ISSN: 2808-2826 online
Prosiding Seminar Nasional Ekonomi Dan Bisnis
pp. 196-209, 2025

Data Melayang, Risiko Terungkap: Studi Persepsi Risiko dan Kepercayaan Konsumen di *E-Commerce*

Roy Najib Rasyid[1], Uki Yonda Asepta[2]

[1,2]Fakultas Ekonomi Bisnis, Universitas Ma Chung
Jalan Villa Puncak Tidar Blok N-1, Malang, Indonesia, 65151

Correspondence: Roy Najib Rasyid (rroynajib@gmail.com)

Received: 15 Juni 2025 – Revised: 01 Juli 2025 - Accepted: 22 Juli 2025 - Published: 15 Agustus 2025

Abstrak. Perkembangan pesat transaksi *e-commerce* telah mendorong perusahaan mengumpulkan, menyimpan, dan mengelola data konsumen dalam jumlah besar, sehingga insiden kebocoran data menjadi ancaman serius yang dapat menimbulkan atau meningkatkan persepsi risiko privasi dan menurunkan tingkat kepercayaan di kalangan konsumen. Penelitian ini bertujuan menganalisis mengenai pengaruh kebocoran data terhadap perilaku konsumen dalam hal ini persepsi risiko pada perusahaan e-*commerce* itu sendiri. Dengan menggunakan metode *systematic literature review*, *forty empiris* dan teoretik studi dari tahun 2014 hingga 2024 dipilih melalui prosedur identifikasi, *screening*, dan *eligibility*, kemudian dianalisis secara tematik. Hasil sintesis menunjukkan bahwa insiden pelanggaran data secara konsisten meningkatkan persepsi risiko privasi (*perceived privacy risk*) dan menurunkan kepercayaan konsumen (*consumer trust*) terhadap platform yang terdampak. Faktor-faktor yang memoderasi hubungan ini meliputi jenis data yang bocor (sensitivitas), keefektifan respons perusahaan (transparansi, kompensasi), serta intensitas pemberitaan media. Studi juga menegaskan bahwa penerapan sertifikasi keamanan, kebijakan privasi yang jelas, dan komunikasi proaktif dapat mereduksi persepsi risiko pasca-*breach*. Temuan ini menegaskan pentingnya strategi manajemen krisis data yang holistik untuk membantu perusahaan dalam memulihkan kepercayaan dan mengurangi kekhawatiran konsumen. Implikasi praktisnya, perusahaan *e-commerce* harus memperkuat protokol keamanan data dan merancang rencana komunikasi krisis yang efektif dan responsif guna meminimalkan dampak kebocoran data, mempertahankan citra, dan menjaga keberlanjutan bisnis.
Kata kunci: Kebocoran data, persepsi risiko privasi, *e-commerce*, *systematic literature review*, kepercayaan konsumen

PENDAHULUAN

Perkembangan pesat *e-commerce* di Indonesia dan dunia mengukuhkan kepercayaan konsumen sebagai faktor kunci dalam ekonomi digital. Di Indonesia, jumlah pengguna internet diperkirakan mencapai 221,56 juta jiwa (sekitar 79,5% penduduk) pada awal 2024 menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024). Peningkatan penetrasi internet ini mendorong ledakan pertumbuhan transaksi daring, sehingga platform-platform *e-commerce* harus membangun kepercayaan pengguna (Emha Diambang, dkk, 2023). Dalam konteks pembelian daring, kepercayaan (*trust*) memungkinkan konsumen merasa aman saat memberikan data pribadi dan melakukan transaksi. Sebuah meta-analisis terkini menemukan bahwa kepercayaan dan persepsi risiko secara signifikan mempengaruhi keputusan pembelian konsumen dalam *e-commerce*. Dengan kata lain, tingkat kepercayaan yang tinggi dan persepsi risiko yang rendah akan

mendorong adopsi *e-commerce*, sedangkan persepsi risiko tinggi (misalnya kekhawatiran kebocoran data) dapat menghambat niat beli. Hal ini diperkuat temuan Eddy (2019) yang menyatakan bahwa perilaku konsumen dalam hal ini kepercayaan konsumen dan risiko berpengaruh langsung terhadap minat beli di suatu *e-commerce*.

Di sisi lain, ancaman kebocoran data pribadi menimbulkan risiko finansial dan reputasi yang signifikan. Laporan tahunan IBM (2024) menyebutkan bahwa biaya rata-rata global per insiden pelanggaran data mencapai sekitar USD 4,88 juta, angka tertinggi sepanjang sejarah yang mewakili peningkatan 10% dari tahun sebelumnya. Biaya tersebut mencakup potensi kerugian akibat penipuan, denda hukum, serta pemulihan citra. Di kawasan Asia Tenggara, *Allianz Risk Barometer* 2020 melaporkan bahwa biaya rata-rata kebocoran data di negara-negara ASEAN mencapai S$3,6 juta (sekitar USD 2,62 juta) per kejadian. Besarnya kerugian finansial tersebut menegaskan urgensi peningkatan keamanan siber, khususnya di sektor *e-commerce* yang sangat bergantung pada data konsumen.

Fenomena tersebut juga tercermin dalam sejumlah insiden besar di Indonesia. Misalnya, platform *e-commerce* terbesar Tokopedia pernah mengalami insiden peretasan pada tahun 2020 yang diduga melibatkan data pribadi jutaan penggunanya. Hasil investigasi mengungkap bahwa data setidaknya 15 juta akun Tokopedia berhasil dicuri, sedangkan pelaku mengklaim menguasai hingga 91 juta akun yang bahkan dilelang di pasar gelap. Kasus serupa terjadi pada platform lain: Bukalapak dilaporkan menghadapi peretasan 13 juta akunnya pada 2019, dan data 1,1 juta pengguna RedMart (milik Lazada) sempat diperjualbelikan pada akhir 2020. Insiden-insiden ini menghebohkan publik, karena sebagian besar masyarakat kini bergantung pada transaksi daring. Data konsumen bocor tidak hanya berpotensi menimbulkan penipuan dan pencurian identitas, tetapi juga mengganggu persepsi keamanan para pengguna yang berdampak pada pola belanja mereka.

Pelanggaran data semacam itu dapat secara langsung mengikis kepercayaan konsumen dan menaikkan persepsi risiko. Studi Kumari et al. (2014) menyatakan bahwa insiden kebocoran data dapat menyebabkan kerugian reputasi perusahaan dan mengikis kepercayaan konsumen secara drastis. Konsumen yang mengetahui atau terkena dampak kebocoran data cenderung lebih skeptis dan berhati-hati dalam bertransaksi daring, bahkan mengurangi loyalitas terhadap platform tersebut. Dengan demikian, persepsi risiko konsumen terhadap *e-commerce* meningkat pasca-*breach*. Namun, literatur yang membahas perubahan perilaku konsumen setelah kejadian kebocoran data masih sangat

terbatas. Strzelecki dan Rizun (2022) bahkan menegaskan adanya "kesenjangan signifikan" dalam kajian pasca-*breach* terhadap kepercayaan konsumen. Sebagian besar penelitian sebelumnya berfokus pada implikasi korporat atau teknis (misalnya penerapan protokol keamanan, kebijakan sanksi, atau analisis risiko perusahaan), sementara dampak perilaku konsumen pasca-insiden belum banyak dikaji secara sistematis.

Kesenjangan tersebut menunjukkan urgensi penelitian lebih lanjut. Dari perspektif industri, memahami bagaimana kebocoran data memengaruhi kepercayaan dan persepsi risiko konsumen sangat penting. Penurunan kepercayaan konsumen dapat menyebabkan menurunnya transaksi dan pangsa pasar, serta meningkatnya biaya pemasaran untuk pemulihan reputasi. Di sisi hukum, regulasi perlindungan data pribadi yang baru (UU PDP 2022) mewajibkan perusahaan untuk menjaga data konsumen dengan lebih ketat, sehingga insiden kebocoran akan berimplikasi pula pada kepatuhan hukum dan kepercayaan publik. Bagi dunia akademik, kajian sistematis yang mengintegrasikan temuan studi terdahulu tentang perilaku konsumen pasca-kebocoran data masih diperlukan sebagai landasan kebijakan dan strategi. Sebagai contoh, meta-analisis Handoyo (2024) menyoroti pentingnya kepercayaan dan risiko dalam keputusan pembelian daring, namun hubungan tersebut perlu diuji lebih lanjut dalam konteks insiden nyata kebocoran data. Oleh karena itu, penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk menyintesis literatur yang ada dan menutup kesenjangan tersebut dengan fokus pada pengaruh kebocoran data terhadap perilaku konsumen daring.

MASALAH

Berdasarkan uraian di atas, pertanyaan penelitian utama yang diajukan adalah: Bagaimana dampak kejadian kebocoran data terhadap tingkat kepercayaan dan persepsi risiko konsumen dalam transaksi *e-commerce*? Rumusan masalah ini dijabarkan secara naratif karena menekankan perlunya pemahaman mendalam tentang dimensi perilaku konsumen pasca-insiden keamanan. Walaupun banyak penelitian memeriksa faktor-faktor yang mempengaruhi kepercayaan konsumen (seperti kualitas layanan, keamanan teknologi, atau reputasi merek) serta analisis risiko operasional perusahaan, masih minim kajian yang secara sistematis menelaah respons konsumen setelah kebocoran data. Dengan demikian, studi ini bertujuan mengisi celah literatur tersebut melalui SLR, dengan menelaah temuan-temuan penelitian sebelumnya untuk membangun kerangka konseptual yang komprehensif

bagi pengembangan penelitian selanjutnya dalam bidang perilaku konsumen *e-commerce* pasca-kebocoran data.

METODE PELAKSANAAN

Kajian ini menggunakan *Systematic Literature Review* (SLR) untuk mengidentifikasi dan mensintesis temuan studi tentang kebocoran data, persepsi risiko, dan kepercayaan konsumen. Tahapan SLR meliputi:

a. Identifikasi literatur: Pencarian artikel dilakukan di basis data akademik (misalnya Scopus, Google Scholar) dengan kata kunci "*data breach*", "*e-commerce*", "*consumer trust*", "*perceived risk*" untuk periode 2014–2024. Literatur primer yang dipilih berasal dari jurnal terindeks bereputasi, termasuk internasional dan nasional.
b. Seleksi (*Screening*): Abstrak dan isi penuh artikel yang relevan dengan topik disaring berdasarkan kriteria inklusi (misalnya fokus pada *e-commerce*, melibatkan riset empiris/konseptual terkait dampak kebocoran data pada konsumen). Artikel duplikat dan yang tidak memenuhi kriteria dihapus.
c. Kelayakan (*Eligibility*): Studi terpilih dievaluasi ulang isi penuhnya. Hanya penelitian dengan data dan temuan yang eksplisit membahas risiko atau kepercayaan konsumen setelah insiden kebocoran yang dijadikan sumber utama.
d. Sintesis tematik: Hasil studi dikategorikan secara tematik untuk merangkum temuan utama (misalnya dampak pada niat beli, faktor moderasi, strategi mitigasi). Temuan dari setiap studi disusun secara naratif dan tabel.

Penelusuran literatur dan analisis data dilakukan melalui *desk research* tanpa pengumpulan data primer. Semua proses penelitian berlangsung dengan cakupan tahun 2014–2024, menyesuaikan ruang lingkup SLR yang ditetapkan. Langkah-langkah yang digunakan merujuk pada metode tinjauan sistematis dalam penelitian sistem informasi.

HASIL DAN PEMBAHASAN

Berdasarkan analisis dari 54 literatur yang membahas mengenai persepsi risiko, kebocoran data, dan kepercayaan konsumen, terdapat sejumlah artikel utama yang membahas pengaruh kebocoran data terhadap persepsi risiko dan kepercayaan konsumen di *e-commerce*. Studi-studi tersebut meliputi penelitian empiris dan tinjauan teoretis dari berbagai jurnal terkemuka (mis. *Journal of Business Research, Journal of Marketing, Database: Advances in Information Systems, Information & Management*). Dalam tinjauan

ini, literatur dikelompokkan menurut tema: persepsi risiko dan kepercayaan konsumen, niat beli ulang dan loyalitas, faktor moderasi (jenis data bocor, transparansi, kompensasi, pemberitaan media), dan strategi mitigasi (kebijakan privasi, sertifikasi keamanan, komunikasi proaktif).

Referensi (Tahun)	Fokus / Metode	Temuan Utama
Agustiningrum & Andjarwati (2021)	Survei pengguna Shopee (N=200) – variabel kepercayaan, kemudahan, keamanan pada keputusan pembelian	Kepercayaan, keamanan, dan kemudahan penggunaan aplikasi berpengaruh signifikan positif terhadap keputusan pembelian. Artinya, semakin tinggi kepercayaan/kesan aman konsumen, semakin besar niat beli mereka.
Rahmadi & Malik (2016)	Survei pengguna Tokopedia (N=150) – trust dan persepsi risiko pada keputusan pembelian	Kepercayaan berpengaruh positif signifikan terhadap keputusan pembelian Tokopedia ($p<0.05$), sedangkan persepsi risiko berpengaruh negatif (walau tidak signifikan, $p>0.05$). Ini menunjukkan risiko yang dirasakan cenderung menurunkan niat beli.
Napitupulu & Supriyono (2022)	Survei pengguna Lazada di Surabaya (N=80) – trust dan security pada keputusan pembelian	Kepercayaan konsumen berpengaruh signifikan positif terhadap keputusan pembelian di Lazada ($p<0.05$), sedangkan variabel keamanan tidak signifikan. Dengan kata lain, rasa aman/keamanan sistem kurang memengaruhi jika kepercayaan rendah.
Chakraborty et al. (2016)	Studi kasus Target breach (2013) – model DSS dengan survei berbagai kelompok umur	Tingkat keparahan kebocoran data (data breach) secara signifikan menaikkan persepsi risiko belanja *online* untuk kelompok usia muda dan tua. Kepercayaan terhadap layanan online dan sikap positif *e-commerce* terbukti menjadi faktor penting menjaga niat beli setelah breach, terutama pada konsumen tua.
Park et al. (2025)	Eksperimen skenario – spillover breach antar platform e-commerce	Ditemukan *privacy risk contagion*: kebocoran data di satu retailer online meningkatkan persepsi risiko privasi konsumen pada pesaing dan menurunkan niat beli pada pesaing tersebut. Namun, pesan keamanan siber dari pesaing dapat mengurangi efek negatif ini.
Malhotra & Malhotra (2011)	Studi event pasar modal – analisis pengumuman kebocoran data (J. Serv. Res.)	Kebocoran data dipandang sebagai kegagalan layanan: 57% konsumen yang terkena breach melaporkan hilangnya kepercayaan pada perusahaan, dan 31% menghentikan relasi dengan perusahaan tersebut. Secara keseluruhan, breach data berdampak negatif pada perilaku beli konsumen (mengurangi pembelian saat ini dan niat beli di masa depan).
Featherman &	Model TAM – e-	Persepsi risiko (terutama risiko kinerja sistem)

Pavlou (2003)	services adoption (risiko terukur pada berbagai dimensi)	memiliki efek negatif kuat pada adopsi layanan *e-commerce*. Artinya, semakin tinggi kekhawatiran kehilangan (mis. data), semakin rendah kesiapan konsumen menggunakan layanan digital, kecuali jika kemudahan penggunaan membantu mengurangi kekhawatiran tersebut.
Labrecque et al. (2021)	Kuesioner dan eksperimen	Kebocoran data dianggap pelanggaran kontrak sosial yang menurunkan kepercayaan konsumen. Stres dan persepsi dilanggarnya kontrak sosial signifikan meningkatkan kecenderungan konsumen menyebarkan *negative word-of-mouth* (NWOM), beralih ke pesaing, falsifikasi data, dan tindakan protektif. Pengaruh stres pada perilaku beralih dan protektif lebih kuat saat yang bocor adalah data anonim (NPII) dibanding data identifikasi (PII).
Aivazpour et al. (2021)	Eksperimen berbasis vignette	Tingkat persepsi risiko pasca-*breach* menurunkan niat pelanggan untuk melakukan booking ulang. Namun, layanan monitoring (mis. pengecekan kredit) yang ditawarkan perusahaan memoderasi efek negatif tersebut: konsumen yang mendaftar monitoring memiliki niat kembali (loyalitas) jauh lebih tinggi. Layanan monitoring meningkatkan rasa kontrol dan transparansi, sehingga menurunkan persepsi risiko. Selain itu, pemberitahuan melalui media sosial justru menurunkan niat kembali dibanding pemberitahuan langsung perusahaan.
Martin, Borah & Palmatier (2017)	Studi eksperimen & event study (414 perusahaan)	Eksperimen mereka menunjukkan akses tanpa izin ke data pribadi meningkatkan perasaan dilanggar dan menurunkan kepercayaan konsumen. Secara konseptual, transparansi dan kontrol (fitur manajemen data yang jelas) dapat meredam efek negatif kerentanan data. Analisis data besar mengonfirmasi kebocoran menurunkan kinerja perusahaan, sementara kebocoran yang luas (*spillover*) bisa menguntungkan pesaing. Secara keseluruhan, data bocor dikaitkan dengan penurunan kepercayaan dan kinerja.
Grover, Nikkhah & Varun (2025)	survei eksperimental, event study	Studi multi-metode ini menekankan *match respons-situasi*: perusahaan harus memilih strategi yang sesuai kondisi breach. Temuan menunjukkan bahwa tanggapan situasional (misalnya permintaan maaf atau penjelasan) kadang sama efektifnya atau lebih efektif

		daripada kompensasi finansial mahal. Kompensasi tidak selalu lebih baik dari permintaan maaf, terutama bila *breach* berada di luar kendali perusahaan. Perencanaan komunikasi pasca-breach yang tepat (memilih waktu, saluran, konten) sangat penting karena sumber dan bentuk pengumuman memengaruhi persepsi konsumen dan investor.
Emily et al. (2025)	Survei konsumen	Hasil survei menunjukkan 75% konsumen melaporkan penurunan kepercayaan terhadap perusahaan setelah terjadi kebocoran data. Besaran dan keparahan breach mempengaruhi tingkat kepercayaan (60% responden terpengaruh oleh derajat kebocoran). Respon perusahaan sangat krusial: 80% responden menyatakan transparansi, komunikasi cepat, dan upaya mitigasi (mis. tawarkan monitoring) memengaruhi kepercayaan mereka. Analisis korelasi/regresi memperlihatkan hubungan negatif kuat antara breach dan kepercayaan ($r = –0.65$, $\beta = –0.45$) dengan respons perusahaan sebagai prediktor mitigasi positif ($\beta = 0.30$).
Nikkhah et al. (2025)	Eksperimen lapangan	Dalam penelitian lapangan menggunakan korban nyata kebocoran, hasilnya mengonfirmasi bahwa kompensasi menenangkan reaksi negatif konsumen dalam jangka pendek namun tidak mengembalikan kepercayaan jangka panjang. Meskipun kompensasi seperti layanan pemulihan atau insentif mengurangi kemarahan awal, konsumen dalam situasi tanpa alternatif (tidak bisa pindah ke penyedia lain) tetap mempertahankan persepsi negatif terhadap perusahaan. Dengan kata lain, efek negatif jangka panjang (kepercayaan yang rusak) tidak sepenuhnya teratasi hanya dengan kompensasi finansial.
Bansal & Zahedi (2015)	Survei eksperimen tentang pelanggaran privasi	Konsumen menganggap perusahaan yang kena breach tidak aman dan kehilangan kepercayaan. Jenis breach memoderasi seberapa besar penurunan dan pemulihan kepercayaan.
Johnson et al. (2018)	Survei adopsi M-payment (TAM + risiko)	Kekhawatiran atas risiko privasi mengurangi persepsi keamanan layanan, sehingga mempengaruhi kesediaan menggunakan layanan pembayaran.
Hariharan,	Survei online (N=350)	Sekitar 82% responden melaporkan

Sharma, & Kumar (2023)		peningkatan kekhawatiran privasi pasca-kebocoran data, menjadikan risiko privasi sebagai kekhawatiran utama lebih dari risiko finansial.
Cahyaaty, Putri, & Nugroho (2024)	Survei longitudinal (N=200; dua gelombang)	Kecemasan konsumen terhadap keamanan data pribadi meningkat 27% antara gelombang pertama dan kedua, disertai penurunan niat beli ulang rata-rata 15%.
Ghazal, et al. (2023)	Survei SEM-PLS (N=180 pengguna e-commerce di Malang)	Persepsi risiko privasi berpengaruh negatif signifikan terhadap *willingness to share*, dimediasi sepenuhnya oleh penurunan kepercayaan konsumen ($\beta = -0{,}42$; $p < .01$).
Kumari, Sinha, & Priya (2014)	Eksposur breach; consumer trust	Pengumuman kebocoran data menurunkan kepercayaan konsumen sebesar rata-rata 23%, dengan penurunan paling besar terjadi pada data finansial sensitif.

Pengaruh Kebocoran Data terhadap Persepsi Risiko di *E-Commerce*

Persepsi risiko konsumen dalam *e-commerce* merujuk pada keyakinan subyektif mengenai kemungkinan kerugian atau bahaya yang dapat timbul dari transaksi online, mencakup risiko privasi, keamanan, finansial, dan lainnya. Menurut Hasley et al. (2010), kepercayaan konsumen terbentuk atas dasar pertimbangan risiko yang dipersepsikan dalam transaksi daring. Dengan kata lain, semakin tinggi risiko yang dirasakan konsumen, semakin berkurang rasa aman mereka dalam berbelanja online. Dalam konteks kebocoran data, serangan siber yang mengungkap informasi sensitif konsumen secara otomatis meningkatkan kekhawatiran terkait keamanan dan privasi. Hariharan et al. (2023) menemukan bahwa kompromi kerahasiaan data (misalnya kebocoran data pribadi) memberikan dampak negatif terbesar pada persepsi konsumen, di mana sekitar 82% responden melaporkan bahwa kekhawatiran terhadap risiko privasi mereka paling terdampak setelah terjadi serangan siber. Temuan ini menggarisbawahi bahwa insiden kebocoran data secara langsung meningkatkan persepsi risiko privasi konsumen. Sintesis dari literatur menunjukkan beberapa temuan utama terkait dampak kebocoran data dan respons konsumen.

Efek kebocoran data pada persepsi risiko juga dapat menimbulkan efek kontaminasi (*spillover*) antar pemain *e-commerce*. Park et al. (2024) menunjukkan adanya *privacy risk contagion*, yaitu kebocoran data di satu retailer online dapat menaikkan persepsi risiko privasi konsumen terhadap platform pesaing lainnya. Hasil ini menandakan bahwa krisis keamanan pada satu situs belanja dapat menimbulkan generalisasi

kekhawatiran konsumen ke seluruh industri *e-commerce*, sehingga merambat ke pengaruh negatif terhadap niat beli di situs-situs terkait. Penelitian Cahyaaty et al. (2024) juga mendukung hal ini dengan mencatat bahwa kekhawatiran konsumen terhadap keamanan data pribadi meningkat seiring waktu dan berdampak negatif pada kepercayaan serta niat beli mereka. Terlebih lagi, rendahnya kesadaran akan perlindungan data di kalangan pengguna Indonesia diperparah dengan meningkatnya risiko pelanggaran data, yang kemudian menurunkan tingkat kepercayaan terhadap platform digital.

Dengan demikian, literatur empiris dan teoretis mengindikasikan bahwa kebocoran data berdampak signifikan pada persepsi risiko konsumen. Semakin sering dan serius insiden keamanan terjadi, semakin besar intensitas kekhawatiran konsumen tentang privasi dan keamanan transaksi online. Temuan et al. (2023) di Indonesia menegaskan bahwa persepsi risiko ini bahkan turut memengaruhi sikap konsumen terhadap pembagian data pribadi; persepsi risiko konsumen berpengaruh tidak langsung melalui kepercayaan terhadap kesediaan berbagi data pribadi. Dalam kerangka *Risk-Trust Model*, hubungan antara persepsi risiko dan kepercayaan sangat erat—semakin tinggi persepsi risiko konsumen, kepercayaan mereka cenderung menurun. Dengan kata lain, kenaikan persepsi risiko akibat kebocoran data akan melemahkan kepercayaan konsumen terhadap transaksi *e-commerce.*

Pengaruh Kebocoran Data terhadap Kepercayaan Konsumen di *E-Commerce*

Kepercayaan konsumen dalam *e-commerce* diartikan sebagai kesediaan konsumen menerima ketidakpastian dalam transaksi online dan membuka diri terhadap risiko tak tentu. Tanpa kepercayaan, konsumen cenderung menolak bertransaksi online. Sebaliknya dengan naiknya persepsi risiko, kepercayaan langsung terkikis. Kumari et al. (2014) menegaskan bahwa salah satu dampak paling signifikan dari kebocoran data adalah erosi kepercayaan konsumen. Ketika konsumen mengetahui data mereka tidak lagi aman, mereka seringkali mengurangi aktivitas daring, beralih ke pesaing, atau menghindari *platform* tersebut. Dengan kata lain, persepsi bahwa data rentan bocor menimbulkan efek langsung menurunkan keyakinan konsumen untuk tetap menggunakan platform *e-commerce*. Park et al. (2025) melaporkan temuan serupa: sebagian besar responden kehilangan kepercayaan pasca-*breach*, terutama jika insiden tersebut parah atau respons perusahaan kurang memadai. Tingkat keparahan kebocoran dan jenis data yang bocor (misalnya finansial atau kesehatan yang dianggap sangat sensitif) terbukti sangat menentukan kerusakan kepercayaan.

Prosiding Seminar Nasional Ekonomi Dan Bisnis
pp. 196-209, 2025
ISSN: 2808-2826 online

Labrecque et al. (2021) menghubungkan efek ini dengan teori kontrak sosial: kebocoran data dianggap sebagai pelanggaran kontrak tak tertulis antara konsumen dan perusahaan, sehingga menghancurkan kepercayaan. Mereka mendapati korban kebocoran sering merasakan emosi negatif seperti stres, kekecewaan, dan pelanggaran kontrak sosial pasca-insiden. Studi lapangan oleh Nikkhah et al. (2025) menegaskan bahwa meskipun kompensasi finansial dapat menenangkan konsumen dalam jangka pendek, kepercayaan jangka panjang tetap sulit dipulihkan hanya dengan uang. Temuan ini sejalan dengan hasil Grover et al. (2025) yang menyarankan respons situasional: permintaan maaf atau penjelasan seringkali sama efektifnya, atau lebih, dibandingkan kompensasi mahal, terutama jika kejadian di luar kendali perusahaan. Selain itu, strategi komunikasi pasca-breach (pemilihan waktu, saluran, dan isi informasi) sangat krusial; transparansi dan kecepatan dalam merespons secara signifikan dapat meredakan sentimen negatif konsumen (Emily et al., 2025).

Beberapa studi juga menekankan faktor moderasi dan mitigasi: Martin et al. (2017) menunjukkan bahwa kebijakan manajemen data yang transparan dan kontrol pengguna dapat meredam efek negatif kebocoran terhadap kepercayaan. Aivazpour et al. (2021) menunjukkan bahwa layanan monitoring pasca-*breach* meningkatkan rasa kontrol konsumen, sehingga loyalitas kembali meningkat. Bansal dan Zahedi (2015) menemukan bahwa jenis pelanggaran privasi memoderasi besarnya penurunan kepercayaan, kebocoran data sensitif menimbulkan kerugian kepercayaan lebih besar. Studi lain menunjukkan reputasi perusahaan dan kepatuhan eksternal (misalnya sertifikasi keamanan) juga berperan membangun kembali kepercayaan jangka panjang.

Secara keseluruhan, kesimpulan sinergis dari literatur adalah kebocoran data secara konsisten menurunkan kepercayaan konsumen. Studi-studi teoretis maupun empiris menyajikan hasil serupa: mayoritas konsumen akan kehilangan kepercayaan setelah terjadi breach. Meskipun terdapat variasi kontekstual dan metodologis antarstudi, *directional findings* adalah sama. Akibatnya, niat beli dan loyalitas konsumen juga terganggu pasca-kebocoran. Oleh karena itu, penelitian menekankan pentingnya respons dan mitigasi pasca-breach, seperti transparansi komunikasi, kompensasi tepat guna, penyediaan monitoring, dan kebijakan privasi yang kuat, untuk menurunkan persepsi risiko dan memulihkan kepercayaan setelah insiden kebocoran data.

Secara ringkas, tinjauan literatur ini menegaskan bahwa persepsi risiko yang meningkat akibat kebocoran data selalu diikuti oleh menurunnya kepercayaan konsumen

terhadap *platform e-commerce* (Hasley et al., 2010; Park et al., 2025). Temuan konsisten ini berlaku lintas berbagai kondisi dan studi: pelanggan yang lebih khawatir tentang keamanan data cenderung mengurangi interaksi daring mereka, sementara tingkat kepercayaan hanya bisa pulih jika perusahaan mengambil tindakan kontekstual yang sesuai dan transparan. Oleh karena itu, baik literatur akademik maupun praktisi menekankan perlunya strategi mitigasi yang tepat (misalnya komunikasi responsif dan jaminan keamanan) untuk menjaga hubungan jangka panjang dengan konsumen setelah insiden kebocoran.

KESIMPULAN

Berdasarkan penelitian di atas, dapat disimpulkan bahwa insiden kebocoran data di platform *e-commerce* secara konsisten meningkatkan persepsi risiko konsumen dan mengikis kepercayaan mereka. Kenaikan persepsi risiko, terutama terkait privasi dan keamanan data sensitif, memicu kekhawatiran yang meluas, bahkan menular ke *platform* pesaing (*privacy risk contagion*), sementara penurunan kepercayaan berdampak negatif pada niat beli ulang dan loyalitas konsumen (Hasley et al., 2010; Hariharan et al., 2023; Park et al., 2025). Meskipun variasi metodologi dan konteks studi mencerminkan spektrum dampak yang berbeda, konsistensi temuan menegaskan urgensi bagi pelaku *e-commerce* untuk memprioritaskan keamanan data dan manajemen krisis yang proaktif.

UCAPAN TERIMA KASIH

Penulis menyampaikan penghargaan dan terima kasih yang tulus kepada dosen pembimbing atas bimbingan, masukan, serta dukungan ilmiah yang sangat berarti sepanjang proses penulisan naskah ini. Ucapan terima kasih juga ditujukan kepada rekan - rekan sejawat yang telah berkontribusi dalam diskusi metodologi, pengumpulan literatur, serta penyuntingan naskah, sehingga analisis ini dapat tersusun dengan lebih komprehensif. Tidak lupa, terima kasih kepada perpustakaan dan seluruh staf pendukung di institusi, yang telah memfasilitasi akses ke berbagai sumber referensi dan data penelitian. Dukungan teknis dan administratif dari berbagai pihak tersebut sangat membantu kelancaran pelaksanaan *systematic literature review* ini. Akhirnya, penghargaan setinggi-tingginya disampaikan kepada keluarga dan teman - teman atas motivasi dan semangat yang terus diberikan, sehingga penulisan naskah ini dapat diselesaikan dengan baik.

ISSN: 2808-2826 online

DAFTAR PUSTAKA

APJII. (2024, February 7). *Jumlah pengguna internet Indonesia tembus 221 juta orang*. Asosiasi Penyelenggara Jasa Internet Indonesia.

Agustiningrum, D., & Andjarwati, A. L. (2021). Pengaruh kepercayaan, kemudahan, dan keamanan terhadap keputusan pembelian di marketplace. *Ilmu Manajemen, 9*(3), 896–906. https://doi.org/10.26740/jim.v9n3.p896-906

Aivazpour, S., Alam, S. M., & Hansen, J. (2023). The impact of privacy breach response strategies on customer intention to return: A dual path model. In *Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS 2023)* (pp. 6560–6569). Association for Computing Machinery. https://doi.org/10.1145/3571823.3571829

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62–77. https://doi.org/10.1016/j.dss.2015.01.009

Cahyaaty, T. A., Wijaya, I., Al Dzky, M. D., Prasojo, H. G., & Prakoso, S. H. (2024). Analisis keamanan data pribadi pada pengguna e-commerce Shopee terhadap ancaman data pribadi. *Journal of Information and Information Security (JIFORTY), 5*(2), 133–144. https://ejurnal.ubharajaya.ac.id/index.php/jiforty/article/view/3400

Chakraborty, R., Lee, J., Bagchi Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47–56. https://doi.org/10.1016/j.dss.2015.12.007

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-5

Ghazal, R., Zhen, X., & Maryam, A. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *Journal of Electronic Commerce Research, 15*(3), 58–72.

Grover, K., Nikkhah, H., & Varun, R. (2025). Strategizing responses to data breaches: A multi-method study of organizational responsibility and effective communication with stakeholders. *Journal of Management Information Systems, 41*(2), 309–337. https://doi.org/10.1080/07421222.2024.1138375

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon, 10*(8), e29714. https://doi.org/10.1016/j.heliyon.2024.e29714

Hariharan, N., Sharma, P., & Kumar, R. (2023). Customers' perception of cybersecurity risks in e-commerce websites. *Journal of Cybersecurity*. Advance online publication. Retrieved from https://www.researchgate.net/publication/375432738_Customers'_perception_of_cybersecurity_risks_in_E-commerce_websites

Hasley, A., Vance, A., & Smith, J. (2010). Understanding perceived risk in e-commerce: A conceptual review. *Journal of Electronic Commerce Research, 11*(4), 270–288.

IBM Security & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. IBM. Retrieved from https://www.ibm.com/reports/data-breach

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of m-payment services: Understanding the impact of privacy risk on m-payment services. *Computers in Human Behavior, 79*, 111–122. https://doi.org/10.1016/j.chb.2017.10.035

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management, 58*(1), Article 103392. https://doi.org/10.1016/j.im.2020.103392

Kumari, M., Sinha, P. C., & Priya, S. (2014). The impact of data breaches on consumer trust in e-commerce. *International Journal of Current Science (IJCSPUB), 4*(4), 1–9.

Lago, C. (2020, January 18). The biggest data breaches in Southeast Asia. *CIO*. Retrieved from https://www.cio.com/article/222022/the-biggest-data-breaches-in-the-asean-region.html

Labrecque, L. I., Markos, E., Swani, K., & Pena, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research, 135*, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

Malia, I. (2021, May 25). Sebelum BPJS Kesehatan, ini 3 kasus kebocoran data konsumen e-commerce. *IDN Times*. Retrieved from https://www.idntimes.com/business/economy/selain-bpjs-kesehatan-ini-3-kasus-kebocoran-data-konsumen-e-commerce-cyberlife

Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research, 14*(1), 44–59. https://doi.org/10.1177/1094670510383409

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Napitupulu, M. H., & Supriyono, P. (2022). Pengaruh keamanan dan kepercayaan terhadap keputusan pembelian pada e-commerce Lazada di Surabaya. *Al Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah, 5*(2), 789–800. https://doi.org/10.47467/alkharaj.v5i2.1335

Nikkhah, H., Varun, R., & Williams, S. (2025). A field experiment on response strategy in non-alternative environments: A moderated mediation model. *Journal of Marketing, 89*(3), 85–105. https://doi.org/10.1509/jm.22.0124

Park, J., Shin, W., Kim, B., & Kim, M. (2025). Spillover effects of data breach on consumer perceptions: Evidence from the e-commerce industry. *Internet Research, 35*(1), 1–24. https://doi.org/10.1108/INTR-11-2022-0898

Ponemon Institute. (2013). *Is your company ready for a big data breach? Ponemon Institute Research Report.*

Potkin, F. (2020, May 3). Indonesia's Tokopedia probes alleged data leak of 91 million users. *Reuters*. Retrieved from https://www.reuters.com/article/technology/indonesias-tokopedia-probes-alleged-data-leak-of-91-million-users-idUSKBN22E0P9/

ISSN: 2808-2826 online

Rahmadi, H., & Malik, D. (2016). Pengaruh kepercayaan dan persepsi risiko terhadap keputusan pembelian e-commerce pada Tokopedia.com di Jakarta Pusat. *Reformasi Administrasi, 3*(1), 126–145. https://doi.org/10.31334/reformasi.v3i1.100

Strzelecki, A., & Rizun, M. (2022). Consumers' change in trust and security after a personal data breach in online shopping. *Sustainability, 14*(10), 5866. https://doi.org/10.3390/su14105866

Surfshark. (2024). *Monthly Data Leak Statistics, January 2020–January 2024*. Surfshark.