TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

Urgensi Etika Pelindungan Data Pribadi Konsumen pada Platform E-Commerce di Indonesia

Shidiqi Fathir Rakhman[1], Evy Nurmiati[2]

[1, 2]Fakultas Sains dan Teknologi, Program Studi Sistem Informasi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
Email: [1*]shidiqi.fathir24@mhs.uinjkt.ac.id , [2]evy.nurmiati@uinjkt.ac.id
(* : corresponding author)

Abstrak−Pertumbuhan pesat platform *e-commerce* di Indonesia diiringi meningkatnya kasus kebocoran data pribadi konsumen, seperti insiden Tokopedia (91 juta akun, 2020), Bukalapak (13 juta akun, 2020), dan Indihome (279 juta data, 2024). Meskipun pemerintah telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), kasus pelanggaran terus berulang sehingga menimbulkan pertanyaan mengenai kecukupan pendekatan hukum tanpa diiringi dimensi etika. Penelitian ini bertujuan menganalisis urgensi penerapan etika profesi teknologi informasi (TI) dalam pelindungan data pribadi konsumen pada platform *e-commerce* di Indonesia. Penelitian menggunakan metode studi pustaka (*library research*) dengan pendekatan kualitatif deskriptif terhadap 15 literatur primer terbitan 2022–2025, dianalisis menggunakan teknik *content analysis*. Hasil penelitian menunjukkan bahwa kasus kebocoran data merupakan cerminan pelanggaran multidimensional terhadap lima prinsip kode etik ACM (1.1, 1.2, 1.3, 1.6, 2.5) dan IEEE Code of Ethics, yaitu kontribusi terhadap kesejahteraan publik, menghindari bahaya, kejujuran, penghormatan privasi, dan evaluasi profesional yang komprehensif. Penerapan kerangka CIA Triad dan prinsip *Privacy by Design* menjadi fondasi etis yang esensial. Kepatuhan UU PDP saja tidak cukup tanpa internalisasi nilai etika oleh praktisi TI.

Kata Kunci: Etika Profesi TI; Pelindungan Data Pribadi; E-Commerce; UU PDP; CIA Triad

Abstract−The rapid growth of e-commerce platforms in Indonesia has been accompanied by increasing cases of consumer personal data breaches, such as the Tokopedia (91 million accounts, 2020), Bukalapak (13 million accounts, 2020), and Indihome incidents (279 million records, 2024). Although the government has enacted Law No. 27/2022 on Personal Data Protection (PDP Law), violations continue to recur, raising questions about the adequacy of a purely legal approach without ethical dimensions. This study aims to analyze the urgency of implementing information technology (IT) professional ethics in protecting consumer personal data on e-commerce platforms in Indonesia. The research uses the library research method with a qualitative descriptive approach on 15 primary literatures published in 2022–2025, analyzed using content analysis techniques. The results show that data breach cases reflect multidimensional violations of five principles of the ACM Code of Ethics (1.1, 1.2, 1.3, 1.6, 2.5) and the IEEE Code of Ethics, namely contribution to public welfare, avoiding harm, honesty, respect for privacy, and comprehensive professional evaluation. The implementation of the CIA Triad framework and Privacy by Design principles becomes an essential ethical foundation. Compliance with the PDP Law alone is insufficient without the internalization of ethical values by IT practitioners.

Keywords: IT Professional Ethics; Personal Data Protection; E-Commerce; PDP Law; CIA Triad

1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah lanskap perdagangan secara fundamental. Platform *e-commerce* di Indonesia tumbuh pesat dan menjadi tulang punggung ekonomi digital nasional, dengan jutaan transaksi terjadi setiap hari. Di balik kemudahan transaksi digital tersebut, tersimpan risiko serius terkait keamanan dan kerahasiaan data pribadi konsumen (Afip et al., 2025). Setiap kali konsumen mendaftar atau bertransaksi, mereka menyerahkan informasi pribadi mulai dari nama, alamat, nomor telepon, foto KTP, hingga data finansial kepada platform *e-commerce* (Pohan et al., 2023). Fenomena ini menempatkan data pribadi sebagai komoditas strategis bernilai ekonomi tinggi, sekaligus menjadikannya target utama kejahatan siber di era *big data* (Matondang et al., 2025; Abdullah et al., 2025).

Kasus Tokopedia menjadi insiden kebocoran data terbesar dalam sejarah *e-commerce* Indonesia. Menurut Ardika (2025), data sebanyak 91 juta akun, mencakup identitas, kontak, dan *hash password*, berhasil dieksfiltrasi dan diperjualbelikan di forum peretas sebelum perusahaan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

mengakui insiden secara resmi. Keterlambatan pengakuan ini sendiri merepresentasikan pelanggaran prinsip kejujuran (ACM 1.3) (Afip et al., 2025; Ardika, 2025).

Pola serupa berulang pada Bukalapak (13 juta akun, 2020) dengan eksploitasi kerentanan API dan respons awal yang menyangkal insiden, serta Indihome (279 juta data, 2024) akibat celah API tanpa *rate limiting* yang memadai (Sari et al., 2025; (Halizah et al., 2025). Kasus terkini World App/Worldcoin menambah dimensi baru: pengumpulan data biometrik iris tanpa *informed consent* yang layak pada kelompok rentan ekonomi (Rahman et al., 2025). Keseluruhan pola ini mengindikasikan kelemahan sistemik yang bersumber pada kelalaian etis, bukan sekadar keterbatasan teknis.

Andari & Nurmiati (2026) menegaskan bahwa insiden kebocoran data di Indonesia bukan sekadar kegagalan teknis, melainkan mencerminkan persoalan yang lebih mendasar yaitu lemahnya etika profesional di kalangan tenaga TI. Kajian mereka terhadap kasus BPJS Kesehatan dan data pajak menunjukkan bahwa institusi publik sekalipun rentan terhadap kebocoran yang berakar pada kelalaian etis, dan mengusulkan Kerangka Tanggung Jawab Etis-Teknis (KTET) yang mencakup empat dimensi: teknis-preventif, kepatuhan hukum, transparansi-pelaporan, dan pengembangan kompetensi berkelanjutan (Andari & Nurmiati, 2026).

Sebagai respons terhadap fenomena tersebut, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menjadi payung hukum khusus dalam mengatur pengelolaan data pribadi. UU PDP secara substansial mengadopsi banyak prinsip dari General Data Protection Regulation (GDPR), regulasi pelindungan data Uni Eropa yang berlaku sejak Mei 2018 dan menjadi rujukan global dalam pelindungan data pribadi (Ramadhani, 2022). UU PDP juga mengamanatkan pembentukan Otoritas Pelindungan Data Pribadi (OPDP) sebagai lembaga independen yang ditunjuk Presiden untuk menyelenggarakan pengawasan dan penegakan hukum administratif (Pasal 58–60 UU PDP), serupa dengan European Data Protection Board (EDPB) di Uni Eropa. Regulasi ini mewajibkan setiap pengendali data untuk menerapkan prinsip transparansi, akuntabilitas, dan pelindungan maksimal terhadap data pribadi (Priliasari, 2023). Namun, meskipun regulasi telah hadir, kasus pelanggaran terus terjadi. Data Kementerian Komunikasi dan Informatika menunjukkan terdapat 124 kasus pelanggaran pelindungan data periode 2019–2024, dengan 111 kasus di antaranya merupakan kebocoran data (Matondang et al., 2025). Hanya sekitar 35% responden Indonesia yang memahami hak privasi digital mereka, 65% tidak pernah membaca kebijakan privasi, dan hanya 40% merasa data mereka aman (Abdullah et al., 2025). Realitas ini menimbulkan pertanyaan kritis: apakah pendekatan hukum semata cukup untuk melindungi data pribadi konsumen?

Sejalan dengan hal tersebut, Farha & Nurmiati (2026) menemukan bahwa praktik transparansi dan *informed consent* pada platform *e-commerce* di Indonesia masih diperlakukan sebagai formalitas, bukan sebagai komitmen etis yang substantif. Studi mereka mendokumentasikan bahwa kebocoran data Tokopedia tahun 2020 yang mengekspos lebih dari 91 juta akun bukan semata-mata kegagalan teknis keamanan siber, melainkan juga mencerminkan ketidakcukupan komitmen etis perusahaan dalam melindungi informasi yang dipercayakan konsumen kepada mereka (Farha & Nurmiati, 2026).

Dimensi etika profesi teknologi informasi menjadi sangat relevan untuk dikaji dalam konteks ini. Setiap profesional di bidang TI, baik sebagai pengembang sistem, administrator basis data, maupun analis keamanan siber, terikat oleh kode etik profesi seperti ACM Code of Ethics (Association for Computing Machinery, 2018) dan IEEE Code of Ethics (Institute of Electrical and Electronics Engineers, 2025) yang menjunjung tinggi prinsip integritas, akuntabilitas, dan tanggung jawab terhadap kepentingan publik (Halizah et al., 2025). Selain kerangka kode etik internasional tersebut, prinsip CIA Triad (Confidentiality, Integrity, Availability) juga relevan sebagai standar baku keamanan informasi yang menjadi titik temu antara aspek teknis sistem dan aspek etika profesi (Harahap et al., 2023). Kebocoran data dalam skala besar mempertanyakan komitmen dan implementasi nyata prinsip-prinsip etika tersebut dalam praktik pengelolaan data sehari-hari.

Berdasarkan latar belakang tersebut, penelitian ini mengangkat dua rumusan masalah utama: (1) Bagaimana kasus kebocoran data pribadi pada platform *e-commerce* di Indonesia

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

mencerminkan pelanggaran etika profesi TI ditinjau dari ACM dan IEEE Code of Ethics? (2) Bagaimana penerapan prinsip etika profesi TI dapat memperkuat pelindungan data pribadi konsumen di luar kepatuhan terhadap UU PDP? Tujuan penelitian ini adalah menganalisis urgensi penerapan etika profesi TI dalam pelindungan data pribadi konsumen, memetakan pelanggaran prinsip etika secara eksplisit, sekaligus merumuskan kontribusi etika sebagai pelengkap kerangka hukum yang ada.

2. METODE PENELITIAN

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan metode studi pustaka (*library research*) dengan pendekatan kualitatif deskriptif. Metode ini dipilih karena objek kajian bersifat normatif-konseptual, yaitu menganalisis urgensi penerapan etika dalam pelindungan data pribadi pada platform *e-commerce*, sehingga lebih tepat dikaji melalui telaah literatur dibandingkan penelitian lapangan.

2.2. Sumber Data

Sumber data dalam penelitian ini terdiri dari tiga kategori. Pertama, sumber primer berupa regulasi resmi, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai payung hukum utama yang dianalisis. Kedua, sumber sekunder berupa 15 artikel jurnal ilmiah nasional yang diterbitkan dalam rentang tahun 2022–2025 yang membahas pelindungan data pribadi, etika profesi TI, dan kasus kebocoran data pada platform digital di Indonesia, serta dokumen kode etik profesi yaitu ACM Code of Ethics (Association for Computing Machinery, 2018) dan IEEE Code of Ethics (Institute of Electrical and Electronics Engineers, 2025) yang berfungsi sebagai kerangka analitis untuk memetakan pelanggaran etika profesi. Ketiga, sumber tersier berupa pemberitaan media kredibel mengenai kasus kebocoran data pribadi pada platform *e-commerce* di Indonesia yang digunakan untuk verifikasi kronologi insiden.

2.3. Kriteria Seleksi Literatur

Kriteria seleksi literatur jurnal mencakup empat parameter: (1) artikel jurnal nasional terakreditasi atau jurnal yang memiliki ISSN/E-ISSN resmi, (2) membahas pelindungan data pribadi, etika profesi TI, atau kasus kebocoran data pada platform digital di Indonesia, (3) terbit dalam rentang 2022–2025 untuk menjamin aktualitas, dan (4) tersedia teks lengkap. Berdasarkan kriteria tersebut, terkumpul 15 literatur primer yang kemudian dianalisis menggunakan tabel *review* literatur untuk memetakan metode, fokus kajian, temuan utama, dan relevansinya dengan rumusan masalah.

2.4. Teknik Analisis Data

Teknik pengumpulan data dilakukan melalui telaah dokumen (*document review*), sedangkan analisis menggunakan teknik analisis isi (*content analysis*) dengan tiga tahap: (1) reduksi data dengan mengidentifikasi tema kunci dari setiap literatur, (2) penyajian data dalam bentuk tabel komparatif untuk memudahkan sintesis, dan (3) penarikan kesimpulan dengan mengontraskan temuan literatur terhadap prinsip-prinsip dalam ACM Code of Ethics dan IEEE Code of Ethics, serta kerangka regulasi UU PDP.

3. ANALISA DAN PEMBAHASAN

3.1 Pemetaan Kasus Kebocoran Data pada Platform E-Commerce dan Layanan Digital di Indonesia

Sintesis literatur menunjukkan bahwa kasus kebocoran data pada platform *e-commerce* dan layanan digital di Indonesia bukan fenomena terisolasi, melainkan pola berulang yang mengindikasikan kelemahan sistemik. Tabel 1 menyajikan rangkuman kasus-kasus utama yang relevan dengan kajian ini.

Tabel 1. Pemetaan Kasus Kebocoran Data pada Platform E-Commerce dan Layanan Digital di Indonesia

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

Tahun	Platform	Jumlah Data Bocor	Akar Penyebab Teknis	Pelanggaran Etika Utama
2020	Tokopedia	91 juta akun pengguna	Lemahnya kontrol akses, sistem deteksi intrusi tidak siap, ISO/IEC 27001 belum optimal (Afip et al., 2025).	*Avoid Harm*, *Honesty* (pengumuman tertunda hingga 3 Mei 2020) (Diah & Wiraguna, 2025; Ardika, 2025)
2020	Bukalapak	13 juta akun pengguna	Eksploitasi kerentanan API, kontrol akses tidak memadai (Sari et al., 2025; Diah & Wiraguna, 2025)	*Avoid Harm*, *Honesty* (awalnya membantah insiden) (Diah & Wiraguna, 2025)
2024	Indihome	279 juta data pengguna	Celah keamanan API yang tidak diamankan, tidak adanya *rate limiting* (Halizah et al., 2025)	*Avoid Harm*, *Respect Privacy, Professional Review* (Halizah et al., 2025)
2025	World App / Worldcoin	Data biometrik iris (jumlah belum dipublikasi)	Pengumpulan data biometrik tanpa *informed consent* yang memadai pada kelompok rentan ekonomi (Rahman et al., 2025)	*Respect Privacy, Avoid Harm*, *Contribute to Society* (Rahman et al., 2025)

Tabel 1 menunjukkan bahwa selama periode 2020–2025, terjadi peningkatan baik pada skala data yang bocor (dari 13 juta hingga 279 juta) maupun pada sensitivitas jenis data (mulai dari data demografis hingga data biometrik permanen). Akar penyebab teknis menunjukkan pola yang konsisten: lemahnya kontrol akses, kerentanan API yang tidak diamankan, dan belum optimalnya penerapan standar keamanan internasional seperti ISO/IEC 27001 (Afip et al., 2025; Halizah et al., 2025). Pola berulang ini mengindikasikan bahwa pelanggaran terjadi bukan karena keterbatasan teknologi, melainkan karena pengabaian terhadap praktik keamanan yang sebenarnya sudah dikenal luas di industri TI.

3.2 Pemetaan Pelanggaran Prinsip Kode Etik ACM dan IEEE

Mengacu pada ACM Code of Ethics (Association for Computing Machinery, 2018) dan IEEE Code of Ethics (Institute of Electrical and Electronics Engineers, 2025), analisis terhadap kasus-kasus kebocoran data pada platform *e-commerce* mengidentifikasi setidaknya lima kategori pelanggaran etika profesi TI yang berulang.

Andari & Nurmiati (2026) memperkuat temuan ini melalui kajian lintas sektor yang menunjukkan bahwa etika profesi TI dalam konteks keamanan siber bukan sekadar mematuhi aturan, melainkan membangun "benteng digital" yang dilandasi integritas. Mereka menekankan bahwa kewajiban etis profesional TI dimulai jauh sebelum insiden terjadi, yakni pada tahap perancangan sistem itu sendiri melalui pendekatan *privacy by design*, di mana perlindungan privasi diintegrasikan ke dalam arsitektur sistem sejak awal sebagai manifestasi nyata dari etika profesi yang proaktif, bukan reaktif (Andari & Nurmiati, 2026).

Pertama, pelanggaran prinsip “Contribute to Society and to Human Well-being” (ACM 1.1) yang menjadi prinsip tertinggi dalam kode etik. Prinsip ini menuntut profesional TI untuk memprioritaskan kesejahteraan masyarakat dalam setiap keputusan teknis yang diambil. Kebocoran data berskala 91 juta hingga 279 juta pengguna menunjukkan kegagalan sistemik dalam menempatkan kepentingan publik sebagai prioritas, di mana keputusan desain sistem dan alokasi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

sumber daya keamanan tampak lebih berorientasi pada efisiensi bisnis dibandingkan pelindungan pengguna (Halizah et al., 2025; Diah & Wiraguna, 2025).

Kedua, pelanggaran prinsip "Avoid Harm" (ACM 1.2) dan "Hold Paramount the Safety, Health, and Welfare of the Public" (IEEE). Profesional TI yang mengembangkan dan mengelola sistem *e-commerce* wajib mengantisipasi dan mencegah kerugian yang dapat ditimbulkan teknologinya. Kebocoran data telah menyebabkan kerugian nyata berupa risiko penipuan, *phishing*, pencurian identitas, dan dalam kasus World App, .eksploitasi kelompok rentan ekonomi melalui pertukaran data biometrik dengan insentif kripto bernama Worldcoin (Pohan et al., 2023; Rahman et al., 2025). Halizah et al. (2025) secara eksplisit menyatakan bahwa kegagalan mencegah kebocoran data tidak hanya merupakan kelalaian teknis, tetapi juga pelanggaran etika profesi yang dapat dianalisis melalui kerangka deontologi (etika kewajiban) maupun utilitarianisme (etika konsekuensi).

Ketiga, pelanggaran prinsip "Be Honest and Trustworthy" (ACM 1.3). Kasus Tokopedia menunjukkan keterlambatan signifikan dalam pengumuman insiden, peretasan terjadi 20 Maret 2020 sementara pengakuan resmi baru disampaikan 3 Mei 2020 (Ardika, 2025). Bukalapak bahkan awalnya membantah insiden tersebut (Diah & Wiraguna, 2025). Pola komunikasi defensif ini melanggar kewajiban pelaporan 3x24 jam yang diatur Pasal 46 UU PDP (Republik Indonesia, 2022) sekaligus melanggar prinsip kejujuran profesi. Sari et al. (2025) menunjukkan bahwa pendekatan komunikasi defensif justru memperburuk persepsi publik dan memperpanjang waktu pemulihan kepercayaan.

Keempat, pelanggaran prinsip "Respect Privacy" (ACM 1.6). Penyimpanan data pribadi tanpa enkripsi yang memadai pada data sensitif (seperti email dan nomor telepon dalam kasus Tokopedia) (Afip et al., 2025), pengumpulan data biometrik tanpa *informed consent* yang mendalam pada kasus World App (Rahman et al., 2025), serta absennya prinsip *Privacy by Design* pada arsitektur sistem (Rahmadani et al., 2025; Diah & Wiraguna, 2025) menunjukkan bahwa privasi diperlakukan sebagai pertimbangan tambahan, bukan sebagai prinsip desain fundamental.

Kelima, pelanggaran prinsip "Give Comprehensive and Thorough Evaluations" (ACM 2.5). Profesional TI memiliki tanggung jawab untuk melakukan evaluasi menyeluruh terhadap risiko sistem yang mereka kembangkan, termasuk Data Protection Impact Assessment (DPIA) yang diwajibkan Pasal 34 UU PDP (Diah & Wiraguna, 2025; Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022). Kegagalan industri dalam mengantisipasi serangan API pada Indihome dan kelemahan kontrol akses pada Tokopedia mencerminkan absennya evaluasi etika yang memadai dalam siklus pengembangan produk.

3.3 Penerapan CIA Triad sebagai Dasar Etika Pengelolaan Data

Dalam kasus Tokopedia, meskipun *password* telah dienkripsi, data sensitif lain seperti alamat email dan nomor telepon tidak terlindungi secara optimal sehingga tetap dapat dieksploitasi setelah kebocoran (Afip et al., 2025). Ini menunjukkan bahwa penerapan *Confidentiality* yang parsial tidak memadai sebagai perlindungan yang sesungguhnya.

Prinsip *Integrity* menjamin data tidak dapat dimanipulasi tanpa otorisasi melalui *checksums* dan *audit trail*, sedangkan *Availability* memastikan sistem tetap dapat diakses pengguna yang berhak (Harahap et al., 2023).

Penerapan CIA Triad tidak dapat dilepaskan dari dimensi etis. *Confidentiality* bukan hanya soal teknis enkripsi, tetapi komitmen moral untuk menghormati privasi konsumen sebagai bagian dari hak asasi manusia (Rahmadani et al., 2025). *Integrity* bukan hanya soal mekanisme teknis, tetapi kejujuran profesional dalam mengelola data tanpa manipulasi. *Availability* bukan hanya soal infrastruktur, tetapi tanggung jawab profesional untuk memastikan layanan dapat diandalkan oleh konsumen. Dengan demikian, CIA Triad menjadi titik temu antara aspek teknis Sistem Informasi dengan aspek etika profesi TI (Matondang et al., 2025; Harahap et al., 2023).

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

3.4 Komparasi UU PDP Indonesia dengan GDPR Uni Eropa

Untuk memahami posisi UU PDP dalam konstelasi regulasi pelindungan data global, Tabel 2 menyajikan komparasi parameter utama antara UU PDP Indonesia dengan GDPR Uni Eropa berdasarkan analisis Ramadhani (2022), Rahmadani et al. (2025), dan Abdullah et al. (2025).

Tabel 2. Komparasi UU PDP Indonesia dengan GDPR Uni Eropa

Parameter	UU PDP No. 27 Tahun 2022 (Indonesia)	GDPR (Uni Eropa)
Lembaga Pengawas	Otoritas Prlindungan Data Pribadi (OPDP) belum sepenuhnya terbentuk dan independen (Rahmadani et al., 2025; Abdullah et al., 2025)	European Data Protection Board (EDPB) sudah aktif dengan kewenangan independent (Ramadhani, 2022)
Sanksi Maksimum	Denda administratif hingga 2% pendapatan tahunan (Pasal 57) + sanksi pidana penjara 4–6 tahun dan/atau denda hingga Rp6 miliar (Pasal 67–68) (Diah & Wiraguna, 2025)	Denda hingga 4% pendapatan global tahunan atau €20 juta (Ramadhani, 2022)
Right to be Forgotten	Diatur namun mekanismenya belum eksplisit; perlu jalur pengadilan (Ramadhani, 2022)	Mekanisme efisien tanpa harus melalui pengadilan, hak penghapusan jelas (Ramadhani, 2022)
Privacy by Design	Belum diatur secara eksplisit sebagai kewajiban (Rahmadani et al., 2025; Abdullah et al., 2025)	Diwajibkan eksplisit (Pasal 25 GDPR) (Ramadhani, 2022)
Yurisdiksi Lintas Negara	Secara normatif ekstrateritorial (Pasal 2), namun penegakannya terbatas terhadap pelaku usaha di luar yurisdiksi (Matondang et al., 2025; Abdullah et al., 2025)	Ekstrateritorial; berlaku untuk pengendali di luar UE yang memproses data warga UE (Ramadhani, 2022)
Standardisasi Privacy Policy	Belum ada standardisasi seragam (Ramadhani, 2022)	Standar *template* seragam dan ringkas (Ramadhani, 2022)

Tabel 2 mengonfirmasi bahwa meskipun UU PDP merupakan kemajuan signifikan, masih terdapat beberapa kelemahan implementatif dibandingkan GDPR. Belum terbentuknya OPDP yang independen menjadi kelemahan paling kritis karena tanpa lembaga pengawas yang berwenang, sanksi yang diatur dalam UU PDP berisiko menjadi "macan kertas" (Rahmadani et al., 2025; Abdullah et al., 2025). Selain itu, absennya kewajiban *Privacy by Design* yang eksplisit menyebabkan platform tidak diwajibkan untuk mengintegrasikan pelindungan privasi sejak tahap perancangan sistem, melainkan baru ditambahkan sebagai fitur pelengkap (Rahmadani et al., 2025).

3.5 Urgensi Dimensi Etika di Atas Kepatuhan Hukum

Pengalaman empiris menunjukkan bahwa kepatuhan hukum semata tidak cukup untuk mencegah pelanggaran pelindungan data pribadi. Sejumlah kelemahan implementatif masih ditemui, antara lain keterbatasan yurisdiksi terhadap pelaku usaha di luar negeri, minimnya literasi digital masyarakat dengan hanya 35% memahami hak privasi digital (Abdullah et al., 2025), serta kompleksitas teknologi seperti kecerdasan buatan dan biometrik yang menghadirkan ancaman privasi kontemporer (Matondang et al., 2025; Judijanto & Harsya, 2025; Rahman et al., 2025).

Farha & Nurmiati (2026) menyimpulkan bahwa tata kelola data yang bertanggung jawab hanya dapat terwujud melalui integrasi antara komitmen internal perusahaan, penguatan regulasi dan pengawasan, adopsi teknologi seperti *blockchain* dan *privacy by design*, serta peningkatan literasi digital konsumen secara bersamaan. Studi mereka mengonfirmasi adanya hubungan kausal yang kuat antara praktik etika data dan kepercayaan konsumen: kegagalan etis seperti yang terjadi pada kasus Tokopedia 2020 menunjukkan bahwa kepercayaan yang rusak akibat pelanggaran data jauh lebih sulit dipulihkan dibandingkan bentuk krisis reputasi lainnya (Farha & Nurmiati, 2026).

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

Regulasi hanya menetapkan ambang batas minimum perilaku yang dapat ditoleransi, sementara etika profesi mendorong praktisi menuju standar tertinggi yang benar-benar melindungi pengguna. Profesional TI yang beretika tidak berhenti pada pertanyaan "apakah ini diperbolehkan secara hukum?" tetapi melangkah lebih jauh: "apakah ini yang terbaik bagi kepentingan pengguna dan masyarakat?" (Halizah et al., 2025; Matondang et al., 2025). Diah & Wiraguna (2025)menekankan bahwa kepatuhan regulasi data seharusnya dipandang sebagai fondasi kepercayaan konsumen jangka panjang, bukan sebagai kewajiban yang memberatkan.

Implementasi etika profesi TI dapat diwujudkan melalui empat langkah utama: (1) integrasi nilai etika ACM/IEEE dalam kurikulum pendidikan TI dan pelatihan berkelanjutan (Halizah et al., 2025), (2) penerapan *Security by Design* dan *Privacy by Design* sejak fase perancangan sistem, bukan setelah produk diluncurkan (Pohan et al., 2023; Sari et al., 2025), (3) pelaksanaan audit keamanan dan *penetration* testing secara rutin dan independen, serta (4) peningkatan literasi digital konsumen agar mereka mampu mengenali dan memperjuangkan hak privasi mereka (Tambunan & Nasution, 2023; Abdullah et al., 2025).

4. KESIMPULAN

Berdasarkan analisis terhadap 15 literatur primer dan kasus kebocoran data pada platform *e-commerce* di Indonesia, penelitian ini menyimpulkan tiga temuan utama. Pertama, kasus kebocoran data pada Tokopedia (91 juta), Bukalapak (13 juta), Indihome (279 juta), dan World App mencerminkan pelanggaran multidimensional terhadap lima prinsip kode etik ACM dan IEEE, yaitu Contribute to Society (1.1), Avoid Harm (1.2), Be Honest and Trustworthy (1.3), Respect Privacy (1.6), dan Give Comprehensive Evaluations (2.5). Pelanggaran ini bukan kelalaian teknis semata, melainkan kegagalan etika profesi yang sistemik.

Kedua, penerapan prinsip CIA Triad (Confidentiality, Integrity, Availability) bersama dengan kerangka kode etik ACM dan IEEE menjadi fondasi etis yang esensial dalam pelindungan data pribadi. CIA Triad menjadi titik temu antara aspek teknis Sistem Informasi dengan aspek etika profesi TI, di mana *Confidentiality* merepresentasikan komitmen moral terhadap privasi, *Integrity* merepresentasikan kejujuran profesional, dan *Availability* merepresentasikan tanggung jawab terhadap pengguna.

Ketiga, meskipun UU PDP No. 27 Tahun 2022 telah hadir sebagai payung hukum, komparasi dengan GDPR menunjukkan masih terdapat kelemahan implementatif terutama pada belum terbentuknya OPDP yang independen, absennya kewajiban *Privacy by Design*, dan terbatasnya yurisdiksi lintas negara. Kepatuhan hukum semata tidak cukup tanpa diiringi internalisasi nilai-nilai etika oleh praktisi TI. Etika pelindungan data pribadi merupakan investasi strategis yang fundamental bagi keberlanjutan ekosistem *e-commerce* di Indonesia.

Berdasarkan kesimpulan tersebut, beberapa saran dapat diajukan. Pelaku platform *e-commerce* perlu membangun budaya organisasi yang menempatkan etika dan keamanan data sebagai nilai inti, menerapkan prinsip *Security by Design* dan *Privacy by Design*, serta menunjuk pejabat pelaksana fungsi Pelindungan Data Pribadi sebagaimana diamanatkan Pasal 53 UU PDP. Pemerintah perlu mempercepat pembentukan OPDP yang independen dan mengakomodasi tantangan teknologi seperti AI dan biometrik. Institusi pendidikan perlu mengintegrasikan kode etik ACM/IEEE dalam kurikulum, sedangkan konsumen perlu meningkatkan literasi digital. Penelitian lanjutan disarankan menggunakan pendekatan empiris guna mengukur efektivitas implementasi *Privacy by Design* pada platform *e-commerce* nasional.

REFERENCES

Abdullah, C., Durand, N., & Moonti, R. M. (2025). Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022 di Era Big Data. *Amandemen: Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia*, *2*(3), 233–241. https://doi.org/10.62383/amandemen.v2i3.1073

Afip, Andy, S., C. P., & Pebriani, D. (2025). Analisis Insiden Kebocoran Data 91 Juta Akun Tokopedia: Dampak dan Upaya Penanganannya. *Integrative Perspectives of Social and Science Journal (IPSSJ)*, *2*(3), 4858–4865. https://ipssj.com/index.php/ojs/article/view/578

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 4, No. 3, Tahun 2026
ISSN 3024-8256 (media online)
Hal 518-525

Andari, A. S. S., & Nurmiati, E. (2026). Peran dan Tanggung Jawab Etis Profesional TI dalam Mencegah Kebocoran Data Privasi. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, *2*(3), 3856–3863. https://indojurnal.com/index.php/jejakdigital/article/view/2679

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://journal.pubmedia.id/index.php/lawjustice/article/view/3601

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

Diah, A. S., & Wiraguna, S. A. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. *Jurnal Kajian Hukum Dan Kebijakan Publik*, *2*(2), 1089–1096. https://jurnal.kopusindo.com/index.php/jkhkp/article/view/776

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. https://journal.ppmi.web.id/index.php/jismdb/article/view/3653

Halizah, E., Ismail, R., Mujsi, A. D., Riordan, F. E., & Augustia, A. E. (2025). Analisis Pelanggaran Etika Profesi TI dalam Kebocoran Data 279 Juta Pengguna Indihome: Studi Kasus Tanggung Jawab Perlindungan Data Pribadi Elsa. *TEKNOBIS : Teknologi, Bisnis Dan Pendidikan*, *3*(2), 278–282. https://www.jurnalmahasiswa.com/index.php/teknobis/article/view/3029

Harahap, A. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakeholder. *Jurnal Manajemen dan Pemasaran Digital (JMPD)*, *1*(2), 73–83. https://doi.org/10.38035/jmpd.v1i2.34

Institute of Electrical and Electronics Engineers. (2025). *IEEE Code of Ethics*. https://www.ieee.org/about/corporate/governance/p7-8.html

Judijanto, L., & Harsya, R. M. K. (2025). Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia. *Sanskara Hukum dan HAM*, *3*(3), 141–149. https://doi.org/10.58812/shh.v3i03.543

Matondang, K. A., Handani, T., Handayani, A., & Wati, F. (2025). Etika Bisnis dalam Perlindungan Data Pribadi Konsumen di Era Bisnis Digital: dalam Studi Literatur. *Jurnal Publikasi Sistem Informasi dan Manajemen Bisnis*, *4*(3), 551–565. https://doi.org/10.55606/jupsim.v4i3.5508

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. https://doi.org/10.47861/sammajiva.v1i3.336

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *12*(2), 261–279. http://dx.doi.org/10.33331/rechtsvinding.v12i2.1285

Rahmadani, N. O., Fitri, G. A., & Wiraguna, S. A. (2025). Perlindungan Data Pribadi sebagai Hak Asasi Manusia: Perspektif Hukum berdasarkan UU No. 27 Tahun 2022. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *5*(1), 712–719. https://doi.org/10.56799/peshum.v5i1.9219

Rahman, T. A., Azzahra, S. N., Oktaviani, E., Wibowo, D. K., & Augustia, A. E. (2025). Polemik Etika dan Privasi dalam Pengumpulan Data Biometrik World App. *TEKNOBIS : Jurnal Teknologi, Bisnis Dan Pendidikan*, *3*(2), 250–253. https://jurnalmahasiswa.com/index.php/teknobis/article/view/2984

Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, *3*(1), 73–84. https://doi.org/10.56370/jhlg.v3i1.173

Sari, D. N., Fauzi, A., Alya, S. N., Larasati, I., Sutrisna, K. R., Zami, S. I. Z., & Yunus, N. A. (2025). Analisis Penanganan Insiden Kebocoran Data Tokopedia dan Dampaknya terhadap Kepercayaan Publik. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, *2*(1), 6–14. https://doi.org/10.63217/orbit.v2i1.189

Tambunan, S. F. A., & Nasution, M. I. P. (2023). Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Melakukan Transaksi di E-Commerce. *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)*, *2*(1), 5–7. https://doi.org/10.47233/jemb.v2i1.915

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