Vol 1 No. 3, Februari 2026
E-ISSN: 3110-3898; P-ISSN: 3110-4657; Page 131-138

Pelindungan Data Pelanggan pada Pengembangan Sistem Informasi Transaksi Bisnis dan Pemasaran Digital

Evy Nurmiati[1], Farrel Tryardan Kusuma[2*]
[1-2]UIN Syarif Hidayatullah Jakarta, Tangerang Selatan, Indonesia
Email Korespondensi: farrel.tryardan24@mhs.uinjkt.ac.id

ABSTRAK

Pertumbuhan pesat platform e-commerce dan pemasaran digital berpacukan data memicu kerentanan privasi dan insiden keamanan siber yang masif di Indonesia, seperti kebocoran 91 juta data pelanggan. Penelitian ini bertujuan untuk menganalisis penerapan pelindungan data pelanggan dari perspektif teknis dan etis dalam pengembangan sistem informasi bisnis. Menggunakan metode studi literatur kualitatif, penelitian ini mengevaluasi regulasi pelindungan data (UU PDP Nomor 27 Tahun 2022), standar keamanan (OWASP), dan rekam jejak eksploitasi data pemasaran (dark patterns) berdasarkan analisis tematik terhadap 26 sumber pustaka mutakhir, terdiri dari sekitar 23 literatur akademik serta sejumlah dokumen regulasi dan standar (UU PDP, OWASP, kode etik profesi). Hasil kajian menunjukkan bahwa kerentanan fundamental bermuara pada kelemahan enkripsi peladen (back-end) dan manipulasi antarmuka akuisisi persetujuan (front-end). Untuk memitigasi hal ini, pengembang sistem wajib mengadopsi arsitektur Privacy by Design sejak fase konseptual melalui mekanisme pengaburan data (data masking), pemisahan basis data pemasaran, dan perancangan antarmuka opt-in yang transparan. Kesimpulannya, kepatuhan hukum dan etika keprofesian bukan sekadar tanggung jawab administratif perusahaan, melainkan kewajiban mutlak yang mengakar secara organik pada setiap baris kode yang dirancang oleh praktisi sistem informasi.

***Kata Kunci**: Pelindungan Data Pribadi; E-Commerce; Privacy by Design; Etika Pengembang; Sistem Informasi.*

PENDAHULUAN

Perkembangan ekonomi digital yang pesat telah mengubah lanskap transaksi bisnis dan strategi pemasaran secara radikal. Platform *e-commerce* terkini begitu bergantung pada pengumpulan data pribadi pelanggan berskala masif untuk mempersonalisasi layanan (Amukti & Hermawan, 2025). Informasi *user* terkini telah bertransformasi menjadi

Submitted: 10-01-2026
Revised: 25-01-2026
Acepted: 26-02-2026

komoditas strategis bernilai tinggi untuk meningkatkan efektivitas kampanye pemasaran digital (Yudilestari et al., 2025). Tantangan pelindungan privasi data dalam praktik bisnis *e-commerce* ini turut menjadi sorotan berbagai kajian, baik dari sisi teknis maupun tata kelola bisnis (Jurnal Komunikasi, 2024). Namun, kemajuan teknologi ini justru memicu sebuah paradoks, di mana ketergantungan yang teramat tinggi pada

pemrosesan data secara langsung mengekspos pelanggan terhadap ancaman keamanan siber yang sangat fatal (Matondang et al., 2025). Isu kebocoran data pribadi pada platform *e-commerce* nasional kini menjadi ancaman nyata yang menggugat integritas pengembang sistem informasi. Insiden peretasan 91 juta akun pengguna platform Tokopedia pada tahun 2020 memperlihatkan betapa rentannya perlindungan basis data perusahaan di Indonesia (Syahrevi et al., 2025). Sejalan dengan pola kebocoran data pribadi serupa yang teridentifikasi pada berbagai kasus lain di Indonesia (Utami et al., 2025). Penjualan data sensitive konsumen pada pasar gelap (*dark web*) akibat insiden tersebut terbukti mengikis kepercayaan publik terhadap keamanan platform transaksi elektronik secara drastis (Cahyaaty et al., 2024). Kerentanan pada arsitektur sistem ini sering kali bermuara pada kelalaian teknis di sisi peladen (*server*) yang sebetulnya telah diperingatkan secara global sebagai risiko keamanan tingkat tinggi (OWASP Foundation, 2021).

Lebih jauh lagi, eksploitasi rekam jejak pelanggan untuk kepentingan pemasaran digital turut memicu polemik etika keprofesian yang serius. Praktik eksekusi *marketing broadcast* (pesan siaran) sering kali menargetkan informasi pelanggan tanpa mekanisme persetujuan yang transparan (Farha & Nurmiati, 2026). Pengguna acap kali dimanipulasi melalui rekayasa antarmuka (dark patterns) agar tanpa sadar menyerahkan hak privasi mereka saat bertransaksi (Mathur et al., 2019). Fenomena ini menyoroti adanya kesenjangan yang tajam antara ambisi pencapaian laba bisnis dengan standar kepatuhan etika pengembangan perangkat lunak (ACM/IEEE-CS Joint Task Force, 1999).

Untuk memitigasi ketidakseimbangan ini, pemerintah Indonesia telah meresmikan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Pemerintah Republik Indonesia, 2022). Regulasi ini memaksa penyelenggara sistem elektronik untuk merombak standar kerahasiaan data pengguna. Kendati demikian, mayoritas kajian mengenai privasi data *e-commerce* di Indonesia saat ini masih didominasi oleh pendekatan yuridis normatif (Ardika, 2025). Kajian normatif lain menyoroti bagaimana Undang-Undang Nomor 27 Tahun 2022 memperkuat posisi hukum konsumen *marketplace* dalam memperoleh kepastian atas data pribadinya (Anggriawan et al., 2023). Pendekatan serupa juga menegaskan bahwa kerangka regulasi perlindungan konsumen di Indonesia belum sepenuhnya diikuti oleh kesiapan teknis pelaku usaha *e-commerce* dalam menjaga kerahasiaan data pelanggannya (Priliasari, 2023). Masih terdapat celah penelitian (*research gap*) yang teramat lebar mengenai bagaimana batasan legal ini diterjemahkan ke dalam level teknis oleh seorang developer sejak fase awal perancangan basis data (Maulana et al., 2026). Celah ini juga diidentifikasi secara eksplisit dalam kajian yang memetakan kesenjangan tanggung jawab pelaku usaha *e-commerce* dalam pelindungan data pribadi (Sobandi & Indriati, 2025).

Oleh karena itu, artikel ini bertujuan untuk menganalisis secara teknis dan etis penerapan pelindungan data pelanggan pada pengembangan sistem informasi transaksi bisnis. Dengan menggunakan studi kasus nyata insiden kebocoran data *e-commerce* di Indonesia, kajian ini membedah tanggung jawab developer dalam menyelaraskan arsitektur keamanan dengan prinsip *Privacy by Design* (Cavoukian, 2011). Analisis ini diharapkan mampu memberikan formulasi pedoman yang konkret bagi pengembang

sistem dalam mencegah penyalahgunaan data pemasaran, mematuhi kerangka hukum yang berlaku, serta menjaga kode etik keprofesian secara utuh.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (*literature review*) yang bersifat deskriptif-analitis. Penggunaan metode ini bertujuan untuk mengeksplorasi, mengintegrasikan, dan mengevaluasi teori-teori fundamental serta regulasi hukum yang berkaitan dengan pelindungan data konsumen pada platform digital (Matondang et al., 2025). Melalui pendekatan ini, peneliti mengidentifikasi kesenjangan antara implementasi teknis oleh pengembang perangkat lunak dengan koridor hukum yang berlaku di Indonesia (Maulana et al., 2026). Kronologi penelitian diawali dengan perumusan masalah keamanan siber, diikuti dengan tahapan akuisisi data literatur, hingga tahap sintesis analisis studi kasus.

Tahap akuisisi data dilakukan dengan mengumpulkan dua kategori sumber data utama, yaitu dokumen sekunder regulatif dan artikel jurnal ilmiah sekunder. Dokumen regulatif yang dikumpulkan meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Pemerintah Republik Indonesia, 2022), standar keamanan siber internasional (OWASP Foundation, 2021), serta kode etik profesi teknologi informasi (ACM/IEEE-CS Joint Task Force, 1999). Sementara itu, artikel jurnal ilmiah diperoleh dari basis data digital terindeks dengan rentang terbit tahun 2023–2026 yang berfokus pada dinamika bisnis digital (Amukti & Hermawan, 2025) serta pengelolaan privasi berbasis kecerdasan buatan (Yudilestari et al., 2025).

Seluruh literatur yang telah dikumpulkan kemudian disaring menggunakan teknik analisis isi (*content analysis*). Data yang diperoleh dari studi empiris mengenai kasus peretasan platform belanja daring nasional, seperti kasus Tokopedia (Sirajuddin & Markus, 2026; Syahrevi et al., 2025) dan Shopee (Cahyaaty et al., 2024), dikelompokkan secara tematik. Evaluasi kritis dilakukan dengan mengompilasi bukti-bukti kerentanan sistem tersebut, lalu mengoreksinya menggunakan kacamata arsitektur *Privacy by Design* (Cavoukian, 2011) dan batasan rekayasa antarmuka (Mathur et al., 2019).

HASIL DAN PEMBAHASAN

Evaluasi Celah Keamanan Pada Insiden Peretasan *E-Commerce* Nasional

Insiden kebocoran 91 juta data pengguna Tokopedia pada pertengahan tahun 2020 menjadi preseden terburuk yang mengekspos kerentanan arsitektur pelindungan data di Indonesia. Berdasarkan analisis keamanan, kebocoran berskala masif ini mengindikasikan adanya kelemahan fundamental pada implementasi kontrol akses dan metode enkripsi di sisi peladen (Syahrevi et al., 2025). Data pelanggan yang terdiri dari nama, nomor telepon, hingga surel dapat diekstraksi secara utuh akibat kelalaian dalam menerapkan standar kriptografi tingkat lanjut, sebuah celah keamanan yang secara eksplisit telah diklasifikasikan sebagai risiko tertinggi dalam pedoman pengembangan aplikasi web (OWASP Foundation, 2021).

Peristiwa ini menyoroti bahwa masih banyak perancangan basis data yang mengabaikan mitigasi risiko peretasan tingkat lanjut, sehingga menyebabkan erosi kepercayaan pengguna secara drastis (Cahyaaty et al., 2024). Dari perspektif regulasi dan tata kelola, kelalaian teknis dalam mengamankan pangkalan data ini melanggar prinsip keandalan sistem yang diamanatkan dalam kerangka perundangan transaksi elektronik (Sirajuddin & Markus, 2026). Hal ini membuktikan bahwa keamanan siber tidak bisa lagi

dipandang sebagai fitur tambahan, melainkan pondasi mutlak dari sebuah sistem transaksi yang memproses data publik berskala besar.

Manipulasi *Front-End* Dan Penyalahgunaan Data untuk Pemasaran Digital

Selain ancaman peretasan eksternal, eksploitasi data sering kali bersumber dari rancangan sistem internal itu sendiri, terutama saat mengakuisisi kontak pelanggan untuk kepentingan *marketing broadcast* (pesan siaran promosi). Tidak jarang, rancangan tata letak front-end dimanipulasi memanfaatkan elemen antarmuka web, seperti kotak centang yang disembunyikan secara visual (*hidden checkboxes*) atau penggunaan kontras antarmuka yang mengelabui agar pengguna tanpa sadar memberikan persetujuan penyiaran promosi (Mathur et al., 2019). Praktik dark patterns ini memicu dilema etis yang serius dalam ekosistem bisnis digital (Matondang et al., 2025).

Pemanfaatan rekam jejak transaksi pengguna untuk otomatisasi pemasaran tanpa mekanisme persetujuan eksplisit (opt-in) merupakan bentuk pelanggaran privasi struktural (Yudilestari et al., 2025). Oleh karena itu, batasan moral seorang pengembang sistem tidak hanya diukur dari kemampuan menulis kode yang efisien, tetapi juga dari komitmennya untuk tidak merancang fitur interaktif yang mengeksploitasi ketidaktahuan pengguna di balik layar monitor (Farha & Nurmiati, 2026).

Harmonisasi *Privacy By Design* Dengan Undang-Undang Pelindungan Data Pribadi

Untuk memutus mata rantai kerentanan teknis dan eksploitasi pemasaran tersebut, siklus rekayasa perangkat lunak wajib mengadopsi prinsip *Privacy by Design* sejak fase konseptual (Cavoukian, 2011). Dalam praktiknya, implementasi ini mengharuskan pengembang untuk menerapkan perlindungan data sebagai pengaturan bawaan (privacy as default). Secara teknis, langkah ini diwujudkan dengan memisahkan basis data transaksi sensitif menggunakan algoritma *masking* (pengaburan) identitas, sehingga jika terjadi penetrasi jaringan, kumpulan data tidak dapat dimanfaatkan oleh peretas secara langsung (Amukti & Hermawan, 2025). Selain itu, teknik anonimisasi data juga harus diperbarui secara berkala, mengingat metode konvensional saat ini rentan terhadapa serangan re-identifikasi dalam tata kelola *Big Data* (Razzaq & Nurmiati, 2026).

Langkah arsitektural ini harus diselaraskan secara penuh dengan amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang mewajibkan penyelenggara sistem untuk secara proaktif mencegah kegagalan pelindungan data (Pemerintah Republik Indonesia, 2022). Standar kepatuhan ini merupakan manifestasi langsung dari kode etik profesi teknologi informasi yang menekankan bahwa keselamatan, kesejahteraan publik, dan privasi digital menempati prioritas tertinggi di atas tuntutan komersial (ACM/IEEE-CS Joint Task Force, 1999). Prinsip moralitas dan perilaku etis dari praktisi teknologi ini terbukti menjadi benteng utama dalam menekankan risiko kejahatan siber dan ketirisan informasi pada sebuah sistem (Anugrah et al., 2025).

Dari perspektif perbandingan hukum, tinjauan atas perlindungan data pribadi konsumen *e-commerce* di Indonesia juga masih berpusat pada analisis kesesuaian norma dengan praktik di lapangan (Mansawan et al., 2025). Perubahan kerangka hukum melalui Undang-Undang Nomor 1 Tahun 2024 turut mendorong kajian lanjutan mengenai penguatan perlindungan konsumen atas data pribadi dalam transaksi elektronik (Putra et al., 2024). Tinjauan hukum siber terkini juga menegaskan bahwa penegakan aturan perlindungan data pribadi pada transaksi *e-commerce* di Indonesia masih menghadapi tantangan implementasi lintas sektor (Sinaga et al., 2026), sementara kajian kerangka hukum perlindungan konsumen menggarisbawahi perlunya harmonisasi lintas regulasi yang lebih konsisten (Supriyanto et al., 2025).

Untuk mengilustrasikan pemetaan tanggung jawab tersebut secara lebih sistematis,

Tabel 1 merangkum hasil evaluasi antara celah keamanan yang kerap terjadi pada platform *e-commerce* dengan mitigasi teknis berbasis *Privacy by Design* serta landasan hukumnya.

Tabel 1. Hasil Evaluasi Celah Keamanan dan Mitigasi Berbasis *Privacy by Design* pada *Platform E-commerce*

Aspek Kerentanan	Temuan Kasus & Dampak	Mitigasi Teknis	Kepatuhan Hukum & Aturan
Kelemahan Enkripsi *Back-end*	Peretasan 91 juta data pelanggan (Surel, No. HP, Nama) yang terekspos ke *dark web*.	Implementasi hashing tingkat lanjut (misal: algoritma SHA-256 dipadu salt) dan data masking untuk data sensitif.	UU PDP Pasal 39: Kewajiban mencegah akses tidak sah. OWASP Top 10: Mitigasi *Cryptographic Failures*.
Penyalahgunaan Data untuk *Marketing*	Kontak pengguna digunakan untuk promosi tanpa izin yang jelas.	Pemisahan (*decoupling*) tabel database transaksi operasional dengan basis data *marketing*.	UU PDP Pasal 20: Kewajiban memproses data sesuai tujuan awal (transaksi).
Manipulasi *Front-end*	*Hidden checkbox* yang menjebak pengguna agar menyetujui berlangganan promosi.	Desain antarmuka Opt-In yang eksplisit dan transparan (*Privacy as Default*).	Kode Etik ACM/IEEE: Menghindari sistem yang mengeksploitasi ketidaktahuan pengguna.

Pemilihan algoritma hashing SHA-256 yang dipadukan dengan salt pada Tabel 1 didasarkan pada pertimbangan bahwa algoritma ini merupakan standar kriptografi tahan-benturan (collision-resistant) yang direkomendasikan secara luas untuk melindungi kredensial dan data identitas dari serangan rainbow table maupun brute-force, sekaligus lebih ringan secara komputasi dibandingkan algoritma populer lain seperti bcrypt atau Argon2 untuk sistem transaksi berskala besar dengan volume permintaan tinggi (OWASP Foundation, 2021). Sementara itu, pemisahan (decoupling) basis data transaksi operasional dari basis data pemasaran dipilih sebagai mitigasi utama atas penyalahgunaan data untuk kepentingan marketing, karena pendekatan ini secara struktural membatasi akses silang (cross-access) antar-tim internal tanpa mengubah arsitektur inti sistem transaksi, sehingga lebih mudah diimplementasikan secara bertahap dibandingkan pendekatan enkripsi menyeluruh (full-database encryption) yang cenderung membebani performa sistem. Adapun desain antarmuka opt-in yang eksplisit dipilih sebagai mitigasi manipulasi front-end karena secara langsung menjawab akar masalah dark patterns, yakni ketiadaan persetujuan yang benar-benar disadari oleh pengguna (Mathur et al., 2019). Ketiga pilihan mitigasi ini saling melengkapi dalam mengoperasionalkan prinsip *Privacy by Design* pada tiap lapisan sistem, mulai dari peladen, basis data, hingga antarmuka pengguna.

KESIMPULAN

Penelitian ini menyimpulkan bahwa pelindungan data pelanggan pada pengembangan sistem informasi transaksi bisnis bukan sekadar pemenuhan kewajiban administratif, melainkan keharusan arsitektural yang wajib diimplementasikan sejak fase awal perancangan (*Privacy by Design*). Evaluasi terhadap insiden kebocoran data berskala masif di ekosistem *e-commerce* Indonesia membuktikan bahwa kelalaian teknis dalam enkripsi basis data (*back-end*) serta manipulasi antarmuka untuk mengakuisisi

persetujuan pemasaran secara terselubung (*front-end*) merupakan bentuk pelanggaran etika keprofesian dan regulasi yang sangat serius. Dengan mengharmonisasikan standar keamanan teknis dengan amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), para pengembang sistem memegang kendali penuh dalam mencegah eksploitasi data privasi sekaligus membangun ekosistem digital yang tangguh dan bermoral. Sebagai proyeksi ke depan, kerangka mitigasi ini dapat diadopsi sebagai pedoman audit keamanan dasar bagi unit bisnis skala kecil hingga menengah (*startup*). Untuk penelitian lanjutan, sangat disarankan adanya eksplorasi mengenai otomatisasi deteksi dark patterns pada antarmuka web menggunakan kecerdasan buatan (*Artificial Intelligence*) guna memperkuat pengawasan perlindungan konsumen secara waktu nyata (*real-time*).

DAFTAR PUSTAKA

ACM/IEEE-CS Joint Task Force. (1999). Software Engineering Code of Ethics and Professional Practice. IEEE Computer Society. https://www.computer.org/education/code-of-ethics

Amukti, F. D. W. T., & Hermawan, A. (2025). Tren dan Arah Masa Depan E-Commerce: Kajian Sistematis Literatur Tahun 2018–2024. Journal Economic Excellence Ibnu Sina, 3(2), 102-106. https://doi.org/10.59841/excellence.v3i2.2714

Anugrah, S., Himawan, M. Z., Qalby, N. R., & Nurmiati, E. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi Dalam Konteks Kebocoran Data Bsi (Bank Syariah Indonesia): Studi Literatur Sistematis. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *11*(2), 106-112. https://ojs.unikom.ac.id/index.php/JTK3TI/article/view/17033

Anggriawan, Z., Kemala, R., & Praditya, E. (2023). Analisis Perlindungan Hukum terhadap Data Konsumen Marketplace di Indonesia Berdasarkan Undang-undang No 27 Tahun 2022. Journal Humaniora: Jurnal Hukum dan Ilmu Sosial, 1(2), 36-40. https://doi.org/10.37010/hmr.v1i02.10.

Ardika, I. W. C. (2025). Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce. Indonesian Journal of Law and Justice, 2(3), 1-11. https://doi.org/10.47134/ijlj.v2i3.3601.

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. http://ejurnal.ubharajaya.ac.id/index.php/jiforty/article/view/3400

Cavoukian, A. (2011). *Privacy by Design*: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Farha, Z. L., & Nurmiati, E. (2026). Analisis Etika Penggunaan Data Konsumen dalam Platform E-Commerce. Jurnal Ilmu Sosial, Manajemen, dan Bisnis (JISMDB), 3(3), 127-135. https://doi.org/10.70248/jismdb.v3i3.3653

Jurnal Komunikasi. (2024). Data Privacy in E-Commerce Business: Challenges and Solutions. Jurnal Komunikasi. https://jkm.my.id/index.php/komunikasi/article/download/129/143

Mansawan, I. S. K., Sassan, J., & Bernard, J. (2025). Legal Protection of E-Commerce Consumers' Personal Data Under Indonesian Law. Jurnal Ilmu Hukum Kyadiren, 7(1),

538-554. https://doi.org/10.46924/jihk.v7i1.320

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Narayanan, A., & Marshini, C. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32. https://doi.org/10.1145/3359183

Matondang, K. A., Handani, T., Handayani, A., & Wati, F. (2025). Etika Bisnis dalam Perlindungan Data Pribadi Konsumen di Era Bisnis Digital: Sebuah Studi Literatur. JUPSIM: Jurnal Pusat Studi Ilmu Manajemen, 4(3), 551-565. https://doi.org/10.55606/jupsim.v4i3.5508

Maulana, M. I. A., Yuliartini, N. P. R., & Mangku, D. G. S. (2026). Evaluasi Implementasi Undang-Undang Perlindungan Data Pribadi pada Kasus Kebocoran Data Pengguna E-Commerce di Indonesia. Jurnal Humif, 3(2), 41-51. https://doi.org/10.62383/humif.v3i2.2980

OWASP Foundation. (2021). OWASP Top 10 Web Application Security Risks. OWASP. https://owasp.org/Top10/

Pemerintah Republik Indonesia. (2008). Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008. https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Pemerintah Republik Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara RI Tahun 2022. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-undangan di Indonesia. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12(2), 261–279. https://doi.org/10.33331/rechtsvinding.v12i2.1285.

Putra, F. J., Pratama, A. A., & Susilo, F. A. (2024). Perlindungan Konsumen atas Data Pribadi Dalam Transaksi E-Commerce Pasca Berlakunya Undang-Undang Nomor 1 Tahun 2024. Jurnal HAM dan Ilmu Hukum (Jurisprudentia). https://jurisprudentia.bunghatta.ac.id/index.php/jurisprudentia/article/download/229/41/403

Razzaq, R. S. D., & Nurmiati, E. (2026). Tantangan etika dan privasi terhadap cyber crime big data (Studi literatur). *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, *3*(2), 604-608. https://jurnal.kopusindo.com/index.php/jkhkp/article/download/1646/1387

Sinaga, A. F., Siahaan, P. G., Lbn Batu, D. P., Pinem, M. B., & Rifky, M. (2026). Perlindungan Data Pribadi dalam Transaksi E-Commerce: Tinjauan Hukum Siber Indonesia. JERUMI: Journal of Education Religion Humanities and Multidiciplinary, 4(1). https://rayyanjurnal.com/index.php/jerumi/article/download/8678/7388

Sirajuddin, L., & Markus, D. P. (2026). Analysis of Legal Protection for Tokopedia Consumer Data in Data Leakage Cases in Indonesia. Journal of Law and Justice (JLJ), 4(1), 42-51. https://doi.org/10.33506/jlj.v4i1.5199

Sobandi, S., & Indriati, N. R. (2025). Legal gaps in personal data protection and *e-commerce* responsibilities in Indonesia. International Journal of Law Reconstruction, 9(1). https://jurnal.unissula.ac.id/index.php/lawreconstruction/article/download/45253/12921

Supriyanto, S., Rahardjo, T. M. S., Sumiyati, S., Noerdjaja, H., Pambudi, G. E., & Prabowo,

M. S. (2025). Consumer protection legal frameworks in Indonesia: The challenges of *e-commerce* and data privacy. Research Horizon, 5(2), 119–128. https://journal.lifescifi.com/index.php/RH/article/download/491/399/849

Syahrevi, M., Opat, A. C. S., Saputra, A., Valianda, Y. Z. A., & Augustia, A. E. (2025). Pengaruh Kasus Kebocoran Data Tokopedia dari Tahun 2020-2023 terhadap Kepercayaan Konsumen E-Commerce di Indonesia. TEKNOBIS: Teknologi, Bisnis Dan Pendidikan, 3(3), 408-414. https://jurnalmahasiswa.com/index.php/teknobis/article/view/3102

Utami, T. K., Suryanto, S. O., Putri, K. A., & Asriani, F. (2025). Personal Data Breach Cases in Indonesia: Perspective Of Personal Data Protection Law. Customary Law Journal, 2(2), 1-21. https://doi.org/10.47134/jcl.v2i2.3742

Yudilestari, E. P., Setyaningsih, I., Komara, M. A., & Tarmudi. (2025). AI Marketing Management and Data Privacy Compliance: Effects on Consumer Behavior and Loyalty. Journal of Management and Business Innovations, 7(2). https://jurnal.uinsu.ac.id/index.php/jombi/article/view/28126