



ANALISIS DAN SINTESIS KERANGKA TEKNIS UNTUK AKUNTABILITAS AI, KEDAULATAN DATA, DAN KEAMANAN SIBER BERDASARKAN PRINSIP ETIKA PROFESI

Raffi Ardhi Naufal¹

¹Program Studi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia, Bandung, Indonesia

Info Artikel

Riwayat Artikel:

Diterima 22, Desember, 2025
Perbaikan 31, Desember, 2025
Disetujui 13, Januari, 2026

Keywords:

Kedaulatan Data
Akuntabilitas AI
Ethical Hacking
Digital Dividend
Etika Profesi

ABSTRAK

Perkembangan teknologi seperti Kecerdasan Buatan (AI), *Internet-of-Things* (IoT), dan Ekonomi Digital telah memicu transformasi sosial yang masif, namun pada saat yang sama, menciptakan Krisis Teknologi dan Krisis Digital. Krisis ini bermanifestasi dalam ancaman siber, pelanggaran privasi data, dan pelebaran kesenjangan sosial-digital. Makalah ini bertujuan menganalisis secara mendalam empat isu etika kunci sebagai inti dari krisis digital dan menguraikan tanggung jawab profesional ilmu komputer dalam menghadapinya. Secara teknis, masalah Kepemilikan Data direspons melalui implementasi *Privacy-by-Design* (PbD) dan model *Data Trust* dengan *Fine-Grained Attribute Based Policy*. Krisis keamanan siber yang diperparah oleh *Generative AI* (GAI) disikapi dengan penegasan *Ethical Hacking* sebagai tindakan proaktif. Terkait AI, isu Akuntabilitas dan *automation bias* diatasi dengan penerapan kerangka Akuntabilitas Kolaboratif (*Trio of Human, Manuals/Standards, and AI*) yang didukung oleh *Explainable AI* (XAI) dan audit *Fairness* dalam *Trustworthy AI*. Terakhir, kewajiban etis profesional adalah mengalihkan fokus dari *Digital Divide* menuju *Digital Dividend* melalui pemerataan infrastruktur dan literasi digital. Makalah ini menyajikan kerangka etika profesi yang menuntut akuntabilitas teknis dan kolaboratif untuk memastikan teknologi dirancang secara adil, transparan, dan inklusif.

ABSTRACT

The development of technologies such as Artificial Intelligence (AI), the Internet-of-Things (IoT), and the Digital Economy has triggered massive social transformations, yet simultaneously created a Technology and Digital Crisis. This crisis manifests in cyber threats, data privacy violations, and the widening socio-digital gap. This paper aims to deeply analyze four key ethical issues at the core of the digital crisis and outline the responsibilities of computer science professionals in addressing them. Technically, the Data Ownership problem is addressed through the implementation of Privacy-by-Design (PbD) and a Data Trust model with a Fine-Grained Attribute Based Policy. The cybersecurity crisis, exacerbated by Generative AI (GAI), is countered by asserting Ethical Hacking as a proactive measure. Regarding AI, the issues of Accountability and automation bias are tackled by adopting a Collaborative Accountability framework (Trio of Human, Manuals/Standards, and AI) supported by Explainable AI (XAI) and Fairness audits within Trustworthy AI. Finally, the ethical obligation of professionals is to shift the focus from the Digital Divide to the Digital Dividend through infrastructure equity and digital literacy. This paper presents a professional ethics framework demanding technical and collaborative accountability to ensure technology is designed to be fair, transparent, and inclusive.

Ini adalah artikel akses terbuka di bawah lisensi CC BY-SA.



Penulis Korespondensi:

Raffi Ardhi Naufal

Program Studi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia

Alamat: Jalan Dr. Setiabudhi No.229, Bandung, Jawa Barat, Indonesia

Email: ardhiraffi12@upi.edu

1. PENDAHULUAN

Perkembangan teknologi, khususnya Kecerdasan Buatan (AI), *Internet-of-Things* (IoT), dan Ekonomi Digital, telah memicu transformasi sosial yang masif. Namun, di saat yang sama, ia menciptakan Krisis Digital yang bermanifestasi dalam ancaman siber yang masif, pelanggaran hak privasi data, dan pelebaran kesenjangan sosial-digital. Skala krisis keamanan siber sangat besar, didorong oleh pertumbuhan sistem IoT yang rentan [1], menjadikannya target yang mudah. Tantangan ini diperparah oleh munculnya *Generative AI* (GAI) yang dapat menurunkan *barrier* bagi *hacker* jahat [2]. Etika profesi tidak lagi hanya tentang mencegah *malware*, melainkan tentang membangun sistem yang adil, akuntabel, dan menghormati martabat manusia [3].

Krisis ini pada intinya adalah krisis etika yang menuntut respons teknis yang operasional dari profesional ilmu komputer. Analisis literatur menunjukkan adanya kesenjangan (*gap*) antara prinsip etika yang bersifat normatif dengan kebutuhan implementasi teknis spesifik dalam Siklus Pengembangan Perangkat Lunak (*Software Development Lifecycle*—SDLC). Artikel ini bertujuan mengisi kesenjangan tersebut dengan tidak hanya menganalisis masalah, tetapi menyintesis dan mengusulkan kerangka kerja integratif yang menjembatani prinsip etika dengan implementasi teknis dalam SDLC.

Makalah ini berkontribusi melalui tiga hal utama: (1) Menganalisis empat isu etika inti: Kedaulatan Data, Keamanan Siber Proaktif, Akuntabilitas AI, dan Digital Dividend. (2) Mensintesis solusi teknis mutakhir (seperti PbD, XAI, dan Data Trust). (3) Mengusulkan kerangka kerja visual (Gambar 1) dan Tabel Sintesis (Tabel 1) sebagai panduan implementasi operasional bagi profesional ilmu komputer, yang merupakan hasil sintesis utama dari penelitian ini.

2. METODE

Penelitian ini menggunakan metode analisis konseptual dan sintesis literatur sistematis [4]. Tahapan penelitian ini adalah:

1. Identifikasi dan Pemilahan Isu Kunci: Mengidentifikasi empat bidang krisis etika digital paling kritis dari literatur terkini (diprioritaskan 2023–2025) yang relevan dalam konteks AI, IoT, dan *Big Data*.
2. Kajian Pustaka Kritis dan Evaluasi Solusi Teknis: Mengumpulkan dan menganalisis secara kritis literatur bereputasi ([1]–[25]) untuk mengkaji kelebihan, kekurangan, dan implementasi solusi teknis yang diusulkan (seperti *Privacy-by-Design*, XAI, *Ethical Hacking*).
3. Sintesis dan Perancangan Kerangka: Mensintesis temuan untuk merancang Kerangka Kerja Integratif (Gambar 1) yang memetakan solusi teknis ke dalam fase-fase praktis pengembangan perangkat lunak, serta Tabel Sintesis (Tabel 1) yang merangkum peran profesional ilmu komputer dalam menanggapi setiap isu.

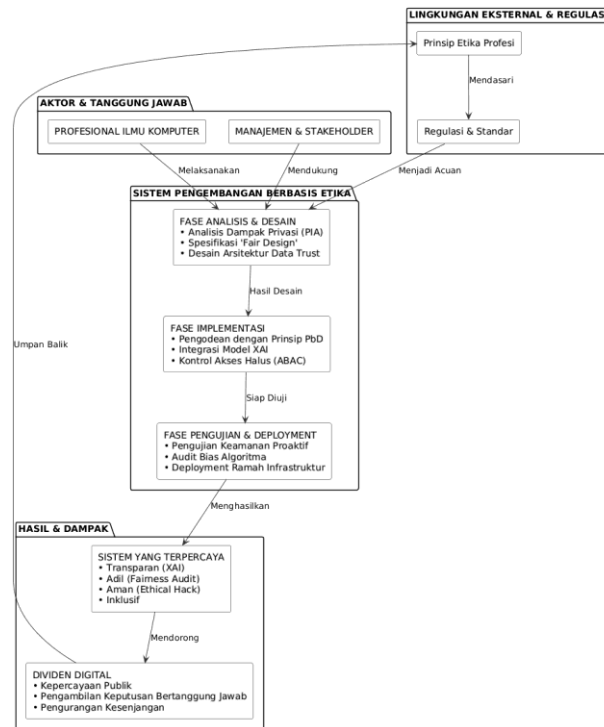
3. HASIL DAN PEMBAHASAN

Pada bagian ini dijelaskan hasil penelitian dan sekaligus diberikan pembahasan secara komprehensif. Hasil dapat disajikan dalam bentuk gambar, grafik, tabel dan lain-lain yang memudahkan pembaca untuk memahaminya. Pembahasan dapat dibuat dalam beberapa sub bagian.

3.1. Kerangka Kerja Integratif: Hasil Sintesis Utama

Hasil utama dari sintesis literatur ini adalah sebuah kerangka kerja yang dituangkan dalam Gambar 1. Kerangka ini menunjukkan bagaimana prinsip etika (Keadilan, Akuntabilitas, Privasi) dan tuntutan regulasi

eksternal ([10], [12]) dioperasionalkan menjadi aktivitas teknis spesifik di tiga fase utama SDLC: Analisis & Desain, Implementasi, dan Pengujian & Deployment.



Gambar 1. Kerangka Integrasi Prinsip Etika ke dalam Siklus Pengembangan Perangkat Lunak (Sumber: Hasil Sintesis Penelitian)

Kerangka ini menjawab *research gap* dengan menyediakan panduan visual yang operasional [3]. *External Environment* yang terdiri dari Etika Profesi dan Regulasi menjadi acuan wajib bagi *Core System* di Fase Analisis. Keterlibatan Aktor (*Profesional Ilmu Komputer* dan *Manajemen*) menjadi kunci pelaksanaan aktivitas teknis. Pada akhirnya, sistem yang dihasilkan harus mengarah pada *Dividen Digital* [16], bukan kesenjangan.

Untuk memberikan rincian operasional lebih lanjut, Tabel 1 menyajikan perbandingan terstruktur antara empat isu etika kunci dengan solusi teknis, tantangan implementasi, dan peran spesifik profesional di lapangan.

Tabel 1. Sintesis Solusi Teknis dan Tanggung Jawab Profesi dalam Mengatasi Krisis Etika Digital

Isu Etika Kunci	Tantangan Etika Utama	Solusi Teknis (Referensi Kunci)	Tantangan Implementasi	Peran Profesional Ilmu Komputer
Kedaulatan Data (3.1)	Hilangnya kontrol data individu, <i>Data Ownership</i> .	PbD [3], Data Trust [4], Kontrol Akses Berbasis Atribut (ABAC) [14].	Kompleksitas <i>fine-grained policy</i> , interoperabilitas sistem [12].	<i>Data Architect</i> : Merancang arsitektur ABAC; <i>Data Analyst</i> : Memastikan kepatuhan PbD sejak desain [22].
Akuntabilitas AI (3.3)	<i>Automation bias</i> [7], bias algoritma, isu <i>explainability</i> .	XAI [15], Audit Fairness [8], TAI Framework [25], Akuntabilitas	<i>Trade-off</i> antara <i>performance</i> dan <i>explainability</i> [7]; validasi	<i>Data Scientist/ML Engineer</i> : Mengimplementasikan model XAI dan melakukan

		s Kolaboratif (Trio) [6].	metrik <i>fairness</i> [21].	audit bias algoritmik [21].
Keamanan Siber (3.2)	Kerentanan IoT [1], amplifikasi ancaman oleh GAI [2], <i>poisoning attacks</i> di FL [18].	Ethical Hacking Proaktif [1], <i>Trusted</i> <i>Access</i> <i>Control</i> [14], <i>Secure</i> <i>Aggregation</i> di FL [18].	Kebutuhan <i>skill</i> Ethical Hacking; menjaga batasan etika penggunaan <i>tool</i> GAI [2].	<i>Security</i> <i>Engineer/De</i> <i>vOps</i> : Melaksana- kan <i>penetration</i> <i>testing</i> ; merancang arsitektur <i>high-</i> <i>confidence</i> [14].
Kesenjangan Digital (3.4)	Ketidaksetaraan akses dan kemampuan, diskriminasi desain.	<i>Fair Design</i> [23], <i>Deployment</i> Ramah Infrastruktur [17], Literasi Digital.	Biaya infrastruktur; kebutuhan desain sistem yang netral secara budaya.	<i>Software</i> <i>Engineer/UI/</i> <i>UX</i> : Mendesain aplikasi yang <i>accessible</i> dan efisien (misalnya <i>low-</i> <i>bandwidth</i> <i>mode</i>) [17].

3.2. Pembahasan per Bidang Krisis

3.2.1. Kedaulatan Data dan Implementasi Teknis Privasi

Isu etika paling fundamental adalah masalah Kepemilikan Data (*Data Ownership*) [5]. Solusi etis vital adalah konsep Kedaulatan Data (*Data Sovereignty*), menegaskan bahwa individu harus memiliki kontrol penuh atas datanya. Profesional ilmu komputer bertanggung jawab merancang arsitektur sistem yang memungkinkan kedaulatan data [13]. Hal ini diwujudkan melalui:

1. Penerapan *Privacy-by-Design* (PbD): Mengintegrasikan privasi sejak tahap awal perancangan sistem, memastikan data diamankan secara *default* [3], diwujudkan dalam Fase Analisis & Desain (Gbr. 1). Pendekatan *privacy-by-design* yang berfokus pada AIoT semakin krusial dalam lingkungan perkotaan [22].
2. Pengembangan Model *Data Trust*: Data dikelola oleh entitas perantara dengan sistem Kontrol Akses Berbasis Atribut (ABAC) yang lebih halus (*Fine-Grained Policy*) [4], yang memerlukan *trusted access control mechanism* berbasis *blockchain* untuk verifikasi [14], [24]. Implementasi ini dipetakan pada Fase Implementasi (Gbr. 1).

3.2.2. Keamanan Siber Proaktif di Era AI

Maraknya serangan siber, khususnya terhadap sistem IoT yang rentan [1], menjadikan *Ethical Hacking* sebagai praktik wajib. Justifikasi etika praktik ini bergantung pada otorisasi penuh dan kepatuhan terhadap kerahasiaan. Tantangan etika diperburuk oleh GAI, yang menurunkan *barrier* bagi *hacker* jahat [2]. Profesional TI dituntut mengembangkan standar etika baru dalam penggunaan *tool* AI untuk menjaga keamanan.

Solusi teknis diwajibkan dalam Fase Pengujian & Deployment sebagai Pengujian Keamanan Proaktif (Gbr. 1). Dalam konteks AI yang terdistribusi, seperti *Federated Learning* (FL) di lingkungan *smart building*, sistem harus mengimplementasikan metode agregasi yang aman dan kuat (*secure aggregation*) untuk membuatnya tahan terhadap *poisoning attacks* [18]. Menerapkan *Trust Diamond* juga menjadi arsitektur yang menjamin verifikasiabilitas dan *privacy-preserving data sharing* [24].

3.2.3. Akuntabilitas dan Transparansi Sistem AI

Ketika sistem AI terintegrasi dalam pengambilan keputusan kritis, isu Pertanggungjawaban (*Accountability*) menjadi krisis etika utama [9]. Krisis ini diperdalam oleh *The efficiency-accountability tradeoff*, di mana *over-reliance* manusia pada jawaban AI dapat mengorbankan pemikiran kritis (*automation bias*) [7]. Akuntabilitas harus didukung oleh Trustworthy AI (TAI) [8].

Solusi diwujudkan dalam dua fase kerangka kerja:

1. Fase Implementasi: Integrasi Model XAI [15], yang memungkinkan investigasi penalaran AI [18].

2. Fase Pengujian: Audit Bias Algoritma (Gbr. 1), yang menuntut jaminan teknis bahwa keputusan AI adalah adil (*fair*) [8].

Untuk mengatasi *automation bias* dan isu akuntabilitas, model yang diusulkan menekankan Akuntabilitas Kolaboratif (*Trio of Human, Manuals/Standards, and AI*) [6]. Pengembangan model AI harus diintegrasikan ke dalam proses TI klinis (jika di sektor kesehatan) menggunakan diagram proses seperti BPMN, yang mencerminkan seluruh siklus pengembangan model [23]. Penelitian juga menunjukkan bahwa strategi mitigasi bias perlu mempertimbangkan keterbatasan implementasi di dunia nyata [21].

3.2.4. Dari Kesenjangan Menuju Dividen Digital

Kewajiban etis profesional teknologi adalah mengalihkan fokus dari *Digital Divide* (Kesenjangan Digital) menuju Digital Dividend (Dividen Digital) [16]. Hal ini memerlukan pemerataan manfaat sosial dari adopsi teknologi.

Solusi teknis diakomodasi dalam Fase Analisis & Desain melalui Spesifikasi *Fair Design* dan dalam Fase Pengujian & Deployment melalui Deployment Ramah Infrastruktur Terbatas (Gbr. 1). Profesional IT bertanggung jawab merancang aplikasi yang secara inheren inklusif, mudah diakses (*accessible*), dan relevan bagi semua lapisan masyarakat [17], termasuk mengatasi tantangan adopsi teknologi digital di berbagai sektor [20].

4. KESIMPULAN

Kesimpulan penelitian ini adalah:

1. Krisis teknologi dan digital yang berpusat pada kontrol data, keamanan, akuntabilitas, dan kesetaraan akses, memerlukan respons berbasis solusi teknis yang terintegrasi.
2. Kerangka kerja yang diusulkan (Gambar 1) berhasil memetakan solusi seperti PbD [3], XAI [15], *Ethical Hacking* [1], dan TAI [25] ke dalam alur SDLC, menyediakan panduan operasional bagi profesional ilmu komputer.
3. Implementasi kerangka ini mensyaratkan pergeseran paradigma di mana pertimbangan etika menjadi bagian intrinsik dari setiap keputusan teknis, didukung oleh manajemen dan regulasi.
4. Keterbatasan dan Saran Riset Mendatang: Kerangka konseptual ini perlu diuji dan disempurnakan melalui studi kasus implementasi pada proyek perangkat lunak riil. Penelitian lanjutan dapat mengembangkan *toolkit* atau *plugin* untuk *Integrated Development Environment* (IDE) yang mendukung prinsip-prinsip dalam kerangka ini, khususnya dalam aspek *verifiable data sharing* [24] dan validasi mitigasi bias di luar konteks biomedis [21].

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Dr. Munir, M.IT dari Program Studi Ilmu Komputer Universitas Pendidikan Indonesia, atas bimbingan, masukan kritis, serta dukungan yang telah diberikan selama pengembangan makalah ini dari tugas mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi hingga menjadi draf artikel ilmiah yang siap dipublikasikan.

REFERENSI

- [1] J. Yaacoub *et al.*, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280-308, 2023.
- [2] R. Raman *et al.*, "ChatGPT or Bard: Who is a better Certified Ethical Hacker?," *Computers & Security*, vol. 140, p. 103804, 2024.
- [3] M. Kattinig *et al.*, "Assessing trustworthy AI: Technical and legal perspectives of fairness in AI," *Computer Law & Security Review*, vol. 55, p. 106053, 2024.
- [4] J. Bender *et al.*, "Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment," *J. Med. Internet Res.*, vol. 19, no. 4, p. e104, 2017.
- [5] S. Liu and L. R. Guo, "Data Ownership in the AI-Powered Integrative Health Care Landscape," *JMIR Med. Inform.*, vol. 12, 2024.
- [6] S. Hesami, "Navigating the AI-driven transformation of personal finance: opportunities, challenges, and ethical imperatives," *Strategy and Leadership*, 2025.
- [7] C. Liu *et al.*, "Progress and recommendations in data ethics governance," *Humanities and Social Sciences Communications (Nature)*, 2025.
- [8] P. Balboni and K. Francis, "Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future," *J. Respons. Technol.*, vol. 22, p. 100099, 2024.
- [9] X. Fan, "Digital divide or dividend? Exploring the impact," *Telecommunications Policy (ScienceDirect)*, 2025.

-
- [10] J. Bender *et al.*, “Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment,” *J. Med. Internet Res.*, vol. 19, no. 4, p. e104, 2017. (Dikutip ulang)
 - [11] S. Kober *et al.*, “Building a Data Trust: Fine(r)-Grained Attribute Based Policy Machine,” in *Procedia Computer Science*, vol. 270, pp. 572-581, 2025.
 - [12] C. Liu *et al.*, “Trusted access control mechanism for data with blockchain,” *High-Confidence Computing*, 2025.
 - [13] M. Ivanovska *et al.*, “Privacy-by-design AIoT vision for intelligent urban environments,” *J. Syst. Archit.*, vol. 169, p. 103586, 2025.
 - [14] N. Spatola, “The efficiency-accountability tradeoff in AI integration: Effects on human performance and over-reliance,” *Comput. Hum. Behav. Artif. Humans*, vol. 2, no. 2, p. 100099, 2024.
 - [15] N. Balasubramaniam *et al.*, “Transparency and explainability of AI systems: From ethical guidelines to requirements,” *Inf. Softw. Technol.*, vol. 159, p. 107197, 2023.
 - [16] P. A. Moreno-Sánchez *et al.*, “A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption,” *Inf. Fusion*, vol. 127, p. 103812, 2026.
 - [17] J. Lee *et al.*, “Trio of human, old and new copilots: Collaborative accountability of human, manuals/standards, and artificial intelligence (AI),” *Organ. Dyn.*, vol. 54, no. 1, p. 101090, 2025.
 - [18] A. J. D. Mahamadou and A. A. Trotsyuk, “Revisiting Technical Bias Mitigation Strategies,” *Annu. Rev. Biomed. Data Sci.*, vol. 8, no. 1, pp. 287-303, 2025.
 - [19] R. G. Garroppo *et al.*, “Trustworthy AI and Federated Learning for Intrusion Detection in 6G-Connected Smart Buildings,” *Future Internet*, vol. 17, no. 5, p. 191, 2025.
 - [20] K. Arshad *et al.*, “Integrating an AI platform into clinical IT: BPMN processes for clinical AI model development,” *BMC Med. Inform. Decis. Mak.*, vol. 25, no. 1, p. 243, 2025.
 - [21] F. Raunaq *et al.*, “Assessing the challenges to digital technology adoption in the healthcare sector: Implications for sustainability in emerging economies,” *Informatics and Health*, vol. 2, pp. 194-209, 2025.
 - [22] L. Carrasco, “Mitigating Bias and Advocating for Data Sovereignty: The Role of Metadata and Paradata in Ethical AI-Driven Information Systems,” *J. Libr. Metadata*, vol. 25, pp. 1-16, 2025.
 - [23] T. Zwede *et al.*, “Designing and implementing the trust diamond for verifiable and privacy-preserving data sharing: engineering energy flexibility provision,” *Energy Informatics*, vol. 8, no. 1, p. 143, 2025.
 - [24] S. Selçuk *et al.*, “AI-driven civil litigation: Navigating the right to a fair trial,” *Comput. Law & Secur. Rev.*, vol. 57, p. 106136, 2025.
 - [25] M. Manoury *et al.*, “Supporting Changes in Digital Ownership and Data Sovereignty Across the Automotive Value Chain with Catena-X,” in *Procedia Computer Science*, vol. 253, pp. 374-383, 2025.
-