dan Arifin (2024) menegaskan bahwa teknik penipuan berbasis manipulasi psikologis ini menjadi semakin efektif karena pengguna sering kali tidak menyadari bahwa mereka sedang diarahkan untuk memberikan informasi sensitif seperti kata sandi, PIN, atau kode OTP.

Selain itu, ancaman terhadap sistem pembayaran digital juga menjadi fokus penting dalam literatur penelitian. Sumarni et al. (2024) menemukan bahwa pencurian data kartu kredit, akses ilegal ke akun dompet digital, dan penyalahgunaan transaksi *online* merupakan bentuk ancaman yang paling sering terjadi dan berdampak langsung terhadap kerugian finansial konsumen. Serangan *malware* dan *spyware* juga disebut sebagai ancaman serius karena mampu mencuri data pribadi secara diam-diam melalui perangkat pengguna tanpa disadari. Lebih jauh lagi, beberapa penelitian menyoroti munculnya serangan *credential stuffing*, yaitu upaya masuk ke akun konsumen dengan memanfaatkan kombinasi email dan kata sandi yang telah bocor dari platform lain. Ancaman ini semakin tinggi karena kebanyakan pengguna menggunakan kata sandi yang sama untuk banyak platform.

Faktor Penyebab Kerentanan Data Pengguna

Kerentanan data pengguna pada platform e-commerce tidak hanya berasal dari aspek teknis sistem, tetapi juga sangat dipengaruhi oleh faktor manusia dan perilaku pengguna. Cahyaaty, Rumapea, dan Lumbantobing (2024) menjelaskan bahwa rendahnya literasi digital merupakan salah satu penyebab utama meningkatnya risiko kebocoran data. Banyak pengguna tidak memahami cara kerja serangan siber dan sering kali mengabaikan tanda-tanda ancaman seperti tautan mencurigakan, permintaan informasi pribadi melalui pesan singkat, atau situs palsu yang menyerupai halaman resmi e-commerce. Kurangnya edukasi mengenai keamanan digital membuat pengguna mudah terjebak dalam serangan *phishing*, *smishing*, dan berbagai bentuk rekayasa sosial lainnya. Kondisi ini semakin diperparah oleh kecenderungan pengguna untuk menyetujui syarat dan ketentuan penggunaan tanpa membaca atau memahami kebijakan privasi platform yang mereka gunakan.

Selain faktor perilaku pengguna, kelemahan pada pengelolaan autentikasi akun juga menjadi penyebab kerentanan yang signifikan. Melyana, Friska, dan Yola (2024) menyoroti bahwa penggunaan kata sandi yang sederhana, penggunaan ulang kata sandi yang sama pada banyak platform, serta ketidakmaksimalan fitur autentikasi berlapis membuat akun pengguna lebih mudah diambil alih. Kebiasaan pengguna menyimpan kata sandi pada perangkat yang tidak aman atau membagikan OTP kepada orang lain juga meningkatkan risiko akses ilegal. Lebih jauh lagi, penelitian tersebut menunjukkan bahwa walaupun fitur keamanan seperti *multi-factor authentication* (MFA) dan *two-factor authentication* (2FA) telah disediakan oleh platform e-commerce, tingkat pemanfaatannya masih rendah karena kurangnya kesadaran pengguna tentang pentingnya perlindungan berlapis.

Faktor teknis juga turut menyumbang terhadap kerentanan keamanan data. Beberapa platform e-commerce masih menghadapi masalah dalam memperbarui sistem keamanan secara berkala atau menerapkan protokol enkripsi yang memadai. Sumarni, Rahayu, dan Arifin (2024) mencatat bahwa celah sistem seperti kode program yang belum diperbarui, konfigurasi server yang kurang optimal, serta kurangnya pengawasan keamanan pada sistem pembayaran membuat data pengguna semakin rentan dieksploitasi. Kelemahan teknis ini sering kali disebabkan oleh keterbatasan sumber daya manusia yang memiliki kompetensi keamanan siber serta belum adanya standar keamanan internal yang ketat pada sebagian penyedia layanan e-commerce.

Dengan demikian, faktor penyebab kerentanan data pengguna merupakan kombinasi dari kelemahan individu pengguna, keterbatasan kesadaran keamanan digital, serta kekurangan dalam infrastruktur dan pengelolaan keamanan platform. Perpaduan faktor-faktor ini membuat pengguna e-commerce lebih rentan menjadi target serangan siber. Oleh karena itu, perlindungan data pribadi tidak hanya memerlukan perbaikan teknologi keamanan, tetapi juga peningkatan edukasi pengguna dan penguatan manajemen keamanan oleh penyedia platform.

Strategi dan Teknologi Perlindungan Data Pribadi

Penelitian menunjukkan bahwa perlindungan data pribadi dalam e-commerce sangat bergantung pada penerapan teknologi keamanan yang berlapis. Melyana, Friska, dan Yola (2024) menekankan bahwa penggunaan *multi-factor authentication* (MFA) merupakan salah satu strategi paling efektif dalam mencegah pengambilalihan akun secara ilegal. Dengan memverifikasi identitas pengguna melalui lebih dari satu metode, seperti kata sandi, OTP, atau biometrik, MFA mampu mengurangi risiko ketika kredensial utama dicuri oleh pihak yang tidak berwenang. Namun, pemanfaatannya masih rendah karena banyak pengguna merasa langkah tersebut merepotkan atau tidak memahami manfaatnya.

Selain autentikasi berlapis, enkripsi data juga menjadi salah satu mekanisme utama dalam menjaga kerahasiaan informasi sensitif. Cahyaaty, Rumapea, dan Lumbantobing (2024) menemukan bahwa platform seperti Shopee telah menerapkan enkripsi dalam proses transmisi dan penyimpanan data untuk memastikan bahwa informasi pribadi tidak dapat dibaca atau dimanfaatkan oleh pihak yang tidak sah. Meskipun demikian, penelitian tersebut menunjukkan bahwa masih banyak pengguna yang tidak memahami cara kerja enkripsi atau kebijakan keamanan yang diterapkan, sehingga muncul persepsi keliru bahwa sistem e-commerce kurang aman.

Di sisi lain, strategi perlindungan data pribadi tidak hanya mencakup teknologi, tetapi juga manajemen risiko dan kebijakan internal perusahaan. Sumarni, Rahayu, dan Arifin (2024) menegaskan bahwa perusahaan harus mengimplementasikan sistem deteksi ancaman secara *real-time*, melakukan pembaruan sistem secara berkala, serta menerapkan audit keamanan untuk mengidentifikasi celah yang berpotensi diserang. Selain itu, pelatihan sumber daya manusia dalam keamanan digital juga menjadi faktor penting agar setiap aktivitas operasional sesuai standar. Oleh karena itu, upaya perlindungan data pribadi yang efektif harus mengintegrasikan teknologi, prosedur manajemen risiko, dan edukasi pengguna secara seimbang.

Dampak Keamanan Data terhadap Kepercayaan dan Perilaku Konsumen

Penelitian dalam SLR ini menunjukkan bahwa keamanan data merupakan faktor penting yang memengaruhi kepercayaan konsumen dalam menggunakan platform e-commerce. Saputra, Fatika, dan Huda (2024) menemukan bahwa tingkat keamanan data yang baik meningkatkan rasa aman konsumen, yang kemudian berdampak positif pada minat mereka untuk melakukan transaksi. Pengguna cenderung lebih loyal dan bersedia melakukan pembelian berulang apabila mereka mengetahui bahwa platform tersebut memiliki mekanisme perlindungan data pribadi yang kuat. Dengan demikian, keamanan data bukan hanya tambahan layanan, tetapi menjadi komponen utama dalam membentuk persepsi positif terhadap sebuah platform e-commerce.

Selain memengaruhi minat beli, keamanan data juga berperan dalam membangun citra dan reputasi sebuah platform. Nafi'ah (2020) menjelaskan bahwa kasus kebocoran data yang terjadi pada beberapa e-commerce besar memberikan dampak signifikan terhadap kepercayaan publik. Kejadian tersebut tidak hanya menimbulkan kerugian bagi pengguna, tetapi juga menurunkan reputasi perusahaan secara keseluruhan. Banyak pengguna menjadi lebih berhati-hati dalam memberikan informasi pribadi mereka dan beralih ke platform yang dianggap lebih aman. Hal ini menunjukkan bahwa satu insiden keamanan dapat berdampak jangka panjang pada perilaku dan persepsi konsumen.

Lebih jauh lagi, beberapa penelitian menyoroti bahwa transparansi mengenai kebijakan privasi dan perlindungan data memiliki pengaruh besar terhadap keputusan pengguna. Cahyaaty, Rumapea, dan Lumbantobing (2024) menemukan bahwa konsumen lebih percaya kepada platform yang menjelaskan secara jelas bagaimana data mereka dikumpulkan, disimpan, dan digunakan. Konsumen juga merasa lebih aman jika perusahaan memberikan informasi tentang teknologi keamanan yang diterapkan, seperti enkripsi dan autentikasi dua

faktor. Dengan kata lain, selain menjaga sistem keamanan yang kuat, kemampuan platform untuk berkomunikasi secara terbuka mengenai kebijakan privasi merupakan faktor penting yang meningkatkan kepercayaan dan kenyamanan pengguna.

Peran Regulasi dalam Perlindungan Data Pribadi

Regulasi memainkan peran penting dalam memperkuat perlindungan data pribadi pengguna e-commerce. Priliasari (2023) menegaskan bahwa keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum yang jelas bagi penyelenggara sistem elektronik dalam mengelola dan melindungi data konsumen. Undang-undang ini mengatur kewajiban platform untuk menjaga kerahasiaan data, melaporkan insiden keamanan, serta menerapkan standar perlindungan yang sesuai. Dengan adanya payung hukum tersebut, pengguna memiliki dasar hukum untuk menuntut perlindungan dan transparansi dari penyedia layanan digital.

Namun, meskipun regulasi telah diterapkan, implementasinya masih menghadapi berbagai tantangan. Sinaga, Hutagalung, dan Sari (2025) menjelaskan bahwa banyak pelaku usaha belum sepenuhnya siap menerapkan standar yang ditetapkan dalam undang-undang karena keterbatasan infrastruktur keamanan serta kurangnya pemahaman mengenai kewajiban kepatuhan data. Selain itu, pengawasan yang belum optimal menyebabkan beberapa platform e-commerce belum menjalankan kewajiban perlindungan data secara maksimal. Kesenjangan antara ketentuan hukum dan praktik di lapangan ini menunjukkan perlunya penguatan mekanisme pengawasan dan peningkatan kapasitas pelaku industri.

Selain aspek kepatuhan penyedia layanan, literatur juga menunjukkan bahwa efektivitas regulasi sangat dipengaruhi oleh tingkat literasi digital masyarakat. Kurniastuti dan Prastyanti (2025) menyoroti bahwa meskipun regulasi tentang perlindungan data pribadi telah ada, pengguna masih sering mengabaikan kebijakan privasi atau tidak memahami hak-hak mereka sebagai pemilik data. Rendahnya kesadaran konsumen terhadap perlindungan data membuat mereka tidak mampu memanfaatkan regulasi yang ada untuk melindungi diri. Oleh karena itu, regulasi yang baik perlu diikuti dengan edukasi yang memadai agar pengguna dapat berperan aktif dalam menjaga keamanan data pribadinya.

Pembahasan

Pembahasan dalam penelitian ini menunjukkan bahwa keamanan e-commerce dan perlindungan data pribadi merupakan isu multidimensional yang dipengaruhi oleh faktor teknis, perilaku pengguna, dan efektivitas regulasi. Temuan dari berbagai penelitian yang direview memperlihatkan bahwa ancaman terhadap data pribadi konsumen semakin beragam seiring pesatnya perkembangan teknologi digital. Ancaman seperti kebocoran data, pencurian identitas, dan serangan rekayasa sosial semakin meningkat tidak hanya karena tingkat kemampuan pelaku kejahatan siber yang semakin tinggi, tetapi juga karena masih adanya kelemahan pada infrastruktur keamanan platform e-commerce. Penelitian Nafi'ah (2020) dan Sumarni et al. (2024) menunjukkan bahwa penyedia layanan belum sepenuhnya mampu mengantisipasi pola serangan yang terus berkembang, sehingga kerentanan sistem masih menjadi salah satu penyebab utama pelanggaran data.

Selain kelemahan teknis, pembahasan juga menunjukkan bahwa perilaku pengguna berperan besar dalam meningkatkan risiko keamanan data. Banyak penelitian, seperti yang dilakukan oleh Cahyaaty et al. (2024), mengungkapkan bahwa rendahnya literasi digital membuat pengguna lebih mudah terjebak dalam serangan *phishing*, tautan palsu, dan permintaan informasi sensitif yang tidak valid. Masalah ini diperburuk dengan kebiasaan pengguna yang masih menggunakan kata sandi lemah, membagikan kode OTP, atau mengabaikan notifikasi keamanan. Meski fitur keamanan canggih seperti *multi-factor authentication* telah tersedia, tingkat pemanfaatannya masih rendah karena pengguna belum

memahami pentingnya perlindungan berlapis. Hal ini menunjukkan bahwa meskipun teknologi keamanan tersedia, efektivitasnya tetap bergantung pada tingkat kesadaran dan perilaku pengguna.

Di sisi lain, berbagai strategi perlindungan data pribadi telah diidentifikasi sebagai langkah yang dapat meminimalkan risiko. Melyana et al. (2024) dan Sumarni et al. (2024) menunjukkan bahwa penerapan MFA, enkripsi data, deteksi ancaman otomatis, dan manajemen risiko keamanan menjadi fondasi utama dalam membangun sistem perlindungan data yang kuat. Namun, penelitian-penelitian tersebut juga menegaskan bahwa teknologi tidak dapat berdiri sendiri tanpa didukung kebijakan internal perusahaan yang jelas, audit keamanan yang berkelanjutan, serta pelatihan sumber daya manusia dalam menjaga keamanan sistem. Upaya perlindungan data perlu dilakukan secara holistik dengan melibatkan aspek teknis, manajerial, serta edukasi kepada pengguna agar mampu menciptakan lingkungan transaksi yang aman.

Pembahasan juga menunjukkan bahwa regulasi memiliki peran sentral dalam meningkatkan perlindungan data pribadi. UU No. 27 Tahun 2022 memberikan dasar hukum yang kuat bagi perlindungan data di Indonesia, tetapi sejumlah penelitian seperti Priliasari (2023) dan Sinaga et al. (2025) menyoroti bahwa implementasi di lapangan masih belum optimal. Banyak pelaku usaha belum menerapkan standar perlindungan data yang sesuai karena keterbatasan infrastruktur, kurangnya pengawasan, serta rendahnya kesadaran kepatuhan hukum. Di sisi lain, pengguna juga belum sepenuhnya memahami hak-hak mereka sebagai pemilik data, sebagaimana dicatat oleh Kurniastuti dan Prastyanti (2025), sehingga tidak mampu memanfaatkan regulasi tersebut secara maksimal. Dengan demikian, efektivitas regulasi tidak hanya ditentukan oleh isi aturan, tetapi juga oleh tingkat pemahaman dan kepatuhan seluruh pihak yang terlibat.

Secara keseluruhan, pembahasan menunjukkan bahwa keamanan e-commerce merupakan hasil interaksi antara kesiapan teknologi, perilaku pengguna, dan efektivitas regulasi. Penelitian-penelitian yang direview menegaskan bahwa perlindungan data pribadi tidak dapat dicapai dengan satu pendekatan tunggal, melainkan melalui kolaborasi antara penyedia platform, konsumen, dan pemerintah. Tantangan yang ada saat ini terutama terkait dengan rendahnya literasi digital, kelemahan teknis yang masih ditemukan pada platform e-commerce, serta kebutuhan akan penguatan implementasi regulasi. Oleh karena itu, perlindungan data pribadi memerlukan upaya simultan dan berkelanjutan agar konsumen dapat melakukan transaksi digital secara aman.

KESIMPULAN

Hasil *Systematic Literature Review* ini menunjukkan bahwa keamanan e-commerce dan perlindungan data pribadi merupakan aspek krusial dalam ekosistem transaksi digital yang terus berkembang. Berbagai penelitian dalam rentang 2014–2024 memperlihatkan bahwa ancaman terhadap data pribadi, seperti kebocoran data, pencurian identitas, dan serangan rekayasa sosial, semakin meningkat seiring tingginya aktivitas transaksi daring. Ancaman ini tidak hanya berasal dari kelemahan teknis sistem, tetapi juga dari rendahnya literasi digital pengguna yang membuat mereka rentan terhadap penipuan dan penyalahgunaan data.

Temuan dari literatur juga menegaskan bahwa strategi perlindungan data pribadi yang efektif memerlukan kombinasi teknologi keamanan seperti *multi-factor authentication*, enkripsi data, dan sistem deteksi ancaman, yang didukung oleh manajemen risiko internal serta kebijakan keamanan yang jelas. Namun, teknologi saja tidak cukup tanpa kesadaran dan perilaku pengguna yang baik, sehingga edukasi digital menjadi elemen penting dalam memperkuat perlindungan data pribadi.

Selain itu, regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan hukum yang kuat bagi upaya perlindungan

data pengguna. Meskipun demikian, efektivitas regulasi sangat bergantung pada tingkat kepatuhan pelaku usaha dan pemahaman pengguna terhadap hak dan kewajiban dalam pengelolaan data pribadi. Oleh karena itu, secara keseluruhan dapat disimpulkan bahwa keamanan e-commerce harus dibangun melalui pendekatan komprehensif yang melibatkan teknologi, regulasi, manajemen risiko, dan edukasi pengguna untuk menciptakan lingkungan transaksi digital yang aman dan terpercaya.

REFERENSI

Cahyaaty, Tata Arya, Indra Wijaya, and Muhamad Dafin Al Dzky. 2024. "Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi." 5(2): 133–44.

Kurniastuti, Devi Fahwi, and Rina Arum Prastyanti. 2025. "Perlindungan Data Identitas Konsumen Dalam Transaksi E-Commerce Berdasarkan Undang-Undang No.27 Tahun 2022 Perlindungan Data Pribadi." 07(2): 121–33.

Kurniawan, Itok Dwi. 2024. "The Importance of Protecting E-Commerce Consumer Personal Data." 2(2): 51–55.

Melyana, Ismi, M Satria Darmawan, and M Ikram Abib Syah. 2024. "Algoritma Autentikasi Multi Factor Sebagai Solusi Untuk Meningkatkan Keamanan Sistem Pembayaran E-Commerce." 4(2): 984–89.

Mori, Zlatan, Vedran Dakic, and Daniela Djekic Regvart. 2024. "Protection of Personal Data in the Context of E-Commerce." (September 2023): 731–61.

Nafi'ah, Rahmawati. 2020. "Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce." 3(1): 7–13.

Priliasari, Erna. 2023. "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia." 12(27): 261–79.

Saputra, Raihan, Bungaran Saing, Achmad Fauzi, and Jihan Luthfi Nabillah. 2024. "Pengaruh Citra Merek Dan Keamanan Data Terhadap Minat Beli Pada E-Commerce Shopee (Studi Literature Review)." 1(2): 66–76.

Sinaga, Sereni M, Diandra Annisa Abdika Pane, and Farah Diba Awira. 2025. "Legal Analysis of Consumer Protection in E-Commerce Transactions in Indonesia Post Personal Data Protection Law." 1(1): 1–12.

Sumarni, Titin, Eni Kurnia, Tiara Rahmadani, and Rio Febrian Saven. 2024. "Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Pembayaran E-Commerce." 1: 15–27.