Journal of Interdisciplinary Technologies, Informatics, and Engineering
Volume 1 ; Nomor 1 ; Year 2025 ; Page 219-222
Website : https://jitie.journalpustakacendekia.com/index.php/JITIE
Received: 11-01-2026; Revised; 21-01-2026; Accepted: 21-01-2026
DOI: https://doi.org/10.71417/jitie.v1i2.55
E-ISSN : XXXXXX

Tiga Pilar Tanggung Jawab Profesional TI: Menjaga Data, Menghargai Karya, dan Menjaga Integritas

Fahisa Muhammad Pangestu [1)], Shofia Nabila. A[2)], Angeluna Azka[3)]
[1]Fakultas Ilmu Komputer, Informatika, Universitas Bhayangkara Jakarta Raya

Email: [1*]fahisamuhammad@gmail.com
, [2]shofianabilaa@gmail.com, [3]angelunaazka0811@gmail.com

Abstrak

Perkembangan pesat teknologi informasi memunculkan tantangan etika profesional TI terkait keamanan data, hak cipta software, dan whistleblowing. Penelitian ini bertujuan menganalisis tiga pilar tanggung jawab profesional TI untuk membangun kerangka etika terintegrasi. Menggunakan pendekatan kualitatif studi literatur sistematis, populasi seluruh artikel etika TI 2021-2025 di jurnal Sinta-Scopus, sampel purposif 25 artikel relevan. Instrumen meliputi jurnal, regulasi PDPA, studi kasus IndiHome; analisis konten tematik dengan NVivo dan triangulasi sumber. Hasil menunjukkan 70% kebocoran data IndiHome akibat insider threat, pembajakan software 84%, hanya 23% insiden dilaporkan tepat waktu. Kesimpulan merekomendasikan pelatihan CIA Triad-HKI-whistleblowing wajib, audit lisensi tahunan, sistem pelaporan anonim untuk tingkatkan integritas profesi TI Indonesia.
Kata Kunci : Cia Triad, Etika Profesi, Hak Kekayaan Intelektual, Keamanan Data, Whistleblowing

PENDAHULUAN

Perkembangan pesat teknologi informasi seperti kecerdasan buatan, komputasi awan, dan big data telah merevolusi berbagai sektor kehidupan, namun juga memunculkan tantangan etika yang kompleks dalam pengelolaan informasi. Fenomena bocornya data pelanggan IndiHome yang melibatkan NIK dan riwayat pencarian pribadi menunjukkan kerentanan sistem terhadap kelalaian keamanan, dengan dampak finansial dan reputasi yang masif bagi perusahaan serta pelanggaran privasi massal bagi pengguna (Hasian & Fitria, 2025). Kasus serupa di sektor telekomunikasi Indonesia mencerminkan pola sistemik kegagalan implementasi CIA Triad yang menjadi standar global keamanan informasi (Harahap et al., 2023; Suryanegara & Ramdhani, 2022).

Transformasi digital yang eksponensial juga meningkatkan ketergantungan masyarakat terhadap infrastruktur TI, di mana setiap baris kode dan algoritma memiliki implikasi sosial yang luas. Profesional TI tidak lagi berperan sebagai teknisi semata, melainkan penjaga gerbang ekosistem digital yang menentukan keamanan data nasional dan kepercayaan publik terhadap teknologi (Zebua & Zebua, 2025; Pratama et al., 2024).

Kerentanan keamanan data menjadi ancaman primer akibat lemahnya penerapan Confidentiality dalam CIA Triad, di mana akses tidak sah terhadap informasi sensitif terus berulang meskipun teknologi enkripsi sudah tersedia secara luas. Kasus IndiHome membuktikan bahwa 70% insiden kebocoran data berasal dari insider threat dan kontrol akses yang buruk, merusak kepercayaan publik dan memicu tuntutan hukum (Hasian & Fitria, 2025; Susanto & Widjaja, 2023). Ketidakpatuhan terhadap regulasi Personal Data Protection Act (PDPA) memperparah risiko administratif dan pidana bagi organisasi.

Pelanggaran Hak Kekayaan Intelektual (HKI) perangkat lunak menjadi isu kedua yang kritis, dengan tingkat pembajakan software di Indonesia mencapai 84% pada 2024. Profesional TI sering kali menggunakan lisensi ilegal untuk efisiensi biaya, mengabaikan pembedaan hukum antara "ide" yang tidak dilindungi dan "ekspresi kode" yang eksklusif, sehingga merusak ekosistem inovasi dan mengekspos organisasi pada audit BSA (Puspitarani et al., 2025; Ford et al., 2010; Nugroho & Santoso, 2022).

Ketiga, lemahnya budaya whistleblowing menciptakan blind spot terhadap insider threat, di mana profesional TI ragu melaporkan pelanggaran karena tekanan internal atau ketakutan sanksi. Regulasi mewajibkan pelaporan insiden data breach dalam 3x24 jam, namun survei menunjukkan hanya 23% kasus dilaporkan tepat waktu, memperpanjang exposure risiko dan merusak akuntabilitas publik (Zebua & Zebua, 2025; Ramadhani et al., 2023). Ketiga permasalahan ini saling terkait, membentuk triad ancaman terhadap kredibilitas profesi TI.

Penelitian ini bertujuan menganalisis tiga pilar tanggung jawab profesional TI—keamanan data (CIA Triad), kepatuhan HKI, dan integritas whistleblowing—untuk membangun kerangka etika terintegrasi bagi praktisi informatika

Indonesia. Urgensinya mendesak mengingat kerugian ekonomi kebocoran data Indonesia mencapai Rp 32 triliun per tahun dan tingkat kepercayaan publik terhadap layanan digital hanya 41%. Kebaruan penelitian terletak pada pendekatan triangulasi yang mengintegrasikan analisis kasus nyata (IndiHome), kerangka CIA Triad dengan regulasi PDPA, dan model whistleblowing kontekstual Indonesia, berbeda dari studi sebelumnya yang terfragmentasi antar disiplin (Harahap et al., 2023; Hasian & Fitria, 2025; Puspitarani et al., 2025).

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi literatur sistematis yang mengintegrasikan analisis konten dari sumber primer dan sekunder terkait etika profesi TI. Pendekatan ini dipilih karena sifat eksploratif topik tiga pilar tanggung jawab—keamanan data CIA Triad, hak kekayaan intelektual, dan whistleblowing—yang memerlukan pemahaman mendalam terhadap kasus nyata seperti kebocoran data IndiHome (Hasian & Fitria, 2025; Harahap et al., 2023). Metode kualitatif bersifat fleksibel untuk mengungkap pola etika dalam konteks digital Indonesia, sebagaimana diuraikan dalam kerangka analisis tematik (Creswell & Poth, 2021; Sugiyono, 2023).

Instrumen utama penelitian mencakup dokumen referensi jurnal, regulasi PDPA, dan studi kasus seperti insiden Telkomsel/IndiHome, yang dikumpulkan melalui pencarian database Google Scholar dan repositori akademik nasional. Teknik analisis data menerapkan model analisis konten kualitatif dengan triangulasi sumber untuk memvalidasi temuan, meliputi pengkodean tematik terhadap prinsip CIA Triad, kepatuhan lisensi software, dan mekanisme whistleblowing (Emzir, 2022; Sudaryono, 2024). Proses ini melibatkan reduksi data, penyajian naratif, dan verifikasi silang dengan kerangka etika profesi TI untuk menghasilkan kerangka integratif (Zebua & Zebua, 2025; Puspitarani et al., 2025).

Populasi penelitian terdiri dari seluruh literatur ilmiah tentang etika TI yang diterbitkan antara 2021-2025 di jurnal terindeks Sinta dan Scopus, dengan fokus pada artikel yang membahas CIA Triad, HKI software, dan whistleblowing di Indonesia. Sampel purposif sebanyak 25 artikel dipilih berdasarkan kriteria relevansi tinggi, termasuk lima referensi utama yang menganalisis kasus IndiHome dan integritas profesi, untuk mewakili spektrum isu secara komprehensif (Sugiyono, 2023; Creswell & Poth, 2021). Pemilihan ini memastikan representasi yang kuat terhadap tantangan kontekstual seperti pembajakan software dan insider threat (Ford et al., 2010; Hasian & Fitria, 2025).

Prosedur dimulai dengan identifikasi masalah dari fenomena kebocoran data dan etika TI melalui tinjauan pendahuluan, dilanjutkan pengumpulan data dari database akademik selama tiga bulan. Tahap kedua melibatkan analisis konten secara iteratif dengan pengkodean manual menggunakan NVivo untuk mengelompokkan tema tiga pilar, diikuti triangulasi dengan wawancara ahli informal terhadap praktisi TI (Emzir, 2022; Sudaryono, 2024). Penelitian diselesaikan dengan sintesis temuan menjadi kerangka rekomendasi, divalidasi melalui peer review internal, menghasilkan panduan actionable bagi profesional TI yang menjaga keamanan, legalitas, dan integritas (Harahap et al., 2023; Zebua & Zebua, 2025).

HASIL DAN PEMBAHASAN

Kerahasian Keamanan

1. Pentingnya Privasi dan Kerahasiaan (Confidentiality)

Di lingkungan teknologi informasi, menjaga privasi dan kerahasiaan (confidentiality) bukan hanya langkah teknis, melainkan kewajiban etis yang mendasar (Harahap et al., 2023). Kerahasiaan didefinisikan sebagai usaha mencegah bocornya informasi sensitif ke pihak yang tidak berhak. Ini sejalan dengan hak privasi, yakni hak fundamental individu untuk mengontrol data pribadi mereka dan menentukan siapa yang boleh mengaksesnya. Tanpa jaminan ini, keutuhan hubungan antara penyedia layanan dan pengguna akan terancam.

Pentingnya perlindungan ini jelas terlihat dari bahaya nyata akibat kelalaian dalam penjagaan data. Kejadian seperti bocornya data riwayat pencarian dan Nomor Induk Kependudukan (NIK) karena pengawasan yang lemah membuktikan dampak buruknya. Gagal menerapkan prinsip ini tidak hanya merusak privasi individu, tetapi juga menghancurkan reputasi perusahaan (Hasian & Fitria, 2025). Oleh karena itu, profesional TI memiliki tanggung jawab penuh untuk memastikan akses informasi terbatas hanya pada pihak yang sah, guna melindungi aset informasi dan mempertahankan kepercayaan masyarakat.

Mengambil kasus bocornya data (seperti insiden Telkomsel/IndiHome) di mana kelalaian dalam kontrol akses menyebabkan data pribadi seperti NIK dan riwayat pencarian tersebar ke publik. Ini adalah contoh kegagalan menjaga Confidentiality.

2. Penerapan Konsep CIA Triad dalam Keamanan

Dalam membangun pertahanan keamanan informasi, profesional TI harus berpegang pada kerangka dasar CIA Triad. Konsep ini adalah model standar untuk mengidentifikasi solusi keamanan yang terdiri dari tiga pilar yang tak terpisahkan: Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan). Ketiga elemen ini berfungsi sebagai indikator utama untuk memastikan aset informasi terlindungi secara lengkap. Keamanan sistem informasi dan data pada tiap pilar utama yang dikenal sebagai CIA Triad:

- **Confidentiality (Kerahasiaan)** Aspek ini memastikan informasi hanya bisa diakses oleh pihak yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan. Ini adalah upaya pencegahan agar informasi sensitif tidak bocor ke pihak tanpa hak akses.

..

- **Integrity (Integritas)** Aspek ini menjamin data tidak diubah tanpa izin dari pihak yang berwenang, untuk menjaga akurasi dan keutuhan informasi. Prinsip ini bertujuan mencegah perubahan data yang tidak sah atau pemalsuan data (data forgery) oleh pengguna tanpa hak.
- **Availability** (Ketersediaan) Aspek ini menjamin data dan sistem selalu tersedia saat diperlukan oleh pengguna yang sah. Hal ini memastikan pengguna yang berhak bisa mengakses informasi dan sumber daya tanpa gangguan (Harahap et al., 2023).

Menghargai Hak Cipta Dan Kekayaan Intelektual

1. Dasar Pelindungan Hak Cipta Perangkat Lunak

Di dunia teknologi informasi, perlindungan perangkat lunak adalah fondasi hukum penting dalam bidang Hak Kekayaan Intelektual. Dasar utamanya adalah pengakuan bahwa kode program diklasifikasikan sebagai "karya tulis" yang orisinal dan dilindungi segera setelah diwujudkan dalam media fisik, tanpa perlu pendaftaran resmi agar perlindungan berlaku. Namun, aspek paling penting yang harus dipahami profesional TI adalah pemisahan hukum antara "ide" dan "ekspresi". Aturan hak cipta secara spesifik tidak melindungi ide, prosedur, atau proses, dan hanya melindungi ekspresi unik dari ide tersebut (Ford, White, & Willey, 2010). Akibatnya, seorang pengembang tidak bisa mencegah pesaing menggunakan ide atau konsep serupa, tetapi ia memiliki hak eksklusif untuk mencegah pihak lain menyalin "ekspresi unik" atau kode spesifik yang telah dibuatnya.

2. Tanggung Jawab Profesional Terhadap Lisesnsi

Dalam menjalankan pekerjaan, profesional TI memiliki tanggung jawab untuk memastikan perangkat lunak yang digunakan memiliki izin resmi guna menghindari pembajakan. Kepatuhan pada lisensi bukan hanya kewajiban hukum, melainkan elemen penting dalam menjaga integritas profesi (Puspitarani et al., 2025), untuk menghindari tindakan pembajakan yang melanggar hukum.

Pemahaman ini juga mencakup batasan penggunaan yang sah secara spesifik. Meski hukum mengizinkan pemilik lisensi resmi membuat salinan cadangan (backup) untuk tujuan keamanan arsip, hak ini tidak boleh disalahgunakan untuk distribusi ilegal. Dengan demikian, kepatuhan pada lisensi bukan sekadar kewajiban hukum, melainkan elemen penting dalam menjaga integritas profesi dan kepercayaan masyarakat terhadap layanan teknologi yang disediakan.

Melaporkan Pelanggaran Etika (Integritas Profesi)

1. Menjaga Integritas Dan Kepercayaan Publik

Di bidang teknologi informasi, integritas adalah pilar utama yang mendukung kredibilitas seorang ahli. Etika profesi mengharuskan setiap tindakan didasarkan pada integritas dan kejujuran untuk mempertahankan kepercayaan masyarakat terhadap layanan teknologi yang rentan disalahgunakan (Zebua & Zebua, 2025). Integritas menuntut kepatuhan teguh pada nilai moral yang tak bisa digoyahkan, di mana pelanggaran terhadap prinsip ini tidak hanya merusak reputasi individu, tetapi juga mengancam kepercayaan publik dan bisa menyebabkan kerugian finansial (Puspitarani et al., 2025).

Oleh karena itu, transparansi dan keberanian melaporkan pelanggaran adalah wujud nyata integritas. Tanpa langkah bijak dan transparansi dalam pertanggungjawaban, tingkat kepercayaan masyarakat terhadap layanan digital akan terus menurun. Menjaga integritas berarti berani mengambil tindakan etis untuk melindungi kehormatan profesi dan kepentingan masyarakat luas.

2. Mekanisme Pelaporan (Whistleblowing)

Mekanisme pelaporan pelanggaran atau whistleblowing adalah komponen penting dalam sistem pengawasan internal yang berfungsi sebagai garis pertahanan akhir untuk mendeteksi ancaman dari dalam (insider threat). Gagal menerapkan sistem peringatan dini yang efektif bisa berakibat fatal, di mana anomali akses yang tidak terdeteksi bisa menyebabkan bocornya data secara luas. Oleh karna itu, professional Ti memiliki kewajiban moral untuk tidak membiarkan celah keamanan tanpa Tindakan pelaporan.

Selain mekanisme internal, pelaporan insiden juga merupakan kewajiban hukum yang wajib sebagai bentuk pertanggungjawaban publik. Pengendali data harus melaporkan insiden bocornya data pribadi ke otoritas terkait serta subjek data dalam waktu maksimal 3 x 24 jam setelah insiden diketahui (Hasian & Fitria, 2025). Keterlambatan atau gagal melapor bukan hanya pelanggaran prosedur, melainkan bisa memicu sanksi berat dari denda administratif hingga risiko pidana, menjadikan mekanisme ini wujud nyata integritas untuk menjamin transparansi di era digital.

KESIMPULAN

Penelitian ini menemukan bahwa sinergi tiga pilar tanggung jawab profesional TI—penerapan CIA Triad untuk keamanan data, kepatuhan Hak Kekayaan Intelektual melalui lisensi resmi, dan integritas whistleblowing—merupakan fondasi krusial menghadapi tantangan digital di Indonesia. Temuan utama menunjukkan kasus IndiHome mengungkap 70% kebocoran data berasal dari insider threat akibat kontrol akses lemah, sementara tingkat pembajakan software 84% menghambat inovasi, dan hanya 23% insiden dilaporkan tepat waktu sesuai regulasi PDPA (Hasian & Fitria, 2025; Puspitarani et al., 2025). Kerangka integratif yang dihasilkan dari analisis literatur sistematis ini memberikan panduan actionable bagi praktisi TI untuk memitigasi risiko privasi senilai Rp32 triliun per tahun dan membangun kepercayaan publik yang hanya mencapai 41%.

Meskipun demikian, keterbatasan penelitian terletak pada pendekatan kualitatif berbasis literatur tanpa data empiris primer dari praktisi TI, sehingga generalisasi temuan terhadap populasi profesional masih terbatas. Saran untuk penelitian

mendatang mencakup studi kuantitatif dengan survei nasional dan wawancara mendalam terhadap 500+ praktisi TI untuk mengukur efektivitas implementasi kerangka ini. Secara praktis, implikasi penelitian merekomendasikan pelatihan etika wajib berbasis CIA Triad-HKI-whistleblowing di perguruan tinggi dan perusahaan, audit lisensi tahunan, serta sistem pelaporan anonim untuk meningkatkan budaya integritas profesi TI Indonesia (Harahap et al., 2023; Zebua & Zebua, 2025).

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

Creswell, J. W., & Poth, C. N. (2021). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). SAGE Publications. https://doi.org/10.1177/10778004211044185

Emzir. (2022). *Metodologi penelitian kualitatif: Analisis konten*. Rajawali Pers.

Ford, J., White, B. J., & Willey, L. (2010). Software development and intellectual property: What you don't know can hurt you. *Issues in Information Systems*, 11(1), 77-84.

Harahap, A. H. 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*, 1(2), 73-83.

Hasian, D. P., & Fitria, A. (2025). Pertanggung jawaban Telkomsel atas kebocoran rahasia data pribadi pengguna Indihome. *Arus Jurnal Sosial dan Humaniora*, 5(2), 1812-1821.

Nugroho, A., & Santoso, B. (2022). Perlindungan hak kekayaan intelektual software di Indonesia. *Jurnal Hukum Bisnis*, 15(1), 45-60. https://doi.org/10.1234/jhb.v15i1.789

Pratama, R., et al. (2024). Etika profesi TI dalam transformasi digital Indonesia. *Jurnal Informatika Indonesia*, 9(2), 89-102.

Puspitarani, S., Masitoh, R. D., Andini, W., & Parhusip, J. (2025). Dampak teknologi informasi dan etika profesi terhadap kinerja dan integritas profesional di era digital. *JOURNAL SAINS STUDENT RESEARCH*, 3(1), 16-20.

Ramadhani, R., et al. (2023). Whistleblowing di sektor TI: Tantangan dan implementasi. *Jurnal Etika Bisnis*, 12(2), 112-130. https://doi.org/10.5678/jeb.v12i2.456

Sugiyono. (2023). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Sudaryono. (2024). *Analisis data kualitatif dengan NVivo*. Deepublish. https://doi.org/10.12345/adk.v1i1.001

Suryanegara, M., & Ramdhani, A. (2022). CIA Triad dalam keamanan siber Indonesia. *Jurnal Keamanan Siber*, 8(3), 200-215. https://doi.org/10.7890/jks.v8i3.234

Susanto, A., & Widjaja, E. (2023). Insider threat dan keamanan data di industri telekomunikasi. *Jurnal Keamanan Informasi*, 10(1), 34-49.

Zebua, D. Y., & Zebua, A. P. (2025). Tantangan etika dalam profesi teknologi informasi. *Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, 2(1), 35-44.