
LITERATUR REVIEW: PELANGGARAN ETIKA TEKNOLOGI INFORMASI KASUS KEBOCORAN DATA PADA MARKETPLACE DI INDONESIA

Oleh

Rizqi Saputri¹, Asmil Januar², Elkin Rilvani³

^{1,2,3}Universitas Pelita Bangsa

E-mail: ¹saputri.puput@gmail.com, ²asmil.januar26@gmail.com,

³elkin.rilvni@pelitabangsa.ac.id

Article History:

Received: 22-05-2026

Revised: 11-06-2026

Accepted: 25-06-2026

Keywords:

Etika Profesi Teknologi
Informasi, Kebocoran
Data

Abstract: Di tengah pesatnya transformasi digital, data telah menjadi sumber daya utama yang menopang berbagai sektor, mulai dari bisnis, layanan publik, hingga pemerintahan. Marketplace menjadi salah satu bentuk nyata dari transformasi digital ini, di mana interaksi antara penjual dan pembeli dilakukan sepenuhnya secara daring. Namun, kemudahan yang ditawarkan oleh marketplace sering kali diiringi dengan permasalahan hukum, terutama terkait dengan keamanan data pribadi pengguna (Aryanti, 2023). Kebocoran data pribadi yang melibatkan jutaan pengguna marketplace di Indonesia menunjukkan masih lemahnya perlindungan hukum terhadap privasi digital. Kasus kebocoran data Tokopedia pada tahun 2020, kebocoran sekitar 91 juta data pengguna Tokopedia pada tahun 2020. Informasi penting seperti nama lengkap, alamat email, nomor telepon, hingga password hash diretas dan dijual melalui dark web. Peretasan ini diperkirakan terjadi pada Maret 2020 dan baru terungkap beberapa bulan kemudian setelah data tersebut diperdagangkan di forum daring. Profesional TI berkewajiban untuk menjaga kerahasiaan informasi, memastikan integritas sistem, dan meminimalkan risiko yang dapat merugikan masyarakat. Prinsip-prinsip tersebut menekankan pentingnya tanggung jawab moral dan profesional dalam menangani data sensitif. Pelanggaran terhadap prinsip ini dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi, serta merusak kepercayaan publik terhadap layanan digital.

PENDAHULUAN

Perkembangan teknologi informasi di Indonesia mengalami pertumbuhan pesat, namun diikuti dengan berbagai kasus pelanggaran etika yang merugikan. Masyarakat kini beralih dari aktivitas ekonomi konvensional menuju sistem perdagangan elektronik yang lebih cepat dan efisien. Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai lebih dari 215 juta jiwa pada tahun 2023 (Sadya, 2023).

Pertumbuhan pesat ini membawa dampak positif dalam berbagai aspek kehidupan, namun juga menimbulkan permasalahan terkait etika penggunaan teknologi informasi. Etika

IT merujuk pada seperangkat prinsip moral yang mengatur penggunaan teknologi informasi secara bertanggung jawab, mencakup privasi, keamanan data, kejujuran, keadilan, dan tanggung jawab sosial.

Marketplace menjadi salah satu bentuk nyata dari transformasi digital ini, di mana interaksi antara penjual dan pembeli dilakukan sepenuhnya secara daring. Namun, kemudahan yang ditawarkan oleh marketplace sering kali diiringi dengan permasalahan hukum, terutama terkait dengan keamanan data pribadi pengguna (Ariyanti, 2023).

Isu keamanan siber menjadi semakin kompleks seiring meningkatnya volume dan nilai data yang dikumpulkan serta meningkatnya serangan siber yang bersifat semakin canggih dan terorganisir. Kebocoran data tidak lagi hanya menyebabkan gangguan teknis sementara, melainkan dapat berdampak sistemik terhadap reputasi, kepercayaan konsumen, serta keberlangsungan operasional perusahaan. Di Indonesia, kesadaran akan pentingnya keamanan data masih relatif rendah, baik di tingkat institusi maupun individu. Hal ini diperparah oleh keterbatasan regulasi yang mengikat secara tegas dalam melindungi data pribadi sebelum tahun 2022.

Kebocoran data pribadi yang melibatkan jutaan pengguna marketplace di Indonesia menunjukkan masih lemahnya perlindungan hukum terhadap privasi digital. Kasus kebocoran data Tokopedia pada tahun 2020, kebocoran sekitar 91 juta data pengguna Tokopedia pada tahun 2020. Informasi penting seperti nama lengkap, alamat email, nomor telepon, hingga password hash diretas dan dijual melalui dark web. Peretasan ini diperkirakan terjadi pada Maret 2020 dan baru terungkap beberapa bulan kemudian setelah data tersebut diperdagangkan di forum daring.

Insiden tersebut tidak hanya meresahkan pengguna karena risiko penyalahgunaan data pribadi, tetapi juga menimbulkan pertanyaan mengenai tanggung jawab etis penyelenggara sistem dalam menjaga keamanan platform digital yang mereka kelola. Pada saat insiden terjadi, Indonesia belum memiliki regulasi khusus yang mengatur perlindungan data pribadi secara komprehensif. Ketiadaan regulasi yang kuat menyebabkan posisi pengguna menjadi lemah dan menimbulkan tuntutan publik terhadap perlunya standar etika serta tata kelola keamanan yang lebih baik bagi perusahaan teknologi. Dalam konteks profesi TI, kasus Tokopedia menunjukkan perlunya penerapan prinsip etika yang ketat dalam pengelolaan sistem informasi dan data pengguna. Tanggung jawab hukum marketplace dalam melindungi data pribadi pengguna mencakup kewajiban untuk menjaga keamanan system dan memberikan pemberitahuan jika terjadi pelanggaran.

Lebih dari 91 juta data pengguna bocor dan dijual di forum online, mengungkap kelemahan praktik perlindungan data dan keamanan siber di perusahaan digital. Penelitian ini menganalisis pelanggaran etika profesi IT dalam kasus tersebut menggunakan pendekatan studi literatur kualitatif. Data dikumpulkan melalui dokumen resmi, berita kredibel, dan literatur ilmiah terkait etika IT dan keamanan data. Temuan menunjukkan pelanggaran prinsip kerahasiaan, tanggung jawab profesional, dan integritas dalam pengelolaan data pengguna.

Profesional TI berkewajiban untuk menjaga kerahasiaan informasi, memastikan integritas sistem, dan meminimalkan risiko yang dapat merugikan masyarakat. Prinsip-prinsip tersebut menekankan pentingnya tanggung jawab moral dan profesional dalam menangani data sensitif. Pelanggaran terhadap prinsip ini dapat menyebabkan kerugian

besar, baik bagi individu maupun organisasi, serta merusak kepercayaan publik terhadap layanan digital (Association for Computing Machinery, 2018).

RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan diatas, maka permasalahan yang dapat dirumuskan adalah Bagaimana bentuk pelanggaran etika teknologi informasi dalam kasus kebocoran data pada marketplace di Indonesia?

METODE PENELITIAN

Dalam kegiatan ini penulis mengambil beberapa hal yang dianggap penting yang dapat dijadikan sebagai acuan untuk penelitian selanjutnya. Metode yang digunakan merupakan studi literatur yang mencari database dari berbagai referensi, seperti jurnal penelitian, review jurnal, buku dan data-data yang berkaitan dengan kebocoran data dan etika profesi IT yang diterbitkan pada tahun 2020-2025. Pencarian literatur dilakukan dengan menggunakan mesin pencari google di internet dengan kata kunci: kebocoran data, pelanggaran etika profesi dan marketplace.

Data yang digunakan dalam penelitian ini dibagi menjadi dua kategori yaitu Sumber Primer melalui Laporan investigasi resmi (misalnya dari Kemenkominfo atau BSSN), teks regulasi (UU PDP, UU ITE), kode etik profesi TI (seperti ACM, IEEE, atau IPKIN), dan pernyataan resmi dari pihak *marketplace* yang mengalami kebocoran data. Dan Sumber Sekunder yang meliputi Artikel jurnal ilmiah nasional dan internasional, buku teks etika komputer/TI, tesis, tesis doctoral, serta artikel berita dari media massa digital yang kredibel mengenai kronologi kasus terkait.

Data dianalisis dalam penelitian ini menggunakan metode Analisis Isi (*Content Analysis*) atau Analisis Tematik (*Thematic Analysis*) yang mengacu pada model Miles dan Huberman yaitu Reduksi Data: Merangkum, memilih hal-hal pokok, dan memfokuskan data pada tema pelanggaran etika profesi TI dan kelalaian *marketplace*. Penyajian Data (*Data Display*): Menyajikan data dalam bentuk matriks ringkasan, tabel komparasi kasus, atau narasi hubungan logis antarteoris etika. dan Penarikan Kesimpulan (*Conclusion Drawing/Verification*): Menyimpulkan pola pelanggaran etika profesi yang terjadi dan merumuskan solusi mitigasinya berdasarkan tinjauan literatur.

Pada tahap pemodelan, algoritma regresi linear digunakan untuk menganalisis hubungan antara data historis dengan hasil penjualan, sehingga menghasilkan model yang mampu memprediksi nilai penjualan secara akurat. Metode ini memungkinkan identifikasi pola tersembunyi dalam data dan mendukung pengambilan keputusan berbasis fakta. Evaluasi model dilakukan untuk memastikan kinerja dan akurasi prediksi dengan mengacu pada metrik statistik yang relevan, seperti nilai *Mean Absolute Error* (MAE) atau *Root Mean Square Error* (RMSE).

TINJAUAN PUSTAKA

Perkembangan teknologi informasi di era digital telah membawa kemudahan dalam berbagai aspek kehidupan, mulai dari transaksi ekonomi, layanan publik, hingga aktivitas sosial. Namun, kemajuan tersebut juga menimbulkan tantangan serius terkait keamanan dan privasi data pribadi. Di Indonesia, penggunaan layanan digital semakin meningkat, sehingga potensi risiko kebocoran data menjadi semakin besar dan memerlukan perhatian khusus,

terutama dari perspektif etika dan profesionalisme bidang teknologi informasi (TI).

Badan Siber dan Sandi Negara (BSSN) melalui Lanskap Keamanan Siber Indonesia 2022 menyebutkan bahwa berdasarkan hasil assessment yang dilakukan pada tahun 2022 ditemukan sebanyak 1.950 celah keamanan dari 457 sistem elektronik pada berbagai aplikasi yang digunakan oleh masyarakat secara luas (Yusuf, Arianto, & Amanda, 2022). Berbagai kasus pelanggaran etika IT masih sering terjadi di Indonesia, mulai dari kebocoran data pribadi, penyalahgunaan informasi, hingga kejahatan siber. Beberapa kasus besar yang menarik perhatian publik antara lain kebocoran data 1,3 miliar penduduk Indonesia dari Pusat Data Nasional (PDN) pada tahun 2024, kebocoran data pengguna e-commerce dan aplikasi transportasi online, serta berbagai kasus penipuan online yang memanfaatkan kelemahan sistem keamanan digital.

Temuan ini sejalan dengan Yudha (2023) mendokumentasikan bagaimana penyedia layanan seperti Tokopedia memiliki tanggung jawab hukum eksplisit atas keamanan data transaksi pengguna. Pohan (2023) melengkapi temuan ini dengan menunjukkan bahwa mekanisme perlindungan hukum konsumen dalam platform digital masih memiliki celah yang signifikan, terutama ketika terjadi kebocoran data. Secara keseluruhan, pola yang muncul dari berbagai kasus tersebut menunjukkan adanya keterkaitan sistemik antara lemahnya standar etika profesi, ketidakmatangan regulasi, dan tingginya frekuensi insiden kebocoran data di Indonesia.

Indonesia belum memiliki regulasi khusus yang mengatur perlindungan data pribadi secara komprehensif. Ketidadaan regulasi yang kuat menyebabkan posisi pengguna menjadi lemah dan menimbulkan tuntutan publik terhadap perlunya standar etika serta tata kelola keamanan yang lebih baik bagi perusahaan teknologi. Dalam konteks profesi TI, kasus Tokopedia menunjukkan perlunya penerapan prinsip etika yang ketat dalam pengelolaan sistem informasi dan data pengguna.

Profesional TI berkewajiban untuk menjaga kerahasiaan informasi, memastikan integritas sistem, dan meminimalkan risiko yang dapat merugikan masyarakat. Prinsip-prinsip tersebut menekankan pentingnya tanggung jawab moral dan profesional dalam menangani data sensitif. Pelanggaran terhadap prinsip ini dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi, serta merusak kepercayaan publik terhadap layanan digital (Association for Computing Machinery, 2018).

Berdasarkan analisis terhadap kode etik profesi, teridentifikasi beberapa pelanggaran prinsip etika yang signifikan:

a. Pelanggaran Prinsip Kerahasiaan (Confidentiality) dan Privasi

Prinsip etika fundamental bagi profesional TI adalah menghormati privasi pengguna dan menjaga kerahasiaan informasi. Prinsip ini juga merupakan bagian inti dari triad keamanan data (*Confidentiality, Integrity, Availability*). Kebocoran 91 juta data pengguna merupakan bukti kegagalan penerapan prinsip ini. Data sensitif seperti nama lengkap, alamat email, nomor telepon, tanggal lahir dan jenis kelamin, serta password hash yang seharusnya dilindungi telah terekspos dan diperjual belikan. Ini menunjukkan bahwa profesional TI yang bertanggung jawab atas arsitektur dan pemeliharaan sistem di Tokopedia gagal mengimplementasikan mekanisme perlindungan yang memadai untuk menjaga kerahasiaan aset data pengguna.

Moricet al. (2024) dalam penelitiannya tentang perlindungan data pribadi dalam konteks

e-commerce menegaskan bahwa kelemahan sistem keamanan siber dan kurangnya implementasi standar privasi yang memadai menjadi faktor utama terjadinya pelanggaran data pribadi dalam skala besar. Lebih buruk lagi, setelah data awal bocor, lebih dari 200.000 password berhasil di-crack dan dibagikan gratis di forum hacker. Ini menunjukkan sistem enkripsi password tidak cukup kuat. Ditemukan bahwa kegagalan dalam menerapkan standar enkripsi yang memadai mencerminkan tidak hanya keterbatasan teknis, tetapi juga kurangnya kesadaran etis terhadap tanggung jawab perlindungan data pengguna (Fauzy & Hafizhah, 2023).

b. Pelanggaran Prinsip Tanggung Jawab Profesional (Responsibility)

Profesional TI memiliki tanggung jawab etis terhadap masyarakat untuk memastikan sistem yang mereka bangun dan kelola aman. Kegagalan dalam mencegah peretasan skala besar ini menunjukkan adanya kelalaian dalam memenuhi tanggung jawab tersebut. Aspek tanggung jawab yang dilanggar mencakup beberapa dimensi kritis. Pertama, dari aspek pencegahan, sistem keamanan tidak cukup tangguh untuk mendeteksi dan mencegah peretasan yang berlangsung dari Maret hingga Mei 2020, selama 2 bulan tanpa deteksi. Kedua, dari aspek deteksi, perusahaan baru mengetahui kebocoran setelah dilaporkan pihak eksternal (*Under the Breach*), bukan dari sistem monitoring internal. Ketiga, respons perusahaan dinilai publik kurang transparan. Tokopedia mengklaim password aman padahal faktanya 200.000 lebih password berhasil di-crack. Keempat, tidak ada notifikasi tertulis kepada pengguna yang terdampak sesuai PP No. 71/2019. Menteri Kominfo Johnny Plate harus memanggil Tokopedia untuk investigasi internal, menunjukkan kurangnya inisiatif proaktif dari perusahaan. Keterlambatan deteksi dan respons yang tidak memadai terhadap insiden keamanan merupakan indikator kuat dari lemahnya budaya tanggung jawab profesional dalam organisasi e-commerce (Strzelecki & Rizun, 2022).

c. Pelanggaran Prinsip Kompetensi Profesional (Competence)

Kode etik ACM menuntut profesional TI untuk terus meningkatkan kompetensi diri dalam praktik profesional. Skala kebocoran data yang masif ini menimbulkan pertanyaan kritis mengenai standar kompetensi keamanan siber yang diterapkan. Indikator kurangnya kompetensi terlihat dari beberapa aspek: sistem enkripsi lemah dimana password hash dapat di-crack dalam jumlah besar, tidak adanya *multi-factor authentication* (MFA) untuk akses kritis, audit keamanan yang tidak memadai sehingga peretasan tidak terdeteksi selama 2 bulan, tidak adanya sistem monitoring real-time untuk aktivitas mencurigakan, serta backup dan recovery plan yang tidak efektif. Profesional TI yang terlibat seharusnya menerapkan standar industri terbaik seperti enkripsi yang kuat, multi-factor authentication, dan audit keamanan rutin untuk memitigasi risiko. Fakta bahwa data dapat diekstraksi dan dijual menunjukkan adanya celah keamanan signifikan yang berakar pada kurangnya kompetensi dalam implementasi pertahanan siber. Perkasa dan Saly (2022) menekankan bahwa kegagalan marketplace dalam melindungi keamanan data pengguna mencerminkan ketidakmampuan dalam menerapkan standar keamanan teknis yang memadai, yang merupakan tanggung jawab profesional fundamental.

d. Pelanggaran Prinsip Integritas

Integritas mencakup kejujuran dalam berkomunikasi dengan publik. Tokopedia mengklaim "*passwords remain protected through encryption*" padahal faktanya 200.000 lebih password berhasil di-crack, data dijual dan disebar gratis di berbagai platform,

serta tidak ada transparansi penuh tentang skala kebocoran. Klaim yang tidak sesuai fakta ini melanggar prinsip integritas profesional. Transparansi dan kejujuran dalam komunikasi pasca-insiden merupakan kewajiban etis yang tidak dapat ditawar, karena berkaitan langsung dengan kepercayaan publik terhadap institusi teknologi (Fauzy & Hafizhah, 2023).

Beberapa penelitian terdahulu mengenai pelanggaran etika profesi teknologi informasi kasus kebocoran data pada marketplace di Indonesia sebagai berikut:

Muharrom, dkk (2025) melakukan penelitian tentang Analisis Etika Profesi IT dalam Kasus Kebocoran Data 91 Juta Pengguna Tokopedia. Dalam penelitian tersebut menunjukkan bahwa Insiden kebocoran data di Tokopedia bukan sekadar kelemahan teknis, melainkan bentuk nyata pelanggaran prinsip etika profesi IT. Terjadi pelanggaran terhadap prinsip utama etika IT, yaitu kerahasiaan (*confidentiality*), tanggung jawab profesional, dan integritas dalam mengelola basis data pengguna. Serta terdapat pula dampak dari pelanggaran etis ini menurunkan tingkat kepercayaan publik secara signifikan terhadap industri e-commerce nasional serta memicu urgensi penegakan hukum siber yang lebih ketat.

Berdasarkan penelitian yang dilakukan oleh Fathir & Evy (2026) yang meneliti tentang Urgensi Etika Pelindungan Data Pribadi Konsumen pada Platform E-Commerce di Indonesia mengemukakan bahwa Kasus kebocoran data e-commerce di Indonesia merupakan refleksi dari pelanggaran multidimensional terhadap kode etik internasional ACM (*Association for Computing Machinery*) dan IEEE. Spesifik melanggar 5 prinsip utama kode etik ACM: kewajiban berkontribusi pada masyarakat, menghindari bahaya/kerugian, bersikap jujur, menghormati privasi, serta melakukan evaluasi profesional yang komprehensif. Penelitian menekankan bahwa penguatan standar etika bagi praktisi IT e-commerce di Indonesia bersifat krusial demi menyelaraskan implementasi teknis dengan kepatuhan UU Perlindungan Data Pribadi (UU PDP).

HASIL DAN PEMBAHASAN

Berdasarkan beberapa penelitian terdahulu, maka dapat dirangkum sebagai berikut:

Tabel 1

NO	NAMA PENELITI	JUDUL PENELITIAN	HASIL PENELITIAN
1	N. Muharrom, dkk. (2025)	Analisis Etika Profesi IT dalam Kasus Kebocoran Data 91 Juta Pengguna Tokopedia	Menemukan adanya pelanggaran prinsip kerahasiaan (<i>confidentiality</i>), integritas, dan tanggung jawab profesional dalam manajemen data. Dampak kelalaian profesi IT ini secara sistemik menurunkan tingkat kepercayaan publik terhadap platform e-commerce.
2	Z. L. Farha & E. Nurmiati (2026)	Analisis Etika Penggunaan Data Konsumen dalam Platform E-Commerce	Menegaskan bahwa kegagalan proteksi bukan sekadar masalah teknis siber, melainkan kegagalan etis (tanggung jawab moral profesional). Profesional IT dan manajemen e-commerce gagal memenuhi

			prinsip kehati-hatian (<i>due diligence</i>) dalam mengelola data konsumen.
3	E. Sirait (2025)	Analisis Etika Bisnis Melalui Perspektif Pembeli Marketplace Indonesia	Menyimpulkan bahwa kebocoran data di <i>marketplace</i> melanggar nilai norma sosial dan prinsip etika bisnis digital. Meskipun kebijakan privasi tertera di platform, terdapat kesenjangan besar (<i>gap</i>) dalam implementasi riil dan pengawasan internal oleh tim IT.
4	H. Wibowo (2022)	Analisis Yuridis Kebocoran Data Marketplace dalam Perspektif UU ITE	Menunjukkan adanya tumpang tindih tanggung jawab etika profesi IT dengan kepatuhan hukum Penyelenggara Sistem Elektronik (PSE). Kebocoran terjadi karena lemahnya pemantauan keamanan berkala yang berujung pada gugatan perdata dan sanksi administrasi.
5	Ramadhani & Suhardiman (2026) Hani Zulfia Zahro (2022)	Tantangan Etika Keamanan Siber dalam Ekosistem Digital Indonesia	Menyatakan bahwa tiadanya lembaga pengawas data pribadi independen yang optimal di Indonesia membuat Kode Etik Teoretis (KTET) bidang TI harus menjadi kompas utama bagi praktisi komputer demi mencegah eksploitasi data pengguna di pasar gelap (<i>dark web</i>).

KESIMPULAN

Berdasarkan hasil analisis dan sintesis terhadap berbagai literatur, penelitian terdahulu, serta regulasi terkait, maka penelitian ini menarik beberapa kesimpulan utama sebagai berikut:

- a. Kegagalan Etis Multidimensi: Kebocoran data pengguna pada platform *marketplace* di Indonesia bukan sekadar kegagalan teknis (*cybersecurity breach*), melainkan manifestasi dari pelanggaran etika profesi TI yang mendasar. Hal ini mencakup pelanggaran prinsip kerahasiaan (*confidentiality*), akuntabilitas, dan prinsip kehati-hatian (*due diligence*) oleh para praktisi TI dan pengelola sistem maketplace.
- b. Kesenjangan Kepatuhan Kode Etik: Ditemukan kesenjangan (*gap*) yang signifikan antara kode etik profesi TI teoretis (seperti standar ACM atau IPKIN) dengan praktik tata kelola data di lapangan. Tekanan bisnis dan kurangnya audit etika internal membuat perlindungan hak privasi pengguna (*privacy rights*) sering kali terabaikan demi efisiensi operasional.
- c. Implikasi Sistemik Hukum dan Sosial: Pelanggaran etika ini berdampak langsung pada runtuhnya kepercayaan publik (*public trust*) terhadap ekosistem digital nasional. Penegakan hukum melalui UU Perlindungan Data Pribadi (UU PDP) dan UU ITE masih menghadapi tantangan besar karena belum optimalnya lembaga pengawas independen yang mengaudit kepatuhan etis para Penyelenggara Sistem Elektronik (PSE).

SARAN

Untuk mengatasi dan memitigasi pelanggaran etika profesi TI di masa mendatang, peneliti mengajukan beberapa rekomendasi, yaitu:

- a. Audit Etika TI Berkala: Perusahaan *marketplace* wajib menerapkan audit kepatuhan etika teknologi (*IT ethics audit*) dan keamanan data secara rutin, bukan hanya saat terjadi insiden.
- b. Internalisasi Kode Etik: Mengintegrasikan kode etik profesi TI internasional dan nasional ke dalam standar operasional prosedur (SOP) tim *developer* dan *data engineer*.
- c. Budaya Akuntabilitas Data: Menerapkan prinsip *Privacy by Design*, di mana perlindungan data pribadi dijadikan pertimbangan utama sejak awal sistem informasi dirancang.
- d. Sertifikasi Etika Profesi: Asosiasi profesi TI di Indonesia perlu memperketat syarat sertifikasi keahlian dengan memasukkan pemahaman etika komputasi sebagai komponen kelulusan utama.

DAFTAR PUSTAKA

- [1] Ariyanti, D. (2023). Hukum Siber dan Perlindungan Data di Indonesia. Yogyakarta: Deepublish
- [2] Association for Computing Machinery. (2018). ACM Code of Ethics and Professional Conduct.
- [3] Farha, Z. L., & Nurmiati, E. (2026). Analisis Etika Penggunaan Data Konsumen dalam Platform E-Commerce. *Journal of Information Systems Management and Digital Business (JISMDB)*, 3(3), 127–135.
- [4] Fauzy, E., & Hafizhah, A. (2023). Legal Analysis of User Personal Data Leak Cases at Tokopedia. In Mahadi : Indonesia Journal of Law (Vol. 2, Issue).
- [5] Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731–761
- [6] Muharrom, N., Wibowo, M. W. U. D., Wibowo, R. T., R., A. P., & Augustia, A. E. (2025). Analisis Etika Profesi IT dalam Kasus Kebocoran Data 91 Juta Pengguna Tokopedia. *TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan*, 3(3), 469–475.
- [7] Pohan, T. D., Irwan, M., Nasution, P., Islam, U., & Sumatera, N. (2023). Perlindungan Hukum Data Pribadi Konsumen dalam Platform E-Commerce. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, 1(3), 42–48.
- [8] Pakpahan, F. M., Suratno, T., & Lestari, D. (2025). Pengaruh Pelanggaran Privasi Data Terhadap Keputusan Pembelian Pengguna Tokopedia Menggunakan Theory Of Planned Behavior (TPB). *Infotek: Jurnal Informatika Dan Teknologi*, 8(2), 686697.
- [9] Perkasa, J., & Saly, J. N. (2022). Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020).
- [10] Ramadhani, A., & Suhardiman, B. (2026). Tantangan Etika Keamanan Siber dalam Ekosistem Digital Indonesia. *Jurnal Jejak Digital*, 4(1), 89–104. indojournal.com
- [11] Sadya, S. (2023). APJII: Pengguna internet Indonesia 215,63 juta pada 2022-2023.

- [12] Sirait, E., & Arjuna, S. (2025). Analisis Etika Bisnis Melalui Perspektif Pembeli Marketplace Indonesia. *Economics and Digital Business Review*, 6(2), 1148–1162.
- [13] Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability (Switzerland)*, 14(10).
- [14] Wibowo, H. (2022). Analisis Yuridis Kebocoran Data Marketplace dalam Perspektif UU ITE. *Jurnal Hukum Siber Indonesia*, 4(1), 32–47
- [15] Yusuf, A., Arianto, T., & Amanda, C. D. (2022). *Lanskap Keamanan Siber Indonesia 2022*. Jakarta: Badan Siber dan Sandi Negara (BSSN).

HALAMAN INI SENGAJA DIKOSONGKAN