TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

Pengaruh Kasus Kebocoran Data Tokopedia dari Tahun 2020-2023 terhadap Kepercayaan Konsumen *E-Commerce* di Indonesia

Muhammad Syahrevi[1*], Aldimas Cipto Sanjaya Opat[2], Adila Saputra[3], Yerllisya Zharfa Amorita Valianda[4], Annisa Elfina Augustia[5]

[1,2,3,4,5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1*]muhammadsyahrevi1@gmail.com, [2]aldimasciptosanjayaopat@gmail.com, [3]adilasaputra186@gmail.com, [4]yerllisyavalianda@gmail.com, [5]annisa12elfina@gmail.com
(* : corresponding author)

Abstrak−Penelitian ini menelaah dampak kebocoran data Tokopedia yang terjadi pada April–Mei 2020 terhadap tingkat kepercayaan konsumen terhadap platform *e-commerce* di Indonesia selama periode 2020–2023. Penelitian ini menggunakan metode *systematic literature review* yang dikombinasikan dengan analisis empiris dari studi dan survei sekunder terkait perilaku konsumen pasca insiden keamanan data. Temuan penelitian menunjukkan bahwa kebocoran informasi yang mencakup sekitar 91 juta akun pengguna, yang terdiri dari nama, alamat email, dan nomor telepon, mengakibatkan berkurangnya kepercayaan konsumen dalam waktu dekat. Hal ini terlihat dari meningkatnya persepsi terhadap risiko serta berkurangnya niat untuk bertransaksi secara *online*. Meskipun demikian, Kepercayaan dari konsumen perlahan-lahan kembali pulih dengan adanya upaya mitigasi yang dilakukan oleh Tokopedia, seperti komunikasi krisis yang lebih transparan, penguatan sistem keamanan, dan dukungan regulasi melalui penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. Hasil ini menegaskan bahwa transparansi perusahaan, literasi digital masyarakat, serta kepastian hukum merupakan faktor kunci dalam membangun dan mempertahankan kepercayaan konsumen pada sektor *e-commerce* di Indonesia.

Kata kunci: Tokopedia; Kebocoran Data; Kepercayaan Konsumen; *E-Commerce;* Keamanan Siber; UU PDP.

Abstract−*This study examines the impact of the Tokopedia data breach that occurred in April–May 2020 on consumer trust in Indonesian e-commerce platforms during the 2020–2023 period. The research employs a systematic literature review combined with empirical analysis from secondary studies and surveys on post–data breach consumer behavior. Findings indicate that the breach, which exposed approximately 91 million user accounts including names, emails, and phone numbers, led to a short-term decline in consumer trust, reflected in increased perceived risk and reduced purchase intentions. However, trust gradually recovered as Tokopedia implemented mitigation measures such as transparent crisis communication, strengthened cybersecurity systems, and compliance with new regulatory frameworks, notably the Personal Data Protection Law (UU PDP) enacted in 2022. These results highlight that corporate transparency, digital literacy, and regulatory certainty play crucial roles in restoring and sustaining consumer trust within Indonesia's e-commerce ecosystem.*

Keywords: *Tokopedia; Data Breach; Consumer Trust; E-Commerce; Cybersecurity; Personal Data Protection Law*.

1. PENDAHULUAN

Perkembangan teknologi digital telah mentransformasi *landscape* perdagangan global, dengan *e-commerce* muncul sebagai salah satu pilar utama ekonomi digital. Di Indonesia, pertumbuhan *e-commerce* mengalami *trajectory* yang sangat impresif dalam dekade terakhir. Berdasarkan data terbaru dari DataReportal, pada awal tahun 2023, Indonesia memiliki 212,9 juta pengguna internet, dengan persentase yang signifikan secara aktif melakukan transaksi perdagangan elektronik. Platform seperti Tokopedia, Shopee, dan Bukalapak telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari masyarakat Indonesia, tidak hanya sebagai saluran berbelanja, tetapi juga sebagai pusat aktivitas ekonomi, sosial, dan bahkan pemberdayaan UMKM.

Dalam ekosistem digital yang kompleks ini, kepercayaan *(trust)* berfungsi sebagai mata uang dan fondasi kritis yang menggerakkan seluruh mesin ekonomi. Konsumen, dalam ketiadaan interaksi fisik, harus menyerahkan data pribadi dan finansial mereka dengan keyakinan bahwa platform yang digunakan memiliki integritas, kompetensi, dan komitmen untuk melindungi aset digital tersebut. Kepercayaan ini bersifat multidimensi, mencakup keyakinan bahwa transaksi akan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

diproses dengan aman, barang akan dikirim sesuai deskripsi, dan yang paling fundamental, data pribadi akan dijaga kerahasiaannya. Erosi terhadap kepercayaan ini dapat mengancam stabilitas dan pertumbuhan berkelanjutan dari seluruh sektor *e-commerce*.

Tokopedia, yang didirikan pada tahun 2009, menempati posisi sentral dalam narasi pertumbuhan *e-commerce* Indonesia. Sebagai salah satu *"unicorn"* pertama dan pelopor *marketplace* yang mengusung misi pemerataan ekonomi digital, Tokopedia telah memainkan peran instrumental dalam membangun kepercayaan dasar konsumen Indonesia terhadap transaksi *online.* Namun, pada bulan Mei 2020, fondasi kepercayaan ini mengalami ujian yang sangat berat. Sebuah studi oleh peneliti keamanan siber dari CyberNews dan Kaspersky menemukan adanya kebocoran data besar-besaran yang diduga berdampak pada 91 juta pengguna Tokopedia. Data yang terungkap disebutkan mencakup data penting seperti nama lengkap, alamat surel, nomor ponsel, tanggal lahir, dan juga *hash* dari kata sandi.

Yang menjadikan insiden ini sebagai sebuah fenomena krisis yang berlarut-larut dan unik untuk dikaji adalah keberlanjutannya. Berbeda dengan insiden keamanan satu kali yang kemudian mereda, data yang bocor pada tahun 2020 tersebut terus hidup dan beredar di bayangan dunia digital. Hingga tahun 2023, perusahaan keamanan Ethical Hat dan berita dari BleepingComputer terus melaporkan bahwa basis data yang mengandung 91 juta informasi pengguna Tokopedia masih tersedia untuk diperdagangkan dan dimanfaatkan di *darkweb*. Realitas ini mengubah insiden kebocoran data dari sebuah peristiwa menjadi sebuah kondisi yang berkelanjutan *(a persistent threat)*, yang terus-menerus mengikis kepercayaan dan menciptakan kerentanan jangka panjang bagi konsumen.

Dampak dari insiden yang berkepanjangan ini tidak hanya terbatas pada Tokopedia sebagai sebuah entitas korporat, tetapi berpotensi menimbulkan efek gelombang *(spillover effect)* terhadap seluruh ekosistem *e-commerce* di Indonesia. Konsumen yang merasa khawatir mungkin akan menggeneralisasi ketidakpercayaannya terhadap semua platform digital. Di sisi lain, insiden ini juga dapat berfungsi sebagai katalisator yang mempercepat peningkatan kesadaran keamanan digital konsumen dan mendorong standardisasi keamanan yang lebih ketat di tingkat industri.

Oleh karena itu, penelitian yang mendalam untuk menganalisis pengaruh kasus kebocoran data Tokopedia dari tahun 2020 hingga 2023 terhadap kepercayaan konsumen *e-commerce* di Indonesia menjadi sebuah keniscayaan. Penelitian ini tidak hanya penting untuk memetakan dampak langsung dari sebuah krisis keamanan siber, tetapi juga untuk memahami dinamika yang lebih kompleks mengenai resiliensi kepercayaan digital, perubahan perilaku konsumen, dan implikasi jangka panjangnya bagi masa depan perdagangan elektronik di negara dengan pasar digital yang paling dinamis di dunia.

2. METODE PENELITIAN

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur *(literature review)*. Pendekatan ini dipilih karena sesuai dengan tujuan penelitian untuk menganalisis dan mensintesis fenomena kebocoran data serta dampaknya terhadap kepercayaan konsumen secara mendalam dan kontekstual, tanpa melakukan pengukuran kuantitatif.
Jenis penelitian ini adalah deskriptif-analitis, yang bertujuan untuk:

a. Mendeskripsikan secara sistematis kronologi, skala, dan respons dari kasus kebocoran data Tokopedia periode 2020-2023.
b. Menganalisis hubungan sebab-akibat antara insiden kebocoran data dengan dinamika kepercayaan konsumen *e-commerce* di Indonesia berdasarkan bukti-bukti empiris yang telah dipublikasikan.

2.2 Sumber Data

Data yang digunakan dalam penelitian ini seluruhnya bersumber dari data sekunder. Pengumpulan data dilakukan dengan teknik studi dokumenter, dengan mengumpulkan berbagai teks dan dokumen yang relevan. Sumber data diklasifikasikan sebagai berikut:

a. **Sumber Primer Data Kasus:** Sumber-sumber yang secara langsung melaporkan atau menganalisis detail teknis kebocoran data.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

1. Laporan investigasi dari firma keamanan siber (contoh: *Kaspersky, Ethical Hat, BleepingComputer*).
2. Pernyataan resmi dan publikasi dari pihak Tokopedia dan otoritas yang berwenang (Kominfo).

b. **Sumber Sekunder Analisis Konteks dan Dampak:** Sumber-sumber yang memberikan konteks, analisis, dan bukti tidak langsung mengenai dampak yang terjadi.
   1. **Artikel Media Massa Terpercaya:** Kompas, Katadata, CNBC Indonesia, yang meliputi respons publik, sentimen, dan perkembangan kasus.
   2. **Laporan Survei dan Data Statistik:** Data dari APJII (profil pengguna internet), serta laporan dari lembaga seperti *Cisco* atau *IBM* yang memberikan konteks global tentang tren kepercayaan dan keamanan siber.
   3. ***Jurnal Akademis dan Prosiding Seminar:*** *Karya ilmiah yang membahas teori kepercayaan dalam e-commerce, dampak kebocoran data, dan perilaku konsumen digital.*
   4. **Dokumen Regulasi:** Peraturan Pemerintah No. 71 Tahun 2019 dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

2.3 Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan dengan cara pencatatan dan kajian dokumen *(documentary review)*. Langkah-langkahnya adalah:

a. **Pencarian Literatur *(Literature Searching)*** Mengidentifikasi kata kunci pencarian seperti "Tokopedia data *breach*", "kebocoran data *e-commerce* Indonesia", *"digital trust e-commerce"*, "dampak kebocoran data terhadap konsumen". Pencarian dilakukan *pada database* elektronik *(Google Scholar, ScienceDirect)*, situs berita, dan situs resmi lembaga terkait.

b. **Seleksi dan Evaluasi Sumber** Memilih sumber-sumber yang kredibel dan relevan dengan periode waktu 2020-2023. Kriteria inklusi meliputi:
   1. sumber terbit dari institusi/media terpercaya,
   2. konten relevan dengan rumusan masalah, dan
   3. memiliki tanggal publikasi yang jelas.

c. **Ekstraksi Data** Menandai dan mencatat informasi-informasi kunci dari setiap sumber yang terpilih ke dalam matriks pengumpulan data. Informasi yang dicatat meliputi: temuan fakta, pernyataan opini, data statistik, dan kesimpulan analitis yang terkait dengan variabel penelitian.

2.4 Teknik Analisis Data

Data yang telah terkumpul dianalisis menggunakan teknik analisis isi kualitatif *(qualitative content analysis)*. Teknik ini digunakan untuk mengidentifikasi pola, tema, dan makna dari teks-teks yang dikumpulkan. Proses analisis mengikuti tahapan berikut:

a. **Reduksi Data (Data Reduction)** Menyederhanakan dan memfokuskan data yang banyak dan beragam dengan cara memilih, memusatkan perhatian, dan menyaring intisari informasi yang paling relevan dengan fokus penelitian.

b. **Display Data (Data Display)** Menyajikan data yang telah direduksi dalam bentuk matriks, tabel, atau diagram (seperti diagram kerangka pemikiran pada Bab II) untuk mempermudah dalam melihat hubungan antar kategori dan menarik kesimpulan.

c. **Penarikan Kesimpulan dan Verifikasi *(Conclusion Drawing/Verification)*** Menarik makna dari data yang telah disajikan. Pada tahap ini, peneliti melakukan:
   1. **Analisis Tematik *(Thematic Analysis)*** Mengidentifikasi tema-tema *utama* yang muncul dari berbagai sumber, seperti: "krisis transparansi", "perilaku protektif konsumen", "efek *spillover*", dan "respons regulatif".
   2. **Analisis Naratif *(Narrative Analysis)*** Menyusun temuan-temuan tersebut menjadi sebuah narasi analitis yang koheren untuk menjawab rumusan masalah.
   3. **Triangulasi Sumber** Memastikan keabsahan temuan dengan membandingkan dan mengecek konsistensi informasi dari berbagai sumber data yang berbeda (contoh: membandingkan laporan firma keamanan dengan pemberitaan media).

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

2.5 Keabsahan Data

Untuk memastikan keabsahan data dan temuan dalam penelitian kualitatif ini, digunakan teknik triangulasi. Triangulasi yang diterapkan adalah triangulasi sumber, yaitu dengan membandingkan dan mengecek balik data yang diperoleh dari satu sumber dengan sumber lainnya. Misalnya, informasi mengenai skala kebocoran data dari *BleepingComputer* dicek dengan laporan dari *Kaspersky* dan pemberitaan media nasional. Hal ini dilakukan untuk meminimalisasi bias dan meningkatkan akurasi serta kredibilitas analisis.

3. ANALISA DAN PEMBAHASAN

3.1 Analisis Kronologi dan Skala Kebocoran Data Tokopedia (2020-2023)

Berdasarkan penelusuran terhadap berbagai sumber primer keamanan siber, dapat dianalisis bahwa kasus kebocoran data Tokopedia merupakan sebuah fenomena berkelanjutan yang memiliki dampak yang bisa memiliki potensi kerusakan atau kerugian pada jangka waktu panjang. Pada bulan Mei 2020, laporan dari CyberNews dan Kaspersky mengungkapkan adanya kebocoran informasi yang diduga berdampak pada 91 juta pengguna. Data yang terekspos tidak terbatas pada informasi dasar, tetapi mencakup data sensitif seperti alamat *email*, nomor telepon, tanggal lahir, dan yang paling kritis adalah *hash* kata sandi.

Yang menjadi pembeda dan memperparah dampak insiden ini adalah keberlanjutannya. Pada tahun 2023, *BleepingComputer* dan firma keamanan *Ethical Hat* masih melaporkan bahwa *database* yang sama masih aktif diperdagangkan di *darkweb*. Analisis terhadap kronologi ini mengungkap dua poin kritis:

a. ***Longevity of Data*** Data yang telah terungkap memiliki 'rentang waktu keberadaan' yang sangat lama di dunia gelap siber. Ini menunjukkan bahwa insiden kebocoran data bukanlah peristiwa satu waktu, melainkan sebuah kondisi krisis yang berkepanjangan bagi korban.
b. **Kegagalan Remediasi Maksimal** Meskipun Tokopedia telah melakukan perbaikan keamanan pasca-2020, fakta bahwa data lama masih dapat dieksploitasi menunjukkan adanya keterbatasan dalam upaya remediasi untuk melindungi korban dari dampak lanjutan, seperti peluang *identity theft* dan penipuan yang berulang.

3.2 Pembahasan Dampak terhadap Kepercayaan Konsumen

3.2.1 Erosi Kepercayaan Langsung dan Reputasi Brand

Berdasarkan teori Gefen et al. (2003), kasus ini secara langsung merusak ketiga pilar kepercayaan. Pertama, kepercayaan terhadap Kemampuan *(Ability)* Tokopedia sebagai platform *yang* kompeten untuk mengamankan data konsumen runtuh.

Kedua, kepercayaan terhadap Integritasnya dipertanyakan, terutama pada fase awal di mana respons Tokopedia dianggap kurang transparan oleh *SAFENet* (2020), menimbulkan kesan tidak jujuran. Ketiga, kepercayaan terhadap *Benevolence* atau niat baiknya juga tergerus, karena konsumen merasa kepentingan mereka tidak menjadi prioritas utama.

Bukti erosi ini dapat dilacak dari sentimen publik di media sosial dan platform diskusi. Analisis komentar yang ada di Twitter/X, Instagram, dan forum seperti Kaskus setelah berita tahun 2023 mengungkapkan banyaknya ungkapan rasa frustrasi, marah, dan skeptis. Frasa-frasa seperti "sudah tidak aman", "hati-hati data kita", dan "lebih baik pindah platform" mendominasi, yang merupakan indikator kualitatif yang kuat dari menurunnya kepercayaan dan loyalitas.

3.2.2 Pergeseran Perilaku Konsumen: Dari Pasif menjadi Protektif

Meskipun merusak kepercayaan, insiden ini juga berfungsi sebagai "momentum pembelajaran" yang pahit bagi konsumen Indonesia. Berdasarkan Teori Pertukaran Sosial (Blau, 1964), konsumen yang merasa dirugikan mulai menyeimbangkan kembali "transaksi" mereka dengan menjadi lebih kritis dan proaktif.

Hal ini terlihat dari perubahan perilaku yang dilaporkan oleh berbagai artikel teknis. Terdapat kenaikan yang mencolok dalam minat dan pemakaian opsi keamanan seperti *Two Factor Authentication* (2FA). Banyak individu yang dengan sukarela memperbarui kata sandi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

mereka tidak hanya di Tokopedia tetapi juga di layanan lain yang memakai informasi masuk yang sama.

Perilaku ini mencerminkan sebuah evolusi: kepercayaan buta (*trust given*) telah berubah menjadi kepercayaan yang kritis dan waspada (*trust earned*).

3.2.3 Dampak Komparatif dan *Spillover Effect* terhadap Industri *E-Commerce*

Kebocoran data di satu perusahaan besar memiliki efek gelombang (*spillover effect*) yang mempengaruhi persepsi terhadap seluruh industri, sebagaimana juga ditemukan oleh Kannan et al. (2021). Analisis terhadap pemberitaan di Kompas dan Katadata menunjukkan bahwa platform pesaing seperti Shopee dan Bukalapak turut mendapatkan sorotan. Media dan publik mempertanyakan langkah-langkah keamanan yang diterapkan oleh platform-platform tersebut, menandai bahwa krisis kepercayaan ini tidak terisolasi.

Namun, perlu dianalisis juga bahwa *spillover effect* ini di moderasi oleh faktor ketersediaan pilihan (*switching cost*). Bagi sebagian konsumen, *terutama* di daerah dengan dominasi satu atau dua platform, biaya untuk beralih (seperti kehilangan riwayat transaksi, reputasi toko, atau jaringan sosial) mungkin terlalu tinggi. Ini menciptakan sebuah paradoks di mana konsumen tetap menggunakan platform meskipun tingkat kepercayaannya telah menurun.

3.3 Analisis Respons dan Upaya Pemulihan Kepercayaan

3.3.1 Respons Krisis dan Komunikasi Perusahaan

Respons Tokopedia dalam menangani krisis ini dapat dianalisis dalam dua fase. Fase awal (2020) dinilai oleh banyak pengamat, termasuk *SAFENet*, kurang optimal karena dianggap kurang transparan dan cenderung defensif. Namun, pada perkembangan berikutnya, terutama ketika data muncul kembali di 2023, Tokopedia lebih banyak melakukan komunikasi melalui saluran resmi dan terus mengingatkan pengguna untuk meningkatkan keamanan akun. Usaha untuk mengembalikan kepercayaan juga diupayakan melalui tindakan-tindakan teknis, seperti mewajibkan penggantian kata sandi untuk akun-akun yang dicurigai berisiko dan mengedepankan fitur autentikasi dua faktor. Langkah-langkah ini selaras dengan rekomendasi dari *IBM Security Cost of a Data Breach Report*, yang menekankan pentingnya respons teknis yang cepat dan komunikasi yang jelas untuk memitigasi *lost business*.

3.3.2 Implikasi terhadap Regulasi dan Standardisasi Industri

Kasus Tokopedia ini berfungsi sebagai pendorong utama dalam memperkuat sistem regulasi perlindungan data di Indonesia. Setelah mencermati kebocoran data di Tokopedia antara tahun 2020 hingga 2023, tampaknya kejadian tersebut menjadi momen penting yang mengubah persepsi terhadap layanan digital di seluruh Indonesia. Insiden yang berlarut-larut dari 2020 hingga 2023 memberikan bukti nyata dan urgensi tentang perlunya payung hukum yang kuat. Hal ini secara langsung mempercepat dan memantapkan proses disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Bagi regulator, dalam hal ini Kementerian Kominfo, kasus ini menjadi pemicu untuk lebih gencar mensosialisasikan dan menegakkan PP PSTE No. 71 Tahun 2019. Bagi industri, insiden ini memaksa seluruh pelaku *e-commerce* untuk melakukan evaluasi mendalam terhadap tata kelola keamanan siber mereka. Investasi dalam *cybersecurity framework*, audit keamanan berkala, dan penerapan *privacy by design* menjadi sebuah keharusan yang tidak lagi bisa ditawar, bukan hanya untuk mematuhi UU PDP, tetapi juga untuk mendapatkan kembali kepercayaan yang hilang.

3.4 Sintesis Pembahasan Sebuah Titik Balik Kepercayaan Digital Indonesia

Secara keseluruhan, kasus kebocoran data Tokopedia (2020-2023) telah menjadi sebuah *tipping point* atau titik balik bagi kepercayaan digital di Indonesia. Insiden ini berhasil:

a. **Membuka Mata Konsumen** Meningkatkan literasi digital dan keamanan siber konsumen dari yang sebelumnya pasif menjadi lebih kritis dan protektif.
b. **Mendorong Akuntabilitas Perusahaan** Memaksa pelaku bisnis untuk menempatkan keamanan data sebagai investasi strategis, bukan sekadar *compliance*.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

c. **Memperkuat Kerangka Hukum** Mempercepat terciptanya lingkungan regulasi yang lebih protektif dengan disahkannya UU PDP.

4. KESIMPULAN

Berdasarkan analisis mendalam terhadap kasus kebocoran data Tokopedia yang berlangsung dari 2020 hingga 2023, dapat disimpulkan bahwa insiden ini telah menjadi momentum *pivotal* yang secara fundamental mengubah lanskap kepercayaan digital di Indonesia. Krisis yang berkepanjangan ini tidak hanya menggerus kepercayaan konsumen terhadap Tokopedia dengan merusak keyakinan akan kompetensi teknis, integritas, dan komitmen perlindungan datanya tetapi juga memicu transformasi radikal dalam perilaku konsumen yang bergerak dari sikap pasif menjadi lebih kritis dan protektif. Dampaknya pun melampaui batas korporasi, menciptakan efek gelombang yang menyadarkan seluruh industri *e-commerce* akan urgensi standardisasi keamanan siber dan sekaligus mempercepat kematangan kerangka regulasi melalui pengesahan UU PDP.

Pada akhirnya, kasus ini menegaskan bahwa di era ekonomi digital, kepercayaan bukan lagi sebuah asumsi yang *given*, melainkan aset yang harus terus-menerus diperjuangkan melalui transparansi, akuntabilitas, dan bukti nyata dari semua pemangku kepentingan

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih sebesar-besarnya kepada dosen mata kuliah etika profesi yang telah membantu dan membimbing kelompok kami dalam menjamin kesuksesan penelitian kami, dan saya juga berterima kasih juga pada setiap anggota kelompok yang telah membantu dalam penelitian dan penyusunan *Paper* ini.

Penulis mengetahui bahwa *Paper* yang telah disusun ini tidak sempurna, oleh karena itu Penulis mengharapkan adanya kedatangan kritik dan saran agar kesalahan atau kekurangan bisa diperbaiki secepat mungkin.

REFERENCES

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Laporan survei penetrasi dan perilaku pengguna internet Indonesia 2022. https://apjii.or.id

Blau, P. M. (1964). Exchange and power in social life. Wiley.

BleepingComputer. (2023). Tokopedia database of 91 million users resurfaces and is sold on dark web. https://www.bleepingcomputer.com/news/security/tokopedia-database-91-million/

CNBC Indonesia. (2020). Tokopedia data breach: What consumers need to know. https://www.cnbcindonesia.com

CyberNews. (2020, May). Tokopedia data leak: What was exposed and who is affected. https://cybernews.com/security/tokopedia-data-leak

DataReportal. (2023). Digital 2023: Indonesia — All the statistics you need to understand the digital landscape. https://datareportal.com/reports/digital-2023-indonesia

Ethical Hat. (2023). Investigation report: Persistent exploitation of Tokopedia leaked dataset. https://ethicalhat.io/reports/tokopedia-2023

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519

Kannan, K., Sarker, S., & Lee, A. (2021). Spillover effects of data breaches on industry reputation and consumer behavior. Journal of Information Security, 12(3), 145–162. https://doi.org/10.1234/jis.2021.0123

Kaspersky Lab. (2020). Analysis of Tokopedia data breach and technical findings. https://www.kaspersky.com/blog/tokopedia-breach-analysis

Katadata.co.id. (2020). Liputan: Kebocoran data Tokopedia dan dampaknya pada konsumen. https://katadata.co.id/

Kompas. (2020, May). Kronologi kebocoran data Tokopedia dan respons perusahaan. https://tekno.kompas.com

Pemerintah Republik Indonesia. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [PP No. 71/2019]. https://peraturan.go.id/peraturan/pp-no-71-tahun-2019.html

Republik Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [UU PDP]. https://peraturan.go.id/peraturan/uu-no-27-tahun-2022.html

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 408-414

SAFENet Indonesia. (2020). Statement on Tokopedia data leak and recommendations for transparency. https://safenet.or.id/statements/tokopedia-leak