STRATEGI PENCEGAHAN KEBOCORAN DATA PADA PLATFORM E-COMMERCE DI INDONESIA

Ibnu Mas'ud, Saemah, Nita Yunita, Neng Tia Fitria, Aditya Farhan Fadlurrohman, Muhammad Ridwan
Program Studi Informatika, Fakultas Sains, Universitas Islam Negeri Sultan Maulana Hasanuddin Banten
ibnumasud@uinbanten.ac.id

ABSTRAK

Perkembangan pesat perdagangan elektronik (e-commerce) mendorong peningkatan pengelolaan data pengguna yang bersifat sensitif, seperti data pribadi dan transaksi, sehingga meningkatkan risiko terjadinya kebocoran data. Permasalahan yang dihadapi adalah belum optimalnya penerapan strategi keamanan data pada platform e-commerce yang menyebabkan kerentanan terhadap serangan siber dan penyalahgunaan informasi. Artikel ini bertujuan untuk mengidentifikasi dan menganalisis strategi pencegahan kebocoran data pada platform e-commerce di Indonesia. Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan menelaah artikel ilmiah, regulasi, dan laporan terkait keamanan data yang dipublikasikan pada periode tertentu. Hasil kajian menunjukkan bahwa strategi pencegahan yang efektif meliputi penerapan enkripsi end-to-end, kontrol akses berbasis prinsip *least privilege*, kepatuhan terhadap regulasi perlindungan data, serta penguatan tata kelola dan manajemen risiko organisasi. Strategi terpadu tersebut mampu meminimalkan risiko kebocoran data dan meningkatkan kepercayaan pengguna terhadap platform e-commerce.

Kata kunci : *kebocoran data, keamanan data, e-commerce, privasi data, SLR*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong terjadinya transformasi digital yang signifikan dalam sektor perdagangan, khususnya melalui pemanfaatan platform e-commerce. Di Indonesia, e-commerce telah menjadi salah satu pilar utama dalam pertumbuhan ekonomi digital, ditandai dengan meningkatnya jumlah pengguna, volume transaksi, serta ragam layanan berbasis digital. Platform e-commerce tidak lagi berperan sebatas sebagai perantara jual beli, melainkan juga sebagai pengelola dan pemroses data pengguna dalam jumlah besar dan berkelanjutan.

Data yang dikelola oleh platform e-commerce mencakup berbagai kategori data pribadi, seperti data identitas pengguna, informasi kontak, preferensi belanja, riwayat transaksi, hingga data keuangan. Karakteristik data tersebut bersifat sensitif dan bernilai strategis, baik bagi pelaku usaha maupun bagi pihak yang memiliki kepentingan tidak sah. Oleh karena itu, keamanan dan perlindungan data menjadi aspek krusial dalam menjamin kepercayaan pengguna serta keberlangsungan operasional platform e-commerce.

Namun demikian, kompleksitas arsitektur sistem e-commerce yang melibatkan berbagai komponen teknologi, seperti aplikasi web dan mobile, basis data terdistribusi, Application Programming Interface (API), serta integrasi dengan layanan pihak ketiga, meningkatkan risiko terjadinya kebocoran data. Ketergantungan pada layanan eksternal, seperti sistem pembayaran digital, penyedia logistik, dan komputasi awan, juga memperluas permukaan serangan (attack surface) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

Berbagai insiden kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa ancaman terhadap keamanan data tidak hanya berasal dari serangan siber yang bersifat teknis, tetapi juga dari kelemahan tata kelola keamanan informasi, kurangnya kesadaran sumber daya manusia, serta tidak optimalnya penerapan standar dan prosedur keamanan. Dampak dari kebocoran data tersebut bersifat multidimensional, mulai dari kerugian finansial, pelanggaran privasi pengguna, hingga menurunnya reputasi dan tingkat kepercayaan publik terhadap platform e-commerce.

Sebagai respons terhadap meningkatnya risiko kebocoran data, Pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Regulasi ini memberikan landasan hukum yang lebih kuat terkait hak subjek data, kewajiban pengendali dan pemroses data, serta sanksi atas pelanggaran perlindungan data pribadi. Meskipun demikian, keberadaan regulasi saja belum cukup untuk menjamin efektivitas perlindungan data apabila tidak diimplementasikan secara konsisten melalui strategi teknis, kebijakan internal, dan tata kelola organisasi yang memadai.

Berdasarkan kondisi tersebut, diperlukan kajian ilmiah yang menelaah secara komprehensif berbagai strategi pencegahan kebocoran data yang relevan dengan karakteristik dan kebutuhan platform e-commerce di Indonesia. Kajian ini diharapkan dapat memberikan pemahaman yang lebih sistematis mengenai pendekatan keamanan data yang tidak hanya berorientasi pada teknologi, tetapi juga mencakup aspek regulasi, manajemen risiko, dan tata kelola organisasi.

Berdasarkan uraian latar belakang tersebut, dapat diidentifikasi bahwa permasalahan utama dalam konteks keamanan data e-commerce di Indonesia adalah belum optimalnya penerapan strategi pencegahan kebocoran data secara menyeluruh dan terintegrasi. Banyak platform e-commerce masih

menerapkan mekanisme keamanan yang bersifat parsial, seperti fokus pada pengamanan jaringan atau aplikasi, tanpa diimbangi dengan kebijakan organisasi dan manajemen risiko yang matang.

Selain itu, penerapan regulasi perlindungan data pribadi sering kali masih bersifat administratif dan belum sepenuhnya diinternalisasi ke dalam proses bisnis dan sistem teknis. Kurangnya pemahaman dan kesadaran sumber daya manusia terhadap pentingnya keamanan data juga menjadi faktor yang memperbesar potensi terjadinya kebocoran data akibat kesalahan manusia (human error).

Permasalahan lainnya adalah belum adanya standar acuan yang komprehensif dan aplikatif yang dapat dijadikan pedoman oleh platform e-commerce dalam merancang dan mengimplementasikan strategi pencegahan kebocoran data yang sesuai dengan kondisi di Indonesia. Akibatnya, meskipun berbagai upaya pengamanan telah dilakukan, risiko kebocoran data dan pelanggaran privasi pengguna masih tetap tinggi.

Penelitian ini bertujuan untuk mengidentifikasi, mengkaji, dan menganalisis berbagai strategi pencegahan kebocoran data yang diterapkan pada platform e-commerce berdasarkan hasil kajian literatur ilmiah dan regulasi yang relevan. Tujuan ini diarahkan untuk memperoleh pemahaman yang komprehensif mengenai pendekatan keamanan data yang efektif dalam konteks e-commerce.

Selain itu, penelitian ini bertujuan untuk menganalisis keterkaitan antara aspek teknis keamanan informasi, kepatuhan terhadap regulasi perlindungan data pribadi, serta tata kelola dan manajemen risiko organisasi. Melalui analisis tersebut, penelitian ini diharapkan mampu merumuskan pendekatan strategis yang terintegrasi dan dapat dijadikan acuan bagi pengelola platform e-commerce dalam meningkatkan keamanan data dan perlindungan privasi pengguna.

Secara khusus, hasil penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan kajian keamanan informasi, serta kontribusi praktis bagi pelaku industri e-commerce dalam merancang kebijakan dan strategi pencegahan kebocoran data yang lebih efektif dan berkelanjutan.

Upaya penyelesaian permasalahan dalam penelitian ini dilakukan melalui pendekatan Systematic Literature Review (SLR). Metode ini dipilih karena mampu memberikan gambaran yang sistematis, terstruktur, dan objektif terhadap perkembangan penelitian terkait strategi pencegahan kebocoran data pada platform e-commerce.

Tahapan penelitian diawali dengan perumusan fokus dan pertanyaan penelitian yang relevan dengan topik keamanan data e-commerce. Selanjutnya, dilakukan pencarian literatur ilmiah dari berbagai basis data akademik yang kredibel, dengan kriteria inklusi dan eksklusi yang jelas untuk memastikan kualitas dan relevansi sumber yang digunakan.

Tahap berikutnya adalah proses seleksi dan evaluasi literatur untuk mengidentifikasi penelitian-penelitian yang membahas strategi teknis, kebijakan organisasi, serta aspek regulasi dalam pencegahan kebocoran data. Literatur terpilih kemudian dianalisis secara mendalam untuk mengidentifikasi pola, temuan utama, serta kesenjangan penelitian yang ada.

Hasil analisis tersebut selanjutnya disintesis untuk merumuskan kerangka strategi pencegahan kebocoran data yang komprehensif dan aplikatif bagi platform e-commerce. Dengan pendekatan ini, penelitian diharapkan mampu memberikan rekomendasi strategis yang tidak hanya relevan secara teoritis, tetapi juga dapat diimplementasikan secara praktis dalam konteks e-commerce di Indonesia.

2. TINJAUAN PUSTAKA

2.1. Keamanan Data pada Platform *E-Commerce*

Platform e-commerce berperan sebagai pengelola data digital dalam skala besar yang mencakup data identitas pengguna, informasi transaksi, serta data finansial. Keamanan data pada platform e-commerce bertujuan untuk menjamin kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi, yang dikenal sebagai konsep CIA Triad dalam keamanan informasi.

Meningkatnya ketergantungan masyarakat terhadap layanan e-commerce menyebabkan data pengguna menjadi aset strategis yang bernilai tinggi, baik bagi pelaku bisnis maupun bagi pelaku kejahatan siber. Menurut beberapa penelitian, lemahnya mekanisme keamanan data dapat menyebabkan kebocoran informasi yang berdampak pada kerugian finansial, pelanggaran privasi, serta menurunnya kepercayaan pengguna terhadap platform digital [1], [6].

Keamanan data pada e-commerce tidak hanya berkaitan dengan pengamanan teknis sistem, tetapi juga melibatkan kebijakan organisasi, kesadaran pengguna, serta kepatuhan terhadap regulasi perlindungan data. Oleh karena itu, keamanan data harus dipandang sebagai proses berkelanjutan yang terintegrasi dalam seluruh siklus pengelolaan sistem e-commerce.

2.2. Kebocoran Data (*Data Leakage*)

Kebocoran data (data leakage) didefinisikan sebagai kondisi ketika data sensitif diakses, dipindahkan, atau disebarluaskan oleh pihak yang tidak memiliki otorisasi. Kebocoran data dapat terjadi baik secara disengaja maupun tidak disengaja, dan sering kali sulit dideteksi dalam waktu singkat [2].

Beberapa penelitian mengklasifikasikan penyebab kebocoran data ke dalam tiga faktor utama, yaitu faktor teknis, faktor manusia, dan faktor organisasi. Faktor teknis mencakup kelemahan sistem keamanan, celah perangkat lunak, serta konfigurasi sistem yang tidak optimal. Faktor manusia berkaitan dengan kesalahan pengguna, seperti penggunaan kata sandi yang lemah, kelalaian dalam mengelola akses,

atau rendahnya kesadaran keamanan informasi. Sementara itu, faktor organisasi meliputi lemahnya kebijakan keamanan, kurangnya audit sistem, serta minimnya manajemen risiko keamanan informasi [3], [4].

Dalam konteks e-commerce, kebocoran data dapat berdampak luas karena melibatkan data pribadi dan finansial pengguna. Dampak tersebut tidak hanya merugikan pengguna secara individual, tetapi juga dapat menurunkan reputasi perusahaan, memicu sanksi hukum, serta menghambat keberlanjutan bisnis digital.

2.3. Penelitian Terdahulu

Penelitian terdahulu terkait keamanan data dan kebocoran data pada platform e-commerce telah dilakukan dari berbagai perspektif, termasuk aspek teknis, regulasi, dan perilaku pengguna. Beberapa penelitian menekankan pentingnya perlindungan hukum dan peran regulasi dalam menjamin keamanan data pribadi konsumen, khususnya dalam menghadapi meningkatnya kasus kebocoran data pada platform e-commerce di Indonesia.

Studi lain berfokus pada evaluasi sistem keamanan teknis yang diterapkan oleh platform e-commerce besar, seperti penggunaan enkripsi data dan autentikasi dua faktor. Meskipun mekanisme tersebut terbukti mampu meningkatkan keamanan sistem, sejumlah penelitian menunjukkan bahwa ancaman siber terus berkembang dan memerlukan pendekatan keamanan yang lebih adaptif dan berlapis.

Selain itu, beberapa penelitian menyoroti peran faktor manusia dan literasi digital pengguna dalam pencegahan kebocoran data. Rendahnya pemahaman pengguna terhadap keamanan dan privasi data dinilai berkontribusi terhadap tingginya risiko kebocoran data, meskipun sistem keamanan teknis telah diterapkan dengan baik.

Berdasarkan hasil penelitian terdahulu tersebut, dapat disimpulkan bahwa pencegahan kebocoran data pada platform e-commerce tidak dapat dilakukan melalui satu pendekatan tunggal. Diperlukan strategi terpadu yang menggabungkan aspek teknis, regulasi, serta tata kelola organisasi untuk menghasilkan sistem keamanan data yang efektif dan berkelanjutan.

Tabel 1. Ringkasan Penelitian Terdahulu

No	Nama Peneliti (Tahun)	Judul & Publikasi	Hasil Utama
1	Graciella D. Phie & Gunardi Lie (2025)	Perlindungan Data Pribadi Konsumen atas Kebocoran Data Pada E-Commerce (Indonesian Journal of Law)	Menekan pentingnya peran hukum dan strategi perlindungan dari pihak e-commerce, pemerintah, dan masyarakat.
2	Yayi N. Silalahi & M. I. P. Nasution (2025)	Tinjauan Sistem Keamanan Data Pelanggan di E-Commerce: Studi Kasus Platform Shopee (J-SIMTEK)	Shopee telah menerapkan enkripsi dan autentikasi dua faktor namun masih menghadapi tantangan siber.
3	Nia Ramadhani & M. I. P. Nasution (2024)	Tantangan Dan Solusi Keamanan Siber Dalam Transaksi E-Commerce (JPSI)	Identifikasi tantangan serangan seperti phishing dan malware; solusi teknis umum.
4	Sinta S. Ayu & M. I. P. Nasution (2023)	Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia (JUEB)	Menemukan kebocoran data pelanggan Tokopedia dan kebutuhan perbaikan regulasi.
5	Tata Arya Cahyaaty et al. (2024)	Analisis Keamanan Data Pribadi Pada PenggunaE-Commerce Shopee Terhadap AncamanData Pribadi (JIFORTY)	Enkripsi & 2FA penting namun tingkat pemahaman pengguna rendah; rekomendasi peningkatan kesadaran.
6	Afzil Ramadian et al. (2024)	Mengukur dan Mengelola Risiko Cybercrime dalam E-Commerce: Peran Strategis Cybersecurity untuk Keamanan Informasi dan Perlindungan Data (Jurnal Ilmiah Edunomika)	Menunjukkan peran penting manajemen risiko dan keamanan siber untuk proteksi aset data.
7	Annisa R. Hartanto et al. (2025)	Perlindungan Privasi dalam Membangun Kepercayaan Penggunaterhadap Platform E-Commerce (PESHUM)	Walaupun ada upaya perlindungan privasi, masih rendah literasi digital dan enforcement hukum.
8	Otieno E. A. (2025)	Data protection and privacy in e-commerce environment: Systematic review (GSC Online Press)	Tuntutan regulasi kuat, teknologi privasi, dan standar internasional memperkuat keamanan data.
9	Hardeep singh et al. (2025)	Examining the Impact of personal Data Breaches on Consumer Trust and Privacy Protection Behavior in E-Commerce (ACR Journal)	Breaches signifikan memengaruhi trust & perilaku proteksi privasi konsumen.
10	As-syiva dan Nasution (2024)	Analisis Keamanan Data Pribadi Pengguna E-Commerce Perspektif Keamanan Dan Privasi (Kohesi)	Keamanan dan privasi data pengguna e-commerce sangat memengaruhi kepercayaan konsumen dan keberlanjutan bisnis digital.

Penelitian terdahulu yang dianalisis menunjukkan bahwa isu kebocoran data pada platform e-commerce telah dikaji dari berbagai sudut pandang, mulai dari aspek teknis, regulasi, hingga faktor pengguna. Beberapa penelitian menekankan pentingnya enkripsi dan autentikasi berlapis, sementara yang lain membahas kebutuhan kepatuhan terhadap regulasi perlindungan data serta peran manajemen risiko organisasi. Kajian tersebut memberikan dasar teoretis yang kuat untuk memahami ruang lingkup keamanan data pada e-commerce, dan menjadi referensi penting dalam penyusunan analisis pada penelitian ini

2.4. Strategi Teknis Pencegahan Kebocoran Data

Strategi teknis merupakan lapisan utama dalam pencegahan kebocoran data pada platform e-commerce. Beberapa strategi teknis yang umum diterapkan meliputi enkripsi data, kontrol akses berbasis peran (role-based access control), serta autentikasi multifaktor. Enkripsi data berfungsi untuk melindungi informasi sensitif agar tidak dapat dibaca oleh pihak yang tidak berwenang, baik pada saat data disimpan maupun ditransmisikan [6], [8].

Selain itu, penerapan prinsip least privilege bertujuan untuk membatasi hak akses pengguna hanya pada data yang benar-benar dibutuhkan sesuai perannya. Pengujian keamanan sistem secara berkala melalui penetration testing dan vulnerability assessment juga menjadi bagian penting dalam mengidentifikasi serta menutup celah keamanan sebelum dimanfaatkan oleh penyerang.

2.5. Regulasi dan Kepatuhan Perlindungan Data

Regulasi perlindungan data pribadi menjadi landasan hukum dalam pengelolaan dan perlindungan data pengguna e-commerce. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum yang mengatur hak subjek data serta kewajiban pengendali dan pemroses data.

Kepatuhan terhadap regulasi ini mendorong platform e-commerce untuk menerapkan kebijakan keamanan data yang lebih sistematis dan terdokumentasi. Selain regulasi nasional, adopsi standar internasional seperti ISO/IEC 27001 dan ISO/IEC 27701 juga berperan dalam meningkatkan kematangan sistem manajemen keamanan informasi dan privasi data [7], [13].

2.6. Tata Kelola dan Manajemen Risiko Organisasi

Tata kelola dan manajemen risiko organisasi merupakan faktor penentu keberhasilan penerapan strategi keamanan data. Beberapa penelitian menunjukkan bahwa kebocoran data sering kali disebabkan oleh kelemahan internal organisasi, seperti kurangnya pelatihan keamanan siber, minimnya pengawasan, dan lemahnya budaya keamanan informasi.

Pendekatan manajemen risiko yang terstruktur memungkinkan organisasi mengidentifikasi, menilai, dan memitigasi potensi ancaman terhadap data secara sistematis. Program pelatihan keamanan informasi, audit keamanan berkala, serta monitoring sistem secara berkelanjutan merupakan langkah penting dalam membangun sistem pertahanan berlapis (defense in depth) yang efektif [14], [17].

3. METODE PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) sebagai pendekatan utama untuk mengkaji strategi pencegahan kebocoran data pada platform e-commerce. SLR merupakan metode penelitian sekunder yang dirancang untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian terdahulu secara sistematis, transparan, dan terstruktur. Penggunaan metode ini memungkinkan peneliti memperoleh gambaran menyeluruh mengenai perkembangan penelitian, kecenderungan pendekatan, serta solusi yang telah diusulkan terkait permasalahan kebocoran data.

Pemilihan SLR didasarkan pada karakteristik permasalahan penelitian yang bersifat kompleks dan multidisipliner, mencakup aspek teknologi, regulasi, serta tata kelola organisasi. Kebocoran data tidak hanya disebabkan oleh kelemahan teknis, tetapi juga oleh faktor manusia, kebijakan internal, dan lemahnya kepatuhan terhadap regulasi. Oleh karena itu, diperlukan metode penelitian yang mampu mengintegrasikan berbagai sudut pandang keilmuan agar hasil kajian tidak bersifat parsial.

Selain itu, metode SLR memberikan kerangka kerja yang sistematis sehingga setiap tahapan penelitian dapat ditelusuri dan dipertanggungjawabkan secara ilmiah. Dengan demikian, penelitian ini tidak hanya menyajikan ringkasan literatur, tetapi juga menghasilkan sintesis konseptual yang dapat menjadi dasar rekomendasi strategis bagi pengembangan keamanan data pada platform e-commerce.

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini merupakan penelitian kualitatif dengan pendekatan Systematic Literature Review (SLR). Pendekatan kualitatif dipilih karena penelitian berfokus pada pemaknaan, interpretasi, dan pengkajian mendalam terhadap konsep, model, dan strategi pencegahan kebocoran data yang dikemukakan dalam berbagai publikasi ilmiah. Penelitian ini tidak bertujuan menguji hubungan kuantitatif antar variabel, melainkan membangun pemahaman komprehensif terhadap fenomena kebocoran data pada platform e-commerce.

Melalui pendekatan SLR, peneliti dapat menelaah secara kritis berbagai penelitian terdahulu untuk mengidentifikasi pendekatan yang dominan digunakan, efektivitas strategi yang telah diterapkan, serta tantangan yang masih dihadapi dalam implementasi keamanan data. Proses ini

memungkinkan peneliti membandingkan hasil penelitian dari berbagai konteks dan sudut pandang keilmuan, sehingga diperoleh gambaran yang lebih objektif dan holistik.

Pendekatan ini juga relevan karena bidang keamanan data terus berkembang seiring meningkatnya kompleksitas teknologi dan ancaman siber. Oleh karena itu, pengkajian literatur secara sistematis menjadi penting untuk memetakan evolusi strategi keamanan data serta menemukan celah penelitian yang dapat dijadikan dasar pengembangan studi lanjutan.

3.2. Tahapan Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan sistematis yang disusun untuk menjamin konsistensi, transparansi, dan keterulangan proses penelitian. Tahapan tersebut meliputi perencanaan penelitian, pencarian literatur, seleksi literatur, analisis literatur, dan sintesis hasil.

a. Perencanaan Penelitian
   Tahap perencanaan diawali dengan identifikasi permasalahan penelitian, yaitu meningkatnya kasus kebocoran data pada platform e-commerce yang berdampak pada kerugian finansial, menurunnya kepercayaan pengguna, serta potensi pelanggaran hukum terkait perlindungan data pribadi. Permasalahan ini kemudian dirumuskan menjadi tujuan penelitian dan pertanyaan penelitian yang berfokus pada strategi pencegahan kebocoran data.
   Pada tahap ini, peneliti juga menetapkan ruang lingkup penelitian, termasuk batasan topik, periode publikasi literatur, serta fokus pembahasan yang mencakup aspek teknis, regulasi, dan tata kelola organisasi. Perencanaan dilakukan secara matang untuk meminimalkan bias subjektif peneliti dan memastikan bahwa seluruh tahapan penelitian berjalan sesuai kerangka metodologis SLR.
b. Pencarian Literatur
   Tahap pencarian literatur dilakukan secara sistematis dan terstruktur untuk memperoleh sumber ilmiah yang relevan, kredibel, dan mutakhir. Penelusuran dilakukan melalui beberapa basis data ilmiah bereputasi, yaitu Google Scholar, IEEE Xplore, ScienceDirect, dan SpringerLink, yang dikenal luas sebagai penyedia publikasi ilmiah berkualitas di bidang teknologi informasi dan keamanan siber.
   Pencarian dilakukan menggunakan kombinasi kata kunci seperti data leakage, data breach, e-commerce security, data privacy, dan data protection. Kata kunci dikombinasikan dengan operator Boolean untuk memperluas sekaligus memfokuskan hasil pencarian. Proses ini dilakukan secara iteratif, disertai penyaringan awal berdasarkan judul dan abstrak, guna mengidentifikasi literatur yang memiliki keterkaitan langsung dengan fokus penelitian.
   Selain itu, peneliti juga melakukan penelusuran daftar pustaka dari artikel terpilih (snowballing) untuk menemukan literatur relevan lainnya yang berpotensi terlewat. Pendekatan ini bertujuan untuk meningkatkan kelengkapan dan kedalaman literatur yang dianalisis.
c. Seleksi Literatur
   Literatur yang diperoleh kemudian diseleksi secara bertahap menggunakan kriteria inklusi dan eksklusi. Seleksi awal dilakukan dengan meninjau judul dan abstrak untuk mengeliminasi artikel yang tidak relevan. Selanjutnya, seleksi lanjutan dilakukan melalui pembacaan teks lengkap untuk menilai kesesuaian isi artikel dengan tujuan penelitian.
   Tahap seleksi bertujuan untuk memastikan bahwa hanya literatur yang memiliki kualitas metodologis yang baik dan kontribusi substansial terhadap topik penelitian yang digunakan. Proses ini juga membantu mengurangi risiko bias informasi dan duplikasi data dalam tahap analisis.
d. Analisis Literatur
   Artikel terpilih dianalisis secara mendalam menggunakan pendekatan analisis isi (content analysis). Analisis difokuskan pada identifikasi konteks penelitian, pendekatan metodologis, jenis ancaman kebocoran data, serta strategi pencegahan yang diusulkan atau diterapkan.
   Selain mengkaji masing-masing artikel secara individual, peneliti juga melakukan analisis komparatif antar penelitian untuk menemukan pola, kecenderungan, serta perbedaan pendekatan. Tahap ini menghasilkan pemetaan konseptual yang menjadi dasar pengelompokan dan sintesis hasil penelitian.
e. Sintesis Hasil
   Tahap sintesis dilakukan dengan mengintegrasikan hasil analisis literatur ke dalam kerangka konseptual yang komprehensif. Temuan dari berbagai artikel dikelompokkan berdasarkan kesamaan tema, pendekatan, dan fokus strategi pencegahan kebocoran data.
   Sintesis bertujuan untuk membangun pemahaman yang utuh mengenai strategi pencegahan kebocoran data pada platform e-commerce, sekaligus mengidentifikasi celah penelitian dan peluang pengembangan kajian di masa mendatang.

3.3. Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi ditetapkan untuk menjamin kualitas, relevansi, dan kebaruan literatur yang digunakan. Kriteria inklusi mencakup artikel jurnal dan prosiding ilmiah nasional maupun internasional yang membahas keamanan data, kebocoran data, atau perlindungan data pada platform digital, dipublikasikan dalam lima tahun terakhir, dan tersedia dalam bentuk teks lengkap.

Kriteria eksklusi mencakup artikel non-ilmiah, publikasi yang tidak relevan dengan topik penelitian, serta artikel yang tidak dapat diakses secara lengkap.

Penerapan kriteria ini bertujuan untuk membangun landasan teoritis yang kuat dan dapat dipertanggungjawabkan.

3.4. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui studi dokumentasi dengan menghimpun data sekunder berupa artikel ilmiah, prosiding, laporan institusional, dan dokumen regulasi yang relevan. Data yang dikumpulkan dianalisis untuk memperoleh informasi mengenai pola kebocoran data, faktor penyebab, serta strategi pencegahan yang telah dikembangkan.

Studi dokumentasi dipilih karena sesuai dengan karakteristik SLR yang berfokus pada eksplorasi dan analisis sumber tertulis sebagai basis utama pengambilan kesimpulan ilmiah.

3.5. Teknik Analisis Data

Analisis data dilakukan dengan pendekatan analisis isi untuk mengekstraksi informasi penting dari setiap literatur terpilih. Proses analisis mencakup pengkodean tema, pengelompokan konsep, serta interpretasi temuan penelitian.

Hasil analisis kemudian diklasifikasikan ke dalam tiga kategori utama, yaitu strategi teknis, strategi regulasi dan kepatuhan, serta strategi tata kelola dan manajemen risiko organisasi. Klasifikasi ini bertujuan untuk menghasilkan pemetaan strategi yang sistematis dan mudah dianalisis.

3.6. Alur Penelitian

Alur penelitian dimulai dari identifikasi permasalahan dan perumusan tujuan penelitian, kemudian dilanjutkan dengan pencarian dan seleksi literatur secara sistematis. Artikel terpilih dianalisis dan disintesis untuk menghasilkan pemahaman komprehensif mengenai strategi pencegahan kebocoran data.

Tahap akhir penelitian adalah penarikan kesimpulan dan perumusan rekomendasi berbasis hasil sintesis literatur, yang diharapkan dapat memberikan kontribusi teoretis dan praktis bagi pengembangan keamanan data pada platform e-commerce.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

Hasil penelitian menunjukkan bahwa strategi pencegahan kebocoran data pada platform e-commerce dapat dikelompokkan ke dalam tiga kategori utama, yaitu strategi teknis, strategi regulasi dan kepatuhan, serta strategi tata kelola dan manajemen risiko organisasi. Pengelompokan ini didasarkan pada kesamaan fokus intervensi yang berulang dalam literatur, yaitu apakah strategi berorientasi pada penguatan kontrol sistem dan perlindungan data (teknis), penguatan kerangka akuntabilitas dan standar minimum perlindungan (regulasi/kepatuhan), atau penguatan proses organisasi dan faktor manusia (tata kelola/risiko) [10].

Secara umum, literatur yang dianalisis mengindikasikan bahwa kebocoran data pada e-commerce merupakan fenomena yang bersifat multidimensional. Kebocoran data jarang disebabkan oleh satu titik kegagalan, melainkan cenderung terjadi karena kombinasi kerentanan teknis, proses organisasi yang belum matang, serta perilaku pengguna atau karyawan yang rentan terhadap rekayasa sosial [8], [10]. Karakteristik e-commerce yang melibatkan data sensitif dan transaksi berulang, serta integrasi dengan pihak ketiga seperti payment gateway, layanan logistik, penyedia cloud, dan layanan analitik, memperluas permukaan serangan (*attack surface*) dan meningkatkan kompleksitas kontrol keamanan yang perlu diterapkan [1], [8].

Pada aspek teknis, literatur menekankan bahwa proteksi data harus dilakukan pada dua kondisi utama, yaitu saat data disimpan (*data at rest*) dan saat data ditransmisikan (*data in transit*). Enkripsi dipandang sebagai kontrol dasar untuk mengurangi risiko data dapat dibaca ketika terjadi akses tidak sah atau intersepsi komunikasi [4]. Namun, efektivitas enkripsi dipengaruhi oleh praktik pendukung seperti manajemen kunci dan penerapan kebijakan akses yang ketat, sehingga strategi teknis sering muncul bersama kontrol akses berbasis peran (RBAC) dan prinsip *least privilege* [7]. Penggunaan autentikasi multifaktor (MFA) juga direkomendasikan untuk memperkuat proteksi akun, terutama akun dengan hak akses tinggi [8]. Selain itu, pengujian keamanan berkala seperti *vulnerability assessment* dan *penetration testing* diposisikan sebagai proses pencegahan proaktif agar kelemahan dapat ditemukan dan diperbaiki sebelum dimanfaatkan [11]. Sejumlah literatur juga menekankan pentingnya monitoring, pencatatan log, dan deteksi ancaman untuk mempercepat respons insiden dan mengurangi dampak kebocoran [3], [8].

Pada aspek regulasi dan kepatuhan, hasil kajian menunjukkan bahwa kepatuhan terhadap regulasi perlindungan data pribadi, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), berperan dalam mendorong organisasi menyusun kebijakan keamanan dan privasi yang lebih sistematis [12]. Regulasi mendorong adanya akuntabilitas dalam pengelolaan data, termasuk pengaturan pemrosesan data, transparansi, retensi, serta mekanisme penanganan insiden [12]. Selain regulasi nasional, adopsi standar internasional seperti ISO/IEC 27001 dan ISO/IEC 27701 dipandang mampu meningkatkan kematangan keamanan informasi dan manajemen privasi melalui kerangka sistem manajemen yang menekankan penilaian risiko, penerapan kontrol, audit berkala, dan perbaikan berkelanjutan [2].

Pada aspek tata kelola dan manajemen risiko organisasi, literatur menegaskan bahwa faktor manusia dan proses organisasi sering menjadi sumber risiko yang signifikan. Kesalahan konfigurasi, kelalaian prosedur, penggunaan kredensial yang tidak aman, serta keberhasilan serangan rekayasa sosial seperti *phishing* menjadi faktor yang sering disebut

[5], [9]. Karena itu, pelatihan keamanan informasi dan peningkatan kesadaran keamanan siber menjadi strategi penting yang tidak dapat dipisahkan dari kontrol teknis [5], [9]. Audit berkala, evaluasi hak akses, monitoring berkelanjutan, pemisahan tugas, serta manajemen risiko pihak ketiga juga disoroti sebagai langkah tata kelola untuk menjaga konsistensi penerapan keamanan pada operasi sehari-hari [1], [7], [10]. Ringkasan literatur terpilih yang dianalisis dan pemetaan strategi yang ditekankan pada masing-masing sumber disajikan pada Tabel 2.

Tabel 2. Sintesis Literatur Terpilih terkait Strategi Pencegahan Kebocoran Data pada Platform E-Commerce

NO	Sumber (Penulis, Tahun)	Fokus Kajian	Strategi yang Ditekankan	Kategori Strategi
1	Zhang & Chen (2022)	Kerentanan integrasi pihak ketiga	Pengamanan integrasi, pengendalian API, evaluasi keamanan vendor	Teknis / Risiko Pihak Ketiga
2	Pratama & Nugroho (2023)	Kepatuhan perlindungan data	Kebijakan internal dan prosedur insiden yang lebih sistematis	Regulasi & Kepatuhan
3	Sarker (2010)	Analitik untuk keamanan siber	Deteksi ancaman berbasis data, monitoring, penguatan respons	Teknis (Deteksi/Monitoring)
4	Alasmary et al. (2020)	E-commerce berbasis cloud	Enkripsi, kontrol akses, penguatan konfigurasi cloud	Teknis
5	Parsons et al. (2020)	Faktor manusia	Awareness training, kepatuhan kebijakan, budaya keamanan	Tata Kelola/SDM
6	Martin (2020)	Privasi & minimasi data	Data minimization, retensi data, pembatasan pengumpulan data	Teknis (Privasi)
7	Smith & Brooks (2021)	Insider threats	Pembatasan hak akses, audit akses, monitoring aktivitas internal	Tata Kelola/Risiko
8	ENISA (2021)	Threat landscape	Pemetaan ancaman, kesiapan respons insiden, kontrol berlapis	Manajemen Risiko
9	Siponen et al. (2020)	Kepatuhan karyawan	Faktor perilaku/organisasi, penegakan kebijakan, compliance	Tata Kelola/SDM
10	von Solms & van Niekerk (2020)	Governance keamanan siber	Kerangka tata kelola, penugasan peran, kontrol proses	Tata Kelola
11	Shostack (2020)	Threat modeling	Identifikasi ancaman sejak desain, pencegahan proaktif	Teknis (Desain)
12	UU PDP (2022)	Regulasi PDP Indonesia	Kewajiban pengelolaan data dan perlindungan hak subjek data	Regulasi & Kepatuhan

Tabel 2 menunjukkan bahwa strategi teknis berperan sebagai fondasi pengamanan sistem dan perlindungan data, strategi regulasi dan kepatuhan berfungsi sebagai kerangka penguat akuntabilitas organisasi, sedangkan strategi tata kelola dan manajemen risiko memastikan strategi teknis dan kepatuhan dapat dijalankan secara konsisten dan berkelanjutan [10]. Hasil sintesis ini memperlihatkan bahwa ketiga kategori strategi tidak berdiri sendiri, melainkan membentuk rangkaian kontrol yang saling melengkapi dalam upaya pencegahan kebocoran data pada ekosistem e-commerce [8].

4.2. Pembahasan

Pembahasan hasil SLR menunjukkan bahwa pencegahan kebocoran data pada platform e-commerce tidak efektif apabila dilakukan secara parsial. Kontrol teknis, kepatuhan regulasi, dan tata kelola organisasi merupakan tiga komponen yang saling menguatkan. Kontrol teknis menyediakan perlindungan langsung pada level sistem, regulasi menyediakan kerangka akuntabilitas dan standar minimum perlindungan, sedangkan tata kelola memastikan bahwa kontrol teknis dan kebijakan kepatuhan dijalankan secara konsisten serta dapat dipertahankan dalam jangka panjang [10]. Interaksi antarkomponen ini memperkuat relevansi pendekatan berlapis (*defense in depth*), yakni keamanan dibangun melalui beberapa lapisan kontrol sehingga kegagalan pada satu lapisan tidak serta-merta menyebabkan insiden besar [8].

Pada lapisan teknis, dominasi rekomendasi seperti enkripsi, kontrol akses berbasis peran, prinsip *least privilege*, autentikasi multifaktor, dan pengujian keamanan berkala dapat dipahami karena e-commerce memproses data pribadi dalam skala besar dan kontinu [4], [8]. Namun, literatur mengindikasikan bahwa kegagalan pencegahan sering terjadi bukan karena teknologi tidak tersedia, melainkan karena implementasi dan operasi sehari-hari tidak konsisten. Contohnya, enkripsi dapat menjadi kurang efektif apabila manajemen kunci tidak distandardisasi atau tidak diaudit; RBAC dapat kehilangan fungsi apabila hak akses tidak ditinjau ulang secara periodik; MFA menjadi tidak optimal apabila akun berprivilege tinggi masih mengandalkan autentikasi tunggal; serta pengujian keamanan berkala menjadi formalitas apabila temuan kerentanan tidak ditindaklanjuti melalui remediasi yang terukur [7], [11]. Hal ini menegaskan bahwa strategi teknis perlu dipahami sebagai proses berkelanjutan, bukan tindakan satu kali.

Karakteristik ekosistem e-commerce yang terintegrasi dengan pihak ketiga juga memperluas permukaan serangan. Integrasi dengan layanan

pembayaran, logistik, cloud, dan analitik membuka jalur risiko kebocoran yang tidak selalu berasal dari sistem internal [1], [8]. Karena itu, strategi teknis perlu diperluas dengan kontrol terhadap integrasi dan pertukaran data, misalnya melalui pengamanan API, pembatasan data yang dibagikan, autentikasi antarsistem, serta pemantauan trafik dan aktivitas integrasi [1]. Dalam konteks ini, kontrol teknis internal akan lebih efektif apabila didukung tata kelola manajemen risiko pihak ketiga, termasuk evaluasi vendor dan penetapan persyaratan keamanan dalam kerja sama [1], [10].

Dari sisi regulasi dan kepatuhan, keberadaan UU PDP mendorong organisasi menempatkan perlindungan data sebagai kewajiban yang melekat pada proses bisnis [12]. Namun, literatur juga menyoroti tantangan implementasi pada tingkat organisasi, seperti keterbatasan sumber daya keamanan, variasi kematangan proses antar organisasi, serta rendahnya literasi keamanan [2], [8]. Kondisi ini dapat mendorong kepatuhan menjadi sekadar administratif apabila tidak diterjemahkan ke prosedur operasional. Karena itu, adopsi ISO/IEC 27001 dan ISO/IEC 27701 dipandang relevan sebagai kerangka sistem manajemen yang mengarahkan organisasi melakukan penilaian risiko, menetapkan kontrol prioritas, mendokumentasikan kebijakan, menjalankan audit, dan melakukan perbaikan berkelanjutan [2]. Dengan pendekatan tersebut, kepatuhan dapat diposisikan sebagai mekanisme yang mendorong konsistensi implementasi, bukan sekadar pemenuhan dokumen.

Pada dimensi tata kelola dan manajemen risiko organisasi, literatur menekankan bahwa faktor manusia merupakan salah satu pemicu penting kebocoran data. Kesalahan konfigurasi, kelalaian prosedur, penggunaan kredensial yang tidak aman, serta keberhasilan serangan rekayasa sosial menunjukkan bahwa kontrol teknis dapat dilemahkan oleh perilaku yang tidak aman [5], [9]. Karena itu, pelatihan keamanan informasi dan peningkatan kesadaran keamanan siber perlu dilakukan secara periodik dan dilengkapi evaluasi, misalnya simulasi phishing dan penegakan SOP keamanan [5]. Audit berkala, evaluasi hak akses, pemisahan tugas, dan monitoring aktivitas akun berprivilege tinggi diperlukan untuk menekan risiko internal serta memperkuat akuntabilitas pengelolaan data [7], [10]. Selain itu, pemetaan ancaman dan kesiapan respons insiden juga penting agar organisasi mampu mendeteksi, mengendalikan, dan memulihkan layanan ketika terjadi insiden [8].

Pembahasan ini juga menegaskan peran *privacy-by-design* dan *data minimization* sebagai strategi pencegahan struktural. Dalam praktik e-commerce, organisasi sering terdorong mengumpulkan data secara luas untuk personalisasi dan pengembangan layanan. Namun, semakin banyak data yang dikumpulkan dan disimpan, semakin besar pula dampak ketika insiden terjadi. Karena itu, pembatasan pengumpulan data pada data yang benar-benar diperlukan, penerapan kebijakan retensi yang jelas, serta penghapusan data yang sudah tidak relevan dapat mengurangi "nilai kebocoran" dan memperkecil dampak terhadap pengguna [6]. Pendekatan ini juga dapat meningkatkan kepercayaan pengguna karena pengelolaan data terlihat lebih bertanggung jawab dan transparan [12].

Implikasi praktis dari hasil penelitian ini adalah perlunya platform e-commerce menjadikan perlindungan data sebagai bagian inti dari operasional bisnis. Organisasi disarankan menetapkan kontrol teknis minimum yang wajib diterapkan pada seluruh proses pengelolaan data pribadi, seperti enkripsi pada penyimpanan dan transmisi, kontrol akses berbasis peran dengan prinsip *least privilege*, autentikasi multifaktor untuk akun dengan akses sensitif, serta pengujian keamanan berkala yang diikuti remediasi kerentanan secara terukur [4], [7], [11]. Selain itu, organisasi perlu membangun monitoring dan pencatatan log yang memadai agar deteksi anomali dan respons insiden dapat dilakukan lebih cepat [3], [8]. Dari sisi kepatuhan, organisasi perlu menerjemahkan UU PDP ke dalam kebijakan dan prosedur internal yang operasional, seperti pengelolaan persetujuan pemrosesan data, transparansi kebijakan privasi, retensi dan penghapusan data, serta SOP penanganan insiden [12]. Mengingat keterlibatan pihak ketiga dalam ekosistem e-commerce, evaluasi keamanan vendor, pembatasan data yang dibagikan, dan pengamanan integrasi API perlu diposisikan sebagai bagian dari manajemen risiko agar peluang kebocoran dari jalur eksternal dapat diminimalkan [1], [10].

Penelitian ini memiliki beberapa keterbatasan. Hasil sintesis bergantung pada literatur yang tersedia dan dapat diakses, sehingga terdapat kemungkinan beberapa studi relevan tidak terikut dalam kajian karena perbedaan kata kunci, batasan akses, atau kriteria seleksi. Selain itu, penelitian ini menekankan sintesis konseptual, sehingga temuan lebih berfokus pada pengelompokan strategi dan interpretasi literatur, bukan pada pengukuran efektivitas strategi secara empiris di lapangan. Variasi konteks organisasi dan kematangan keamanan pada platform e-commerce juga dapat memengaruhi relevansi implementasi strategi tertentu, sehingga penerapan strategi perlu disesuaikan dengan karakteristik organisasi dan tingkat kesiapan sumber daya [10].

Berdasarkan temuan dan keterbatasan tersebut, penelitian lanjutan dapat diarahkan pada pengujian empiris efektivitas strategi pencegahan kebocoran data pada platform e-commerce di Indonesia. Studi kasus multi-platform dapat dilakukan untuk mengevaluasi bagaimana kontrol teknis, kepatuhan regulasi, dan tata kelola organisasi dijalankan dalam praktik, serta faktor apa yang menjadi penghambat implementasi [2], [8]. Selain itu, survei kematangan keamanan informasi dan privasi pada penyelenggara e-commerce dapat digunakan untuk memetakan tingkat kesiapan

organisasi terhadap UU PDP dan mengidentifikasi kontrol yang paling berdampak dalam menurunkan risiko kebocoran [12]. Penelitian lanjutan juga dapat mengembangkan model evaluasi kepatuhan yang mengintegrasikan indikator teknis (misalnya kontrol akses, enkripsi, monitoring), indikator kepatuhan (kebijakan privasi, SOP insiden), dan indikator tata kelola (audit, pelatihan, manajemen vendor) agar rekomendasi yang dihasilkan lebih aplikatif dan dapat dijadikan acuan peningkatan keamanan secara bertahap [1], [10].

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang dilakukan melalui pendekatan *Systematic Literature Review* (SLR), dapat disimpulkan bahwa pencegahan kebocoran data pribadi pada platform *e-commerce* merupakan permasalahan yang bersifat kompleks dan memerlukan pendekatan yang holistik. Hasil kajian menunjukkan bahwa strategi pencegahan yang efektif tidak hanya bergantung pada aspek teknis, seperti penerapan enkripsi data, kontrol akses berbasis prinsip *least privilege*, dan autentikasi multifaktor, tetapi juga harus didukung oleh kepatuhan terhadap regulasi perlindungan data serta tata kelola dan manajemen risiko organisasi yang baik. Integrasi antara strategi teknis, regulasi, dan organisasi terbukti mampu meminimalkan risiko kebocoran data dan meningkatkan kepercayaan pengguna terhadap platform *e-commerce*. Berdasarkan temuan tersebut, penelitian selanjutnya disarankan untuk mengkaji penerapan strategi pencegahan kebocoran data secara empiris pada platform *e-commerce* tertentu, serta mengevaluasi efektivitas implementasi regulasi perlindungan data dan standar keamanan informasi dalam praktik nyata.

DAFTAR PUSTAKA

[1] Y. Zhang and J. Chen, “Security vulnerabilities in third-party integrations of e-commerce platforms,” *Information Systems Frontiers*, vol. 24, no. 3, pp. 713–728, 2022.

[2] R. A. Pratama and Y. Nugroho, “Compliance with personal data protection regulation in Indonesian e-commerce platforms,” *Journal of Information Security and Applications*, vol. 73, p. 103410, 2023.

[3] I. H. Sarker, “Cybersecurity data science: A comprehensive overview,” *Journal of Big Data*, vol. 7, no. 41, pp. 1–29, 2020.

[4] A. Alasmary, A. Alhaidari, and M. Alqahtani, “Data breach prevention strategies in cloud-based e-commerce systems,” *Journal of Information Security and Applications*, vol. 54, p. 102528, 2020.

[5] K. Parsons *et al*., “Human aspects of information security: Awareness, behavior and compliance,” *Computers & Security*, vol. 88, p. 101604, 2020.

[6] P. Martin, “Data minimization and privacy protection in digital platforms,” *Computer Law & Security Review*, vol. 36, p. 105381, 2020.

[7] S. T. Smith and L. R. Brooks, “Insider threats and organizational risk management in information systems,” *Journal of Information Security*, vol. 12, no. 2, pp. 89–101, 2021.

[8] European Union Agency for Cybersecurity (ENISA), *Threat Landscape for E-Commerce*, Brussels, Belgium, 2021.

[9] M. Siponen, M. Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An empirical study,” *Information & Management*, vol. 57, no. 8, p. 103344, 2020.

[10] R. von Solms and J. van Niekerk, “Cybersecurity and information security governance,” *Computers & Security*, vol. 98, p. 102010, 2020.

[11] A. Shostack, “Threat modeling for secure system design,” *IEEE Security & Privacy*, vol. 18, no. 6, pp. 68–72, 2020.

[12] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, 2022.