Inovan Publisher

Orbit: Jurnal Ilmu Multidisplin Nusantara

| ISSN (Online) 3064-5883 |

DOI: 10.63217/orbit.v2i1.189

Analisis Penanganan Insiden Kebocoran Data Tokopedia dan Dampaknya terhadap Kepercayaan Publik

Devita Naila Sari[1], Achmad Fauzi[2], Sabila Nur Alya[3], Intan Larasati[4], Kesya Rizkianti Sutrisna[5], Syafi'il Ibad Zam Zami[6], Niko Ahmad Yunus[7]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, nailasari1213@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, sabilaalyaa@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, intanlarasati110503@gmail.com
[5]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, kesyarizkiantii@gmail.com
[6]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, syafilibad14@gmail.com
[7]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, nikoahmad726@gmail.com

Corresponding Author: nailasari1213@gmail.com

Abstract: *This study analyzes the handling of the 2020 Tokopedia data breach incident involving 91 million user accounts and its impact on public trust. Using a descriptive qualitative method through a systematic literature review (SLR), this study identifies the characteristics of the incident that occurred due to the exploitation of security vulnerabilities in the API endpoint, which included personal data such as email addresses, phone numbers, usernames, and password hashes. Analysis based on the ISO/IEC 27001 standard and information security management principles shows that Tokopedia's response had significant weaknesses in the areas of prevention, early detection, communication transparency, and compliance with data protection obligations. Although the company updated its security systems after the incident, its defensive approach and lack of transparency in crisis communication actually worsened public perception. These findings indicate that the decline in public trust was not only caused by the large scale of the data breach, but also by the delayed response, lack of transparency, and the spread of negative opinions through social media. This study found that in order to restore public trust after a data security incident, visible technical improvements, consistent and transparent communication, compliance with data protection regulations, and the implementation of comprehensive and sustainable international security standards are necessary.*

Keywords: *Data Breach, Tokopedia, Information Security Management, Public Trust, Crisis Communication, ISO/IEC 27001*

Abstrak: Penelitian ini menganalisis penanganan insiden kebocoran data Tokopedia tahun 2020 yang melibatkan 91 juta akun pengguna serta dampaknya terhadap kepercayaan publik. Dengan menggunakan metode kualitatif deskriptif melalui Systematic Literature Review (SLR), penelitian ini mengidentifikasi karakteristik insiden yang terjadi akibat eksploitasi celah keamanan pada endpoint API, mencakup data pribadi seperti email, nomor telepon, nama

pengguna, dan hash password. Analisis berdasarkan standar ISO/IEC 27001 dan prinsip manajemen keamanan informasi menunjukkan bahwa respons Tokopedia memiliki kelemahan signifikan dalam aspek pencegahan, deteksi dini, transparansi komunikasi, dan kepatuhan terhadap kewajiban perlindungan data. Meskipun perusahaan melakukan pembaruan sistem keamanan pasca-insiden, pendekatan komunikasi krisis yang defensif dan kurang transparan justru memperburuk persepsi publik. Temuan ini menunjukkan bahwa peningkatan kepercayaan publik tidak hanya disebabkan oleh skala kebocoran yang besar, tetapi juga karena keterlambatan respons, kurangnya transparansi, dan penyebaran opini negatif melalui media sosial. Studi ini menemukan bahwa untuk mendapatkan kembali kepercayaan publik setelah insiden keamanan data, diperlukan perbaikan teknis yang terlihat, komunikasi yang konsisten dan transparan, kepatuhan terhadap peraturan perlindungan data, dan penerapan standar keamanan internasional yang lengkap dan berkelanjutan.

Kata Kunci: Kebocoran Data, Tokopedia, Manajemen Keamanan Informasi, Kepercayaan Publik, Komunikasi Krisis, *ISO/IEC 27001*.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan *e-commerce* sebagai sarana transaksi digital yang praktis dan efisien. Namun, kemudahan ini juga diiringi oleh meningkatnya risiko keamanan siber, termasuk pencurian data, peretasan sistem, dan manipulasi informasi. Di Indonesia, kesadaran akan pentingnya perlindungan data masih relatif rendah, sementara regulasi yang mengatur keamanan data pribadi sebelum tahun 2022 dinilai belum cukup kuat untuk melindungi kepentingan konsumen. Kondisi ini membuat insiden kebocoran data menjadi ancaman nyata bagi platform digital.

Salah satu insiden terbesar yang pernah terjadi adalah kebocoran data pengguna Tokopedia pada tahun 2020. Sebanyak 91 juta data pengguna bocor dan diperjualbelikan di *dark web* akibat peretasan yang dilakukan oleh kelompok *ShinyHunters*. Data yang dibocorkan meliputi nama lengkap, email, nomor telepon, tanggal lahir, *username*, hingga *hash password*. Peristiwa ini menyoroti lemahnya sistem keamanan informasi perusahaan serta minimnya transparansi dalam penanganan insiden (Lestari & Prabowo, 2020). Kasus ini juga menjadi pendorong percepatan pengesahan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022).

Berbagai penelitian terdahulu menunjukkan fenomena menarik terkait dampak insiden ini terhadap perilaku dan persepsi konsumen. Studi Rahmania, Pradekso, dan Ayun (2021) mengungkap bahwa terpaan berita kebocoran data berpengaruh signifikan terhadap kepercayaan pengguna, meskipun sebagian besar pengguna tetap memilih menggunakan Tokopedia karena minimnya pengetahuan mereka tentang insiden tersebut. Sebaliknya, penelitian Roos, Setyabudi, dan Gono (2022) menemukan bahwa kebocoran data tidak berpengaruh signifikan terhadap citra Tokopedia karena kualitas layanan yang dirasakan pengguna masih dianggap memadai.

Dari perspektif konsumen, penelitian lain menunjukkan bahwa sebagian besar pengguna tidak mengalami dampak langsung meskipun data mereka bocor, meski terdapat keluhan mengenai *spam*, penyalahgunaan informasi pribadi, dan aktivitas mencurigakan. Kajian hukum dan keamanan informasi juga menyoroti bahwa Tokopedia belum memenuhi standar perlindungan data yang optimal (Wijaya, 2021). Beberapa penelitian menyimpulkan bahwa perusahaan kurang menerapkan sistem pemantauan aktif, enkripsi menyeluruh, dan standar keamanan seperti *ISO/IEC 27001*, serta dinilai kurang transparan dalam komunikasi krisis saat insiden terjadi.

Berdasarkan berbagai temuan tersebut, terlihat adanya kesenjangan antara tingkat keparahan insiden kebocoran data dengan tingginya tingkat kepercayaan pengguna terhadap Tokopedia. Fenomena ini menimbulkan pertanyaan mengenai bagaimana penanganan insiden

dilakukan, bagaimana komunikasi krisis dibentuk, serta faktor apa yang memengaruhi resiliensi kepercayaan publik meskipun terjadi pelanggaran data berskala besar (Hartono & Dewi, 2023). Oleh karena itu, penelitian ini bertujuan menganalisis penanganan insiden kebocoran data Tokopedia dan dampaknya terhadap kepercayaan publik dengan meninjau aspek teknis keamanan informasi, regulasi yang berlaku, dan respons masyarakat. Secara khusus, penelitian ini bertujuan mengidentifikasi kronologi dan karakteristik insiden kebocoran data Tokopedia serta sejauh mana data pengguna yang terekspos, menganalisis langkah-langkah penanganan insiden yang dilakukan Tokopedia dan mengevaluasi efektivitasnya berdasarkan prinsip manajemen krisis digital dan standar keamanan siber, serta menganalisis dampak insiden terhadap tingkat kepercayaan publik dan persepsi pengguna melalui data sekunder.

Berdasarkan latar belakang yang telah diuraikan diatas maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana kronologi dan karakteristik insiden kebocoran data yang terjadi pada Tokopedia, serta sejauh mana data pengguna yang terekspos dapat diidentifikasi melalui sumber-sumber sekunder yang kredibel?
2. Bagaimana langkah-langkah penanganan insiden yang dilakukan oleh Tokopedia, dan sejauh mana respons tersebut dapat dinilai efektif berdasarkan prinsip-prinsip manajemen krisis digital, keamanan siber, serta standar penanganan kebocoran data yang umum digunakan?
3. Apa saja dampak insiden kebocoran data terhadap tingkat kepercayaan publik terhadap Tokopedia, dan bagaimana persepsi, sentimen, serta keyakinan pengguna dapat dianalisis melalui data sekunder seperti pemberitaan, laporan analitik, serta respons publik di ruang digital?

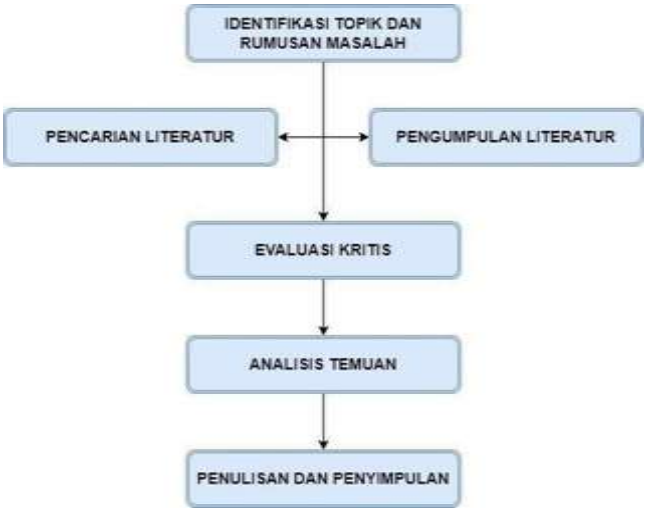
METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode *Systematic Literature Review* (SLR). Jenis penelitian ini adalah penelitian deskriptif yang bertujuan untuk menganalisis dan mensintesis temuan-temuan dari berbagai literatur terkait insiden kebocoran data Tokopedia tahun 2020. Subjek penelitian adalah berbagai dokumen ilmiah berupa jurnal, prosiding, dan laporan penelitian yang membahas insiden kebocoran data Tokopedia, penanganan insiden siber, serta dampaknya terhadap kepercayaan publik dalam konteks Indonesia.

Waktu penelitian dilakukan pada periode November 2025 hingga Desember 2025. Pencarian literatur dilakukan melalui database daring seperti *Google Scholar* dengan menggunakan kata kunci pencarian yang relevan, antara lain "*data breach* Tokopedia", "penanganan insiden siber Indonesia", "*cybersecurity e-commerce*", "kepercayaan publik terhadap platform digital", dan "respons perusahaan terhadap kebocoran data". Proses pencarian juga dibantu oleh platform berbasis *AI* seperti *Connected Papers* dan *Research Rabbit* untuk memperluas jaringan referensi dan menemukan literatur yang saling berkaitan.

Instrumen penelitian yang digunakan adalah protokol *Systematic Literature Review* (SLR) dengan kriteria inklusi yang telah ditetapkan. Kriteria inklusi meliputi jurnal, prosiding, atau laporan penelitian yang diterbitkan antara tahun 2019-2024, membahas insiden kebocoran data, penanganan insiden siber, atau dampaknya terhadap kepercayaan publik khususnya pada konteks Indonesia, serta tersedia dalam bentuk teks lengkap. Berdasarkan proses seleksi tersebut, terpilih 15 literatur primer yang paling relevan dengan topik penelitian.

Prosedur dan teknik penelitian dilakukan melalui beberapa tahapan, berikut adalah diagram tahapannya:



Gambar 1. Diagram langkah-langkah pelaksanaan penelitian

Metode penelitian ini mengumpulkan dan menganalisis informasi dari berbagai sumber tertulis untuk memahami topik penelitian secara mendalam.

HASIL DAN PEMBAHASAN

Kronologi dan Karakteristik Insiden Kebocoran Data

Insiden kebocoran data Tokopedia pada tahun 2020 tercatat sebagai salah satu pelanggaran keamanan siber terbesar di Indonesia. Diperkirakan sekitar 91 juta akun pengguna terekspos di forum peretas, dengan data yang bocor meliputi email, nama pengguna, nomor ponsel, hingga hash password. Menurut Afip et al. (2025), insiden ini bukanlah kejadian mendadak, melainkan akumulasi dari kerentanan sistem yang tidak terdeteksi dalam periode waktu yang panjang. Hasil analisis mereka mengungkap bahwa pola serangan memanfaatkan celah pada *endpoint* API, yang memang menjadi salah satu titik paling rawan dalam ekosistem aplikasi *e-commerce* berskala besar.

Meski data yang bocor tergolong data pribadi dasar, dampak yang ditimbulkan tidak bisa dianggap sepele. Jenis data seperti ini rentan digunakan untuk serangan lanjutan, seperti *credential stuffing*, yaitu upaya masuk ke akun pengguna di platform lain dengan menggunakan kombinasi email dan *password* yang sama. Kerentanan ini semakin besar mengingat mayoritas pengguna internet cenderung menggunakan *password* serupa di berbagai layanan, sehingga meskipun *password* telah di-*hash*, risiko penyalahgunaan tetap signifikan.

Temuan ini diperkuat oleh analisis Nuranisa dan Lukitasari (2024), yang menyatakan bahwa pencurian data pada platform *e-commerce* umumnya melibatkan kombinasi teknik *phishing*, pembobolan database, serta eksploitasi celah autentikasi. Dalam konteks Tokopedia, posisinya sebagai salah satu platform *e-commerce* terbesar di Indonesia menjadikannya target yang sangat menarik bagi pelaku kejahatan siber, mengingat volume dan nilai data pengguna yang sangat tinggi.

Dampak langsung dari insiden ini tidak hanya bersifat teknis, tetapi juga psikologis dan reputasional. Kepercayaan publik terhadap keamanan platform mengalami penurunan tajam, ditandai dengan meningkatnya kekhawatiran pengguna akan potensi penyalahgunaan data pribadi mereka. Sentimen negatif yang tersebar luas di media sosial, ditambah dengan pemberitaan masif di berbagai media massa, turut memperbesar skala kepanikan publik. Meskipun faktanya sebagian besar data yang bocor tidak mencakup informasi finansial sensitif seperti nomor kartu kredit, persepsi keamanan yang terganggu ini memiliki implikasi jangka panjang terhadap loyalitas pengguna dan citra perusahaan secara keseluruhan.

Analisis Langkah-Langkah Penanganan Insiden

Respons awal Tokopedia terhadap insiden kebocoran data menuai berbagai kritik, terutama terkait pendekatan komunikasi yang dinilai kurang memadai. Rahmania et al. (2020) dan Roos et al. (2020) mencatat bahwa sikap perusahaan pada fase awal cenderung defensif, di mana Tokopedia membantah adanya kebocoran data sensitif dan menegaskan bahwa password pengguna tetap aman karena telah terenkripsi. Narasi ini justru memicu persepsi ambigu di kalangan publik, terutama ketika bukti-bukti kebocoran mulai beredar luas di forum peretas. Meskipun perusahaan kemudian mengambil langkah dengan memberlakukan *reset password* secara paksa kepada seluruh pengguna, banyak pihak menilai bahwa langkah tersebut dilakukan tanpa disertai penjelasan yang memadai, sehingga menimbulkan kesan kurang transparan.

Dari sisi teknis, Afip et al. (2025) mengakui bahwa Tokopedia telah melakukan sejumlah tindakan responsif pasca-insiden, seperti pembaruan sistem autentikasi, pengetatan enkripsi data, serta pemutakhiran infrastruktur *firewall*. Namun, implementasi langkah-langkah teknis ini tidak diimbangi dengan komunikasi publik yang jelas dan terperinci. Keterbatasan informasi yang disampaikan kepada pengguna menciptakan kesenjangan antara tindakan nyata yang telah dilakukan perusahaan dengan ekspektasi masyarakat yang menginginkan penjelasan menyeluruh mengenai akar masalah, proses penanganan, serta jaminan keamanan di masa mendatang.

Fachrudin et al. (2024) menjelaskan bahwa manajemen keamanan yang baik harus memiliki empat elemen penting: pencegahan, deteksi, respons cepat, dan pemulihan. Jika kerangka ini diterapkan pada kasus Tokopedia, terlihat jelas bahwa langkah pencegahan mereka masih lemah. Masalah utamanya adalah tidak adanya sistem deteksi dini dan monitoring yang berjalan secara terus-menerus, sehingga celah keamanan baru diketahui setelah dimanfaatkan oleh peretas. Hal serupa juga diungkapkan oleh Paramita et al. (2022) yang menggunakan standar *ISO 27001* untuk mengevaluasi keamanan data. Mereka menekankan bahwa keamanan data yang efektif membutuhkan audit rutin dan pengukuran tingkat keamanan secara berkala. Dalam kasus Tokopedia, penilaian risiko dan monitoring berkelanjutan tampaknya belum berjalan dengan baik.

Dari sisi hukum, Fathur (2020) menyatakan bahwa Tokopedia sebenarnya memiliki tanggung jawab moral untuk melindungi data pengguna, meskipun saat itu Undang-Undang Perlindungan Data Pribadi (UU PDP) belum berlaku. Menurut Anindya dan Subiyanto (2025), UU PDP mewajibkan platform digital untuk melakukan beberapa hal penting: melaporkan insiden secara formal, memberitahu pengguna yang terdampak, dan melakukan audit keamanan secara berkala. Jika standar UU PDP diterapkan pada kasus tahun 2020, beberapa langkah yang diambil Tokopedia belum memenuhi persyaratan yang seharusnya. Kekurangan paling nyata terlihat pada kurangnya pemberitahuan resmi kepada pengguna yang datanya bocor, serta minimnya transparansi dalam menjelaskan bagaimana kebocoran tersebut bisa terjadi.

Jika dilihat secara menyeluruh, penanganan insiden kebocoran data Tokopedia memiliki beberapa kelemahan di berbagai aspek. Dari sisi teknis, meskipun ada upaya perbaikan sistem, tidak ada bukti bahwa Tokopedia melakukan audit eksternal yang hasilnya dipublikasikan kepada masyarakat (Paramita et al., 2022). Dari sisi komunikasi, cara perusahaan menyampaikan informasi dinilai kurang terbuka dan cenderung tertutup, sehingga justru menurunkan kepercayaan publik (Rahmania et al., 2020; Roos et al., 2020). Dari sisi hukum, kewajiban untuk memberitahu pengguna yang terdampak dan melaporkan insiden secara formal belum dilakukan dengan baik (Anindya & Subiyanto, 2025). Dari sisi manajemen risiko, pengelolaan risiko keamanan belum sepenuhnya mengikuti standar praktik terbaik seperti *ISO 27001* (Paramita et al., 2022).

Dampak Insiden terhadap Kepercayaan Publik

Rahmania et al. (2020) menemukan bahwa berita kebocoran data yang terus-menerus muncul di media berpengaruh besar terhadap kepercayaan pengguna Tokopedia. Informasi yang beredar secara masif di media sosial membuat persepsi risiko semakin tinggi, meskipun sebenarnya dampak langsung terhadap akun keuangan pengguna relatif kecil. Temuan ini

diperkuat oleh penelitian Roos et al. (2020), yang menunjukkan bahwa opini negatif yang menyebar melalui komentar di *Twitter* dan forum digital semakin memperburuk citra Tokopedia. Masalahnya, komentar dan keluhan negatif menyebar jauh lebih cepat dibandingkan klarifikasi resmi dari perusahaan.

Sihombing et al. (2023) menjelaskan bahwa kerusakan reputasi akibat kebocoran data bersifat jangka panjang. Meskipun Tokopedia berhasil memperbaiki layanan dan meningkatkan sistem keamanan, kepercayaan konsumen tidak langsung pulih dalam waktu singkat. Bahkan, banyak pengguna yang memilih mengurangi aktivitas transaksi mereka selama beberapa minggu hingga bulan setelah insiden terjadi. Dari berbagai penelitian tersebut, dapat disimpulkan bahwa keamanan data bukan sekadar masalah teknis, tetapi juga masalah psikologis dan reputasi.

Penelitian Saputra et al. (2025), yang menganalisis keamanan aplikasi DANA, menunjukkan bahwa platform digital yang memiliki sistem manajemen sekuriti yang lebih proaktif dapat mempertahankan kepercayaan publik meskipun terjadi insiden kecil. Perbandingan ini menunjukkan bahwa strategi komunikasi keamanan berperan penting dalam menjaga loyalitas pengguna. Tokopedia, dalam kasus ini, dinilai lambat dalam membangun narasi perlindungan, menunjukkan peningkatan keamanan secara terlihat, dan memberikan edukasi kepada pengguna tentang risiko pasca-insiden.

Jika seluruh temuan jurnal disintesiskan, maka faktor-faktor utama penurunan kepercayaan publik adalah:

1. Besarnya skala kebocoran - 91 juta akun membuat insiden ini dikategorikan *massive breach*, sehingga memicu kepanikan publik (Afip et al., 2025)
2. Minimnya transparansi awal dari Tokopedia - pengguna membutuhkan kejelasan, bukan pernyataan normatif, ketidakjelasan respons membuat publik berasumsi negatif (Rahmania et al., 2020)
3. Amplifikasi risiko melalui media dan *electronic word of mouth* - berita dan komentar negatif memperburuk persepsi risiko (Roos et al., 2020)
4. Tidak terlihatnya langkah keamanan baru secara langsung - peningkatan keamanan banyak dilakukan di sisi server, sehingga tidak terlihat oleh pengguna (Sihombing et al., 2023)
5. Penilaian bisnis dan hukum tentang tanggung jawab data - UU PDP semakin memperkuat persepsi bahwa platform wajib bertanggung jawab penuh atas keamanan data (Anindya & Subiyanto, 2025).

Jika dilihat dari perspektif manajemen risiko berbasis *ISO 27001* (Paramita et al., 2022), Tokopedia hanya memenuhi sebagian siklus keamanan yaitu respons dan pemulihan, tetapi lemah pada aspek deteksi dan pencegahan. Untuk memulihkan citra perusahaan setelah insiden seperti ini, diperlukan tiga hal penting: transparansi dalam menjelaskan apa yang terjadi dan bagaimana masalah ditangani, konsistensi komunikasi publik yang jelas dan berkelanjutan, serta peningkatan fitur keamanan yang terlihat seperti penggunaan OTP, notifikasi login dari perangkat baru, dan autentikasi dua faktor, sehingga pengguna merasakan langsung adanya perbaikan.

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu

No.	Judul dan Penulis	Persamaan	Perbedaan
1.	Pengaruh Terpaan Berita Tentang Kebocoran Data Pengguna Tokopedia dan Aktivitas *Word of Mouth* Terhadap Tingkat Kepercayaan Dalam Menggunakan Tokopedia	Sama-sama membahas dampak kebocoran data Tokopedia terhadap persepsi dan kepercayaan pengguna.	Fokus pada pengaruh terpaan berita dan *word of mouth* secara kuantitatif, sedangkan penelitian ini menggunakan pendekatan SLR yang lebih komprehensif.

	(Rahmania, Pradekso, & Ayun, 2021)		
2.	Pengaruh Terpaan Berita Kebocoran Data Pengguna Tokopedia dan Terpaan *E-Word of Mouth* Terhadap Citra Tokopedia (Roos, Setyabudi, & Gono, 2021)	Sama-sama mengkaji dampak insiden kebocoran data Tokopedia terhadap persepsi publik.	Fokus pada citra perusahaan melalui analisis terpaan berita dan *e-WoM*, sedangkan penelitian ini menganalisis penanganan insiden dan kepercayaan publik secara menyeluruh.
3.	TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN (Fathur, 2022)	Sama-sama membahas kasus kebocoran data Tokopedia dan aspek tanggung jawab perusahaan.	Fokus pada aspek yuridis dan tanggung jawab hukum, sedangkan penelitian ini lebih luas mencakup manajemen keamanan dan komunikasi krisis.
4	ANALISIS DAMPAK KEJAHATAN SIBER TERHADAP KEPERCAYAAN KONSUMEN DALAM BERBELANJA DI TOKOPEDIA (Sihombing et al., 2023)	Sama-sama menganalisis dampak kebocoran data terhadap kepercayaan konsumen Tokopedia.	Menggunakan metode kuantitatif dengan kuesioner, sedangkan penelitian ini menggunakan *systematic literature review* untuk analisis yang lebih komprehensif.
5.	Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi (Anindya & Subiyanto, 2025)	Sama-sama membahas kasus kebocoran data Tokopedia dan kewajiban perlindungan data.	Fokus pada analisis yuridis berdasarkan UU PDP, sedangkan penelitian ini mengintegrasikan aspek teknis, komunikasi, dan manajemen keamanan.
6.	ANALISIS INSIDEN KEBOCORAN DATA 91 JUTA AKUN TOKOPEDIA: DAMPAK DAN UPAYA PENANGANANNYA (Afip, Andy, Ciayu, & Delia, 2025)	Sama-sama menganalisis kronologi insiden, dampak, dan upaya penanganan kebocoran data Tokopedia.	Fokus pada evaluasi teknis berdasarkan *CIA Triad* dan *ISO 27001*, sedangkan penelitian ini lebih komprehensif dengan menambahkan analisis komunikasi krisis dan kepercayaan publik.
7.	Peranan Penting Manajemen Sekuriti di Era Digitalisasi (Fachrudin, Respaty, Adilah, & Sinlae, 2024)	Sama-sama membahas pentingnya manajemen keamanan informasi di era digital.	Bersifat konseptual umum tentang manajemen sekuriti, sedangkan penelitian ini mengaplikasikan konsep tersebut pada studi kasus spesifik Tokopedia.
8.	Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Data Pengguna Pada Aplikasi Dana (Saputra, Satriawan, & Saputra, 2025)	Sama-sama membahas penerapan manajemen sekuriti untuk melindungi data pengguna pada aplikasi digital.	Fokus pada aplikasi Dana dengan strategi preventif, sedangkan penelitian ini menganalisis kasus kebocoran pada Tokopedia dengan evaluasi *incident response*.
9.	Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) *ISO 27001:2013* (Paramita et al., 2022)	Sama-sama menggunakan standar *ISO 27001* sebagai framework evaluasi keamanan informasi.	Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) *ISO 27001:2013*
10.	Tindak Pidana Pencurian	Sama-sama menganalisis	Fokus pada aspek hukum

Data Dan Privasi Pengguna Dalam Transaksi *E-Commerce* (Studi Kasus Pada Aplikasi Tokopedia) (Nuranisa & Lukitasari, 2024)	kasus kebocoran data Tokopedia dari perspektif hukum dan tanggung jawab perusahaan.	pidana dan pertanggungjawaban korporasi, sedangkan penelitian ini mengintegrasikan aspek teknis manajemen keamanan, komunikasi krisis, dan dampak kepercayaan publik secara holistik.

KESIMPULAN

Insiden kebocoran data Tokopedia tahun 2020 yang mengekspos 91 juta akun pengguna menunjukkan kelemahan serius dalam manajemen keamanan informasi platform *e-commerce* Indonesia. Penelitian ini menemukan bahwa penanganan insiden oleh Tokopedia memiliki kelemahan mendasar di berbagai aspek. Dari sisi teknis, perusahaan belum menerapkan siklus keamanan ideal berdasarkan standar *ISO 27001*, khususnya pada aspek pencegahan dan deteksi dini, sehingga kebocoran baru terdeteksi setelah data dijual di forum peretas. Meskipun dilakukan perbaikan teknis seperti pembaruan autentikasi dan pengetatan enkripsi, implementasinya tidak disertai transparansi dan komunikasi yang memadai.

Respons komunikasi krisis Tokopedia cenderung defensif dan minim transparansi dalam menjelaskan kronologi, akar masalah, dan langkah penanganan, menciptakan kesenjangan antara tindakan nyata dengan ekspektasi publik yang diperparah oleh amplifikasi sentimen negatif di media sosial. Dampak terhadap kepercayaan publik bersifat *multidimensional*: secara psikologis terjadi peningkatan persepsi risiko, secara reputasional citra Tokopedia menurun dengan berkurangnya intensitas transaksi, namun sebagian besar pengguna tetap menggunakan platform karena minimnya pengetahuan tentang risiko aktual, kualitas layanan yang memadai, dan keterbatasan alternatif.

Evaluasi hukum menunjukkan penanganan belum memenuhi prinsip perlindungan data yang seharusnya, khususnya dalam pemberitahuan formal dan audit eksternal. Penelitian ini menegaskan bahwa pemulihan kepercayaan publik memerlukan transparansi komunikasi krisis, implementasi fitur keamanan yang terlihat pengguna (seperti autentikasi dua faktor dan notifikasi *login*), edukasi proaktif, serta komitmen berkelanjutan terhadap standar keamanan internasional, sehingga platform *e-commerce* perlu mengadopsi kerangka manajemen keamanan yang proaktif dan terintegrasi mencakup aspek teknis, komunikasi, *legal compliance*, dan manajemen reputasi.

REFERENSI

Rahmania, T., Pradekso, T., & Ayun, P. Q. (2021). *Pengaruh Terpaan Berita Tentang Kebocoran Data Pengguna Tokopedia dan Aktivitas Word of Mouth Terhadap Tingkat Kepercayaan Dalam Menggunakan Tokopedia*. *Interaksi Online*, 9(2), 161-169.

Roos, A. B. E., Setyabudi, D., & Gono, J. N. S. (2021). *Pengaruh Terpaan Berita Kebocoran Data Pengguna Tokopedia dan Terpaan E-Word of Mouth Terhadap Citra Tokopedia*. *Interaksi Online*, 9(2), 33-39.

Fathur, M. (2020, November). *Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen*. *In National Conference on Law Studies* (NCOLS) (Vol. 2, No. 1, pp. 43-60).

Sihombing, G. P., Hamzah, H. A., Tian, C., Lianda, T. A. C., Daniswara, M. D., & Saputra, M. N. (2023). *Analisis Dampak Kejahatan Siber Terhadap Kepercayaan Konsumen Dalam Berbelanja Di Tokopedia*. *Jurnal Ekonomika dan Manajemen*, 12(2), 110-120.

Anindya, R. P., & Subiyanto, A. E. (2025). *Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi*. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 1105-1112.

Afip, A., & Ciayu Pahlawati, S. (2025). *Analisis insiden kebocoran data 91 juta akun Tokopedia: Dampak dan upaya penanganannya*. *Integrative Perspectives of Social and Science Journal*, 2(03 Juli), 4858-4865.

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). *Peranan Penting Manajemen Sekuriti di Era Digitalisasi*. *Nusantara Journal of Multidisciplinary Science*, 2(1), 94-102.

Saputra, F., Satriawan, N., & Saputra, R. (2025). *Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Data Pengguna Pada Aplikasi Dana*. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(3), 142-154.

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). *Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi* (KAMI) ISO 27001: 2013. *Bulletin of Information Technology* (BIT), 3(4), 374-379.

Nuranisa, A. (2024). *Tindak Pidana Pencurian Data dan Privasi Pengguna dalam Transaksi E-Commerce (Studi Kasus pada Aplikasi Tokopedia)*.