

Peran Etika Profesi Teknologi Informasi dalam Penanggulangan Kejahatan Siber di Indonesia

De Karl Azzahra¹, Evy Nurmiati²

^{1,2}Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
surel: ¹de.karl24@mhs.uinjkt.ac.id, ²evy.nurmiati@uinjkt.ac.id

Info Artikel

Sejarah artikel:

Diterima 15-06-2026

Revisi 11-07-2026

Diterima 07-08-2026

Kata kunci:

Etika Profesi
Kejahatan Siber
UU ITE
Keamanan Data
Kerangka PAPA

ABSTRAK

Percepatan digitalisasi di Indonesia menghadirkan beragam kemudahan, tetapi sekaligus memperluas ruang terjadinya kejahatan siber, mulai dari penyanderaan data (ransomware) pada infrastruktur nasional, kebocoran data berskala besar di sektor keuangan dan kesehatan, hingga penipuan yang mengeksploitasi manipulasi psikologis pengguna. Meskipun penguatan aspek teknis terus diupayakan, manusia yang mengelola sistem tetap menjadi titik paling rentan. Bertolak dari persoalan tersebut, penelitian ini mengkaji sejauh mana etika profesi bidang teknologi informasi (TI) dapat berperan sebagai upaya preventif terhadap kejahatan siber di Indonesia. Penelitian menggunakan metode studi kepustakaan (library research) dengan pendekatan kualitatif deskriptif, menelaah sumber primer berupa UU No. 1 Tahun 2024 tentang ITE serta sumber sekunder berupa artikel jurnal, buku, dan publikasi ilmiah lain yang relevan. Hasil analisis menunjukkan bahwa modus kejahatan siber yang menonjol, seperti phishing, kebocoran data, dan ancaman dari orang dalam (insider threat), umumnya berakar pada diabaikannya nilai-nilai etis, yaitu integritas, kerahasiaan, dan akuntabilitas. Oleh karena itu, penerapan etika profesi, khususnya melalui kerangka PAPA (Privacy, Accuracy, Property, Accessibility) dan kepatuhan pada kode etik, menjadi lapis pertahanan preventif yang memperkuat keamanan digital. Penelitian ini menyimpulkan bahwa keselarasan antara regulasi (UU ITE) dan penghayatan etika profesi merupakan kunci untuk menjaga kedaulatan data sekaligus mewujudkan ruang digital yang lebih aman.

Penulis yang sesuai:

De Karl Azzahra

Program Studi Sistem Informasi Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Email: de.karl24@mhs.uinjkt.ac.id

1. PENDAHULUAN

Selama kurang lebih dua dekade terakhir, kemajuan teknologi informasi dan komunikasi mengubah wajah kehidupan masyarakat Indonesia secara mendasar. Digitalisasi kini menyentuh sektor-sektor penting:



pemerintahan bergerak menuju *e-government*, industri perbankan dan keuangan bertumpu pada sistem elektronik, serta layanan publik makin terhubung secara daring [1]. Akses informasi yang makin mudah, biaya yang hemat, dan transaksi yang cepat adalah keuntungan nyata dari revolusi digital. Sayangnya, kemajuan yang sama turut memunculkan celah kerentanan baru yang rumit, terutama berupa kejahatan siber yang mengancam keamanan data dan kedaulatan informasi nasional [1], [2].

Rentetan insiden siber skala besar dalam beberapa tahun terakhir menunjukkan bahwa Indonesia berada dalam situasi yang kritis. Sebagai contoh, serangan *ransomware* Brain Cipher terhadap Pusat Data Nasional (PDN) pada pertengahan 2024 berdampak jauh melampaui gangguan layanan publik: peristiwa itu memperlihatkan rapuhnya infrastruktur digital negara sekaligus mengancam kedaulatan datanya [3]. Sektor keuangan mengalami hal serupa ketika sistem Bank Syariah Indonesia (BSI) diretas pada 2023 dan lebih dari 1,5 TB data nasabah tersebar, sehingga kepercayaan publik terhadap perbankan digital menurun [4]. Di sektor kesehatan, bocornya sekitar 279 juta data peserta BPJS Kesehatan pada 2021 menegaskan lemahnya tata kelola atas informasi sensitif warga [5]. Selain serangan berteknologi tinggi, praktik *phishing* dan rekayasa sosial (*social engineering*) yang memanfaatkan kelalaian serta minimnya pemahaman pengguna juga kian marak. Pola ini menempatkan manusia sebagai mata rantai terlemah dalam keamanan siber [6], sekaligus menandai pergeseran kejahatan digital di Indonesia dari sekadar aksi iseng menjadi kejahatan terorganisir yang terstruktur dan merusak.

Guna merespons ancaman yang terus membesar itu, pemerintah memperkuat dasar hukum lewat Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Aturan ini disiapkan sebagai landasan hukum menyeluruh untuk menata aktivitas siber, menghadirkan kepastian hukum, dan menindak pelaku kejahatan digital [7]. Kendati demikian, penindakan hukum dan pembenahan teknis saja belum mampu menurunkan angka kejahatan siber secara berarti. Berbagai kajian menunjukkan akar persoalannya kerap terletak pada lemahnya kesadaran moral dan etika para pengelola sistem informasi [4], [8].

Di sinilah etika profesi TI menjadi penting sebagai kerangka nilai yang menuntun perilaku praktisi agar bertumpu pada integritas, kejujuran, akuntabilitas, dan perlindungan privasi pengguna [9], [10]. Kode etik berfungsi sebagai rambu agar praktisi tidak menyalahgunakan kewenangannya dan tetap menjaga mutu profesionalisme [10]. Dua kerangka etis kerap dijadikan acuan dalam konteks ini: kerangka PAPA (*Privacy, Accuracy, Property, Accessibility*) gagasan Mason [11] dan prinsip CIA Triad (*Confidentiality, Integrity, Availability*) [8]. Dengan menginternalisasi nilai-nilai etis ini, seorang praktisi TI tidak hanya bertindak sebagai teknisi, tetapi juga sebagai penjaga moral yang memastikan teknologi digunakan secara bertanggung jawab demi kepentingan masyarakat luas [8].

Penelitian-penelitian terdahulu yang membahas kejahatan siber di Indonesia masih terfokus pada dua pendekatan utama secara terpisah, yaitu pendekatan hukum pidana, seperti efektivitas UU ITE dalam menjerat pelaku [12] dan pendekatan teknis, seperti penguatan enkripsi dan keamanan jaringan [2]. Masih jarang penelitian yang secara khusus mengintegrasikan etika profesi sebagai pilar preventif yang strategis dalam penanggulangan kejahatan siber. Padahal, berdasarkan temuan lapangan, banyak insiden kebocoran data justru dipicu oleh kelalaian internal yang berakar pada rendahnya kepatuhan terhadap kode etik, seperti pada kasus akses tidak sah oleh pegawai internal (*insider threat*) di sektor perbankan dan Kesehatan [4], [5]. Dengan demikian, terdapat kesenjangan (*research gap*) antara ketersediaan regulasi dan teknologi keamanan dengan perilaku etis para penggunanya. Penelitian ini hadir untuk mengisi kekosongan tersebut dengan memberikan gambaran holistik mengenai peran etika profesi TI sebagai benteng pertahanan pertama yang bersifat preventif.

Bertolak dari latar belakang dan tinjauan pustaka di atas, studi ini diarahkan untuk mengurai sekaligus menggambarkan secara mendalam peran etika profesi teknologi informasi dalam menanggulangi kejahatan siber di Indonesia. Secara lebih khusus, kajian menyoroti bagaimana penghayatan nilai-nilai etika profesi dapat meredam ancaman dari dalam, mendorong kepatuhan terhadap UU ITE, serta memadukan dimensi hukum dan moral demi terciptanya ekosistem digital yang aman, adil, dan bertanggung jawab. Adapun manfaatnya, temuan penelitian ini diharapkan menjadi rujukan bagi perguruan tinggi dalam memperkuat kurikulum etika profesi, sekaligus bahan pertimbangan bagi pemerintah dan regulator saat menyusun kebijakan keamanan siber yang bertumpu pada pembentukan sumber daya manusia berintegritas.

2. METODE

Penelitian ini menggunakan jenis penelitian studi kepustakaan (*library research*) dengan pendekatan kualitatif deskriptif. Studi kepustakaan dipilih karena penelitian ini bertujuan mengkaji dan menganalisis secara mendalam konsep, teori, serta fenomena yang berkaitan dengan etika profesi teknologi informasi dan kejahatan siber berdasarkan sumber-sumber literatur yang telah tersedia [13]. Pendekatan kualitatif deskriptif digunakan untuk menggambarkan dan menginterpretasikan data secara sistematis, faktual, dan akurat mengenai peran etika profesi TI dalam penanggulangan kejahatan siber di Indonesia [13].

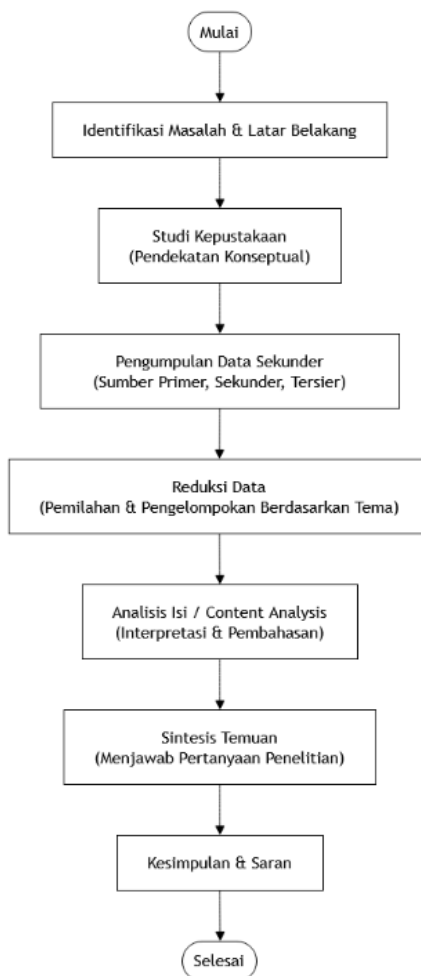
Penelitian ini menggunakan pendekatan konseptual (*conceptual approach*), yaitu dengan mengkaji pandangan para ahli dan doktrin yang berkembang dalam literatur, terutama yang berkaitan dengan konsep etika profesi dan kode etik profesi TI [9], [10], kerangka kerja PAPA [11], serta prinsip CIA Triad [8]. Regulasi yang relevan, khususnya UU ITE, diposisikan sebagai konteks bahan pendukung untuk memahami lingkungan tata kelola keamanan siber, bukan sebagai objek analisis utama [7].

Sumber data dalam penelitian ini adalah data sekunder yang terdiri dari tiga kategori sumber pustaka, yaitu:

1. **Sumber primer**, berupa peraturan perundang-undangan yang berlaku, yaitu UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [7].
2. **Sumber sekunder**, berupa literatur ilmiah yang relevan dengan topik penelitian, meliputi jurnal ilmiah nasional terakreditasi, buku teks, prosiding seminar, dan hasil penelitian terdahulu yang membahas etika profesi, kejahatan siber, keamanan data, dan perlindungan privasi di Indonesia [3], [4], [5], [6], [14].
3. **Sumber tersier**, berupa kamus hukum dan kamus teknologi informasi yang digunakan untuk memperjelas istilah-istilah teknis yang digunakan dalam penelitian.

Teknik pengumpulan data dilakukan melalui studi dokumentasi, yaitu dengan menelusuri, mengumpulkan, dan mencatat berbagai informasi dari sumber-sumber literatur yang berkaitan dengan objek penelitian. Penelusuran literatur dilakukan secara digital melalui basis data seperti SINTA, Google Scholar, dan portal jurnal nasional lainnya, serta perpustakaan digital. Setelah seluruh data terkumpul, dilakukan proses reduksi data dengan memilih dan memilah informasi yang relevan dengan fokus penelitian, kemudian menyajikannya dalam bentuk narasi deskriptif.

Teknik analisis data yang digunakan adalah analisis isi (*content analysis*) dengan pendekatan kualitatif [13]. Analisis isi dilakukan dengan mengkaji secara kritis setiap literatur yang diperoleh untuk menemukan pola, tema, dan hubungan antar konsep yang relevan dengan peran etika profesi TI dalam penanggulangan kejahatan siber. Langkah-langkah analisis meliputi: (1) pengorganisasian data berdasarkan tema utama, yaitu konsep etika profesi TI, modus operandi kejahatan siber, dan peran etika dalam pencegahan; (2) interpretasi terhadap temuan dari berbagai literatur untuk memperoleh pemahaman yang komprehensif; (3) sintesis atau penggabungan temuan tersebut untuk menjawab pertanyaan penelitian; dan (4) penarikan kesimpulan secara induktif. Hasil analisis disajikan secara deskriptif-naratif dalam bentuk uraian yang sistematis dan argumentatif. Untuk memudahkan pemahaman terhadap alur penelitian, berikut disajikan diagram alir (*flowchart*) metode penelitian:



Gambar 1. Diagram Alir Metode Penelitian

Diagram alir tersebut menggambarkan alur penelitian yang dilakukan secara sistematis, dimulai dari identifikasi masalah dan latar belakang, dilanjutkan dengan studi kepustakaan menggunakan pendekatan konseptual, pengumpulan data sekunder (sumber primer, sekunder, dan tersier), reduksi data sesuai tiga tema utama penelitian, analisis isi (*content analysis*), sintesis temuan untuk menjawab pertanyaan penelitian, hingga penarikan kesimpulan dan penyusunan saran.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil penelusuran dan analisis terhadap berbagai literatur yang relevan, penelitian ini menemukan tiga temuan utama yang akan dibahas secara mendalam, yaitu: (1) konsep etika profesi dan kode etik dalam bidang teknologi informasi; (2) modus operandi dan tren kejahatan siber di Indonesia; serta (3) peran etika profesi sebagai instrumen preventif dalam penanggulangan kejahatan siber. Ketiga temuan tersebut disajikan secara deskriptif-analitis untuk menjawab pertanyaan penelitian mengenai bagaimana etika profesi TI berperan dalam menghadapi ancaman kejahatan siber di Indonesia.

3.1. Konsep Etika Profesi dan Kode Etik dalam Bidang Teknologi Informasi

Etika profesi TI pada dasarnya adalah landasan moral yang mengarahkan cara seorang ahli TI memanfaatkan kompetensinya demi kepentingan publik. Pkurofesional TI dihadapkan pada dilema etis dalam pekerjaannya, sehingga mereka harus mampu menyeimbangkan antara penggunaan teknologi inovatif dengan perlindungan informasi pribadi pengguna [9]. Dalam kajian ini, etika profesi TI dipandang sebagai kerangka nilai yang menuntun praktisi saat berhadapan dengan pilihan teknologis yang dilematis. Titik beratnya terletak

pada kejujuran, sikap dapat dipercaya, kesediaan bertanggung jawab, dan komitmen menjaga data pribadi pengguna [5], [10]. Dalam konteks yang lebih operasional, kode etik profesi berfungsi sebagai pedoman tertulis yang secara tegas menyatakan apa yang baik dan benar serta apa yang tidak benar atau tidak baik bagi seorang profesional [10].

Kajian literatur memperlihatkan bahwa etika profesi TI punya ciri khas yang membedakannya dari profesi lain. Bidang ini bersinggungan dengan masyarakat melekat teknologi sekaligus menghasilkan produk yang berdampak luas, sehingga tanggung jawabnya melekat pada keamanan dan keselamatan data [8]. Seorang praktisi TI tidak bebas membangun program atau mengelola sistem tanpa mempertimbangkan perlindungan data dan risiko yang bisa ditimbulkannya [14]. Tuntutan ini selaras dengan prinsip inti etika profesi, yakni tanggung jawab moral, integritas, dan keadilan dalam setiap pekerjaan.

Dalam ranah keamanan siber, salah satu kerangka etis paling relevan adalah PAPA gagasan Mason, yang bertumpu pada empat pilar: privasi (*Privacy*), akurasi (*Accuracy*), kepemilikan (*Property*), dan aksesibilitas (*Accessibility*) [11]. Kerangka ini menuntun praktisi untuk menjaga data pribadi, memastikan informasi akurat, menghormati hak atas data, sekaligus membuka akses hanya bagi pihak yang berwenang [11]. Prinsip CIA Triad yang lazim dianggap sebagai standar teknis pun sesungguhnya sarat muatan etis: memelihara kerahasiaan (*confidentiality*) dan integritas (*integrity*) data adalah kewajiban moral yang tidak bisa ditawar bagi profesional TI [8]. Ketika ketiga prinsip itu diabaikan, yang tercermin sebenarnya adalah merosotnya nilai etika dalam pengelolaan risiko keamanan informasi.

Secara operasional, kode etik menjadi pegangan agar praktisi menjalankan profesinya dengan standar terjaga dan tidak menyimpang. Kode etik dimaknai sebagai kumpulan aturan berperilaku yang bertujuan agar profesional memberi layanan terbaik bagi penggunanya sekaligus melindungi masyarakat dari tindakan yang tidak profesional. Pelanggaran atas kode etik dapat berbuah sanksi, mulai dari sanksi moral hingga pemberhentian dari pekerjaan atau organisasi profesi [10]. Dengan begitu, etika profesi bekerja sebagai kendali internal yang mencegah penyalahgunaan akses istimewa (*privileged access*) atas data yang dikelola [4].

3.2. Modus Operandi dan Tren Kejahatan Siber di Indonesia

Hasil telaah pustaka menunjukkan bahwa modus kejahatan siber di Indonesia kini jauh lebih terorganisir dan berdampak sistemik dibanding era awal yang sekadar berupa vandalisme atau unjuk kemampuan teknis (*hacking*) [8]. Dari berbagai kasus yang telah dipaparkan sebelumnya, pola serangan tersebut dapat dikelompokkan ke dalam tiga modus dominan.

Pertama, *ransomware* yang membidik infrastruktur kritis nasional, sebagaimana tampak pada serangan Brain Cipher terhadap PDN; modus ini menyingkap lemahnya kesiapan mitigasi sekaligus tanggung jawab profesional dalam menjaga keberlangsungan layanan publik [3]. Kedua, kebocoran data massal (*data breach*) di sektor strategis seperti perbankan (BSI) dan kesehatan (BPJS Kesehatan), yang berakar pada rendahnya akuntabilitas dan kelalaian melindungi data sensitif publik [4], [5]. Ketiga, rekayasa sosial (*social engineering*) dan *phishing* yang mengeksploitasi faktor manusia (*human factor*); keberhasilannya lebih ditentukan oleh kelengahan dan rendahnya kepatuhan etis pengguna ketimbang kecanggihan teknis pelaku [6].

Di luar serangan teknis, persekusi digital dan *cyberbullying* turut menjadi ancaman serius di ruang siber Tanah Air. Kekerasan psikis lewat media sosial dan kanal daring ini menyasar harga diri korban serta memicu dampak psikologis berat, mulai dari kecemasan berkepanjangan, depresi, sampai upaya bunuh diri [12]. Fakta ini menegaskan bahwa kerugian kejahatan siber tidak berhenti pada aspek materi, tetapi juga merambah kesehatan mental dan martabat manusia di dunia digital.

Untuk memudahkan pemahaman mengenai kasus-kasus utama dan implikasi etisnya, berikut disajikan tabel ringkasan:

Tabel 1. Kasus Kejahatan Siber di Indonesia dan Implikasi Etisnya

Kasus	Modus Operandi	Dampak Utama	Pelanggaran Etika Profesi Terkait
-------	----------------	--------------	-----------------------------------



Ransomware PDN [3]	Ransomware Brain Cipher	Lumpuhnya layanan publik nasional	Pengabaian prinsip <i>availability</i> dan tanggung jawab profesional dalam mitigasi krisis.
Peretasan Bank Syariah Indonesia (BSI) [4]	Peretasan <i>core banking</i>	Bocornya data nasabah ke <i>dark web</i>	Pengabaian prinsip <i>confidentiality</i> dan <i>integrity</i> dalam pengelolaan akses data perbankan.
Kebocoran Data BPJS Kesehatan [5]	Eksplorasi celah keamanan internal	Tereksposnya 279 juta data peserta	Lemahnya tata kelola etis data publik serta ancaman <i>insider threat</i> .
<i>Phishing & Social Engineering</i> [6]	Manipulasi psikologis pengguna	Pencurian data pribadi dan finansial	Rendahnya kepatuhan terhadap kode etik organisasi dan literasi etis pengguna.

Sumber: Diolah dari berbagai literatur [3], [4], [5], [6].

3.3. Peran Etika Profesi sebagai Instrumen Preventif dalam Penanggulangan Kejahatan Siber

Temuan utama studi ini memperlihatkan bahwa rapuhnya keamanan siber di Indonesia kerap bersumber dari lemahnya kesadaran moral dan etika para pengelola sistem informasi [8]. Hal ini dikuatkan oleh kajian literatur sistematis atas kasus kebocoran data BSI, yang menyimpulkan bahwa nilai tanggung jawab, akuntabilitas, dan kesadaran akan keamanan informasi sangat menentukan terbentuknya budaya keamanan yang efektif [4]. Enkripsi terkuat maupun perangkat keamanan terancang akan kehilangan maknanya bila orang yang mengoperasikannya tidak menjunjung integritas dan tanggung jawab moral. Dalam posisi inilah etika profesi bekerja sebagai pertahanan preventif.

Fungsi preventif itu terwujud lewat sejumlah mekanisme. Pertama, penanaman nilai integritas dan akuntabilitas pada praktisi TI mampu meredam risiko ancaman dari dalam (*insider threat*). Praktisi yang berintegritas sadar untuk tidak menyalahgunakan hak aksesnya atas data sensitif, sehingga kebocoran, baik yang disengaja maupun karena kelalaian, dapat dicegah [4]. Kedua, penerapan kerangka PAPA secara konsisten menempatkan perlindungan data pribadi bukan sekadar kewajiban teknis, melainkan juga kewajiban moral [11]. Sebagai contoh, kasus kebocoran data BPJS Kesehatan memperlihatkan bahwa lemahnya tata kelola dan transparansi pengelolaan data publik secara etis melanggar prinsip akuntabilitas dan kejujuran profesional [5]. Ketiga, etika manajemen risiko mengharuskan praktisi selalu menyiapkan cadangan data (*backup*) serta prosedur *disaster recovery* sebagai wujud tanggung jawab moral kepada publik, sebagaimana tersorot dalam serangan *ransomware* di PDN [3].

Di samping itu, regulasi dan etika profesi saling menguatkan. UU ITE tidak hanya bersifat represif untuk menjerat pelaku *cyber crime*, tetapi juga menjadi rujukan etis yang mendorong terbentuknya ekosistem digital yang bertanggung jawab [1], [7]. Kendati begitu, aturan tanpa penegakan kode etik yang konsisten sulit berjalan efektif. Rendahnya literasi digital dan terbatasnya kemampuan teknis aparat dalam menangani bukti digital yang rumit [6] justru menegaskan pentingnya membangun etika profesi sejak hulu, yakni lewat pendidikan karakter dan kurikulum etika yang serius di perguruan tinggi bidang TI.

Etika profesi berperan sebagai kendali moral yang menjaga agar teknologi tetap dimanfaatkan secara bertanggung jawab. Peran ini sulit digantikan oleh sistem enkripsi secanggih apa pun, sebab keamanan siber tidak hanya bertumpu pada perangkat lunak, tetapi juga pada tata kelola moral dan integritas orang-orang yang mengelolanya.

4. KESIMPULAN



Berdasarkan hasil analisis dan pembahasan terhadap berbagai literatur yang telah dikaji, penelitian ini menyimpulkan bahwa etika profesi teknologi informasi merupakan fondasi moral yang sangat penting bagi para praktisi TI dalam menjalankan tugas profesionalnya. Nilai-nilai integritas, akuntabilitas, dan perlindungan terhadap privasi pengguna, sebagaimana tertuang dalam kode etik profesi dan kerangka PAPA, menjadi pedoman utama yang membedakan profesi TI dari pekerjaan teknis biasa. Tanpa internalisasi nilai-nilai etis ini, seorang profesional TI berpotensi menjadi celah keamanan terbesar (*insider threat*) dalam sistem informasi yang dikelolanya.

Studi ini juga mendapati bahwa kejahatan siber di Indonesia telah berubah menjadi serangan sistemik yang berdaya rusak tinggi. Tiga modus yang paling menonjol mencakup *ransomware* terhadap infrastruktur nasional (misalnya Brain Cipher di PDN), kebocoran data berskala besar pada sektor perbankan dan kesehatan (BSI serta BPJS), dan rekayasa sosial (*social engineering*) maupun *phishing* yang memanfaatkan kelengahan pengguna. Kenyataan ini memperlihatkan bahwa keamanan siber tidak sekadar persoalan teknis, melainkan juga menyangkut perilaku dan tata kelola moral.

Lebih lanjut, etika profesi berperan sebagai instrumen preventif yang krusial dalam penanggulangan kejahatan siber. Internalisasi nilai integritas mampu menekan risiko ancaman dari dalam (*insider threat*), penerapan kerangka PAPA memastikan perlindungan data pribadi sebagai kewajiban moral, dan etika manajemen risiko mendorong profesional TI untuk selalu menyiapkan rencana pemulihan data sebagai bentuk tanggung jawab kepada publik. Regulasi seperti UU ITE dan kode etik profesi memiliki hubungan sinergis; hukum memberikan payung kepastian, sementara etika memberikan kesadaran moral yang mencegah terjadinya pelanggaran sejak dini. Dengan demikian, penelitian ini menegaskan bahwa keamanan siber yang tangguh tidak dapat diwujudkan hanya dengan mengandalkan teknologi enkripsi atau perangkat keamanan tercanggih, melainkan faktor manusia (*human factor*) yang berintegritas dan beretika adalah benteng pertahanan pertama dan utama.

Berdasarkan kesimpulan yang telah diuraikan, penelitian ini merekomendasikan agar penelitian selanjutnya melakukan studi empiris kuantitatif, misalnya dengan menyebarkan kuesioner atau melakukan wawancara mendalam kepada praktisi TI di institusi pemerintah dan perbankan, untuk mengukur secara langsung tingkat kepatuhan terhadap kode etik profesi dan pengaruhnya terhadap kejadian kebocoran data. Selain itu, penelitian mendatang juga disarankan untuk mengkaji secara spesifik tantangan etika profesi dalam menghadapi perkembangan teknologi baru, seperti kecerdasan buatan (*Artificial Intelligence/AI*) dan *Internet of Things* (IoT), yang membawa kompleksitas etis baru yang belum sepenuhnya terjangkau oleh regulasi dan kode etik saat ini. Bagi peneliti yang tertarik pada bidang kebijakan, disarankan pula untuk melakukan studi komparatif antara Indonesia dengan negara lain (misalnya Singapura atau Malaysia) dalam hal penerapan sanksi etis bagi pelanggar kode etik profesi TI, sehingga dapat diperoleh model terbaik yang dapat diadopsi di Indonesia.

REFERENSI

- [1] E. F. Primadany *et al.*, *PENGANTAR HUKUM SIBER INDONESIA*. Serang: Sada Kurnia Pustaka, 2025.
- [2] M. S. Hidayatullah, "Etika Cyber Security: Fondasi Benteng Digital in Tackling Cybercrime," in *Prosiding SAINTEK: Sains dan Teknologi*, Feb. 2025.
- [3] A. Simorangkir, H. Sihombing, P. I. Sihite, and J. Parhusip, "Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber," *Jurnal Sains Student Research*, vol. 2, no. 6, pp. 324–331, Dec. 2024, doi: 10.61722/jssr.v2i6.2966.
- [4] S. Anugrah, N. R. Qalby, M. Z. Himawan, and E. Nurmiati, "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis," *JTK3TI: Jurnal Tata Kelola dan Kerangka Kerja TI*, vol. 11, no. 2, pp. 106–112, 2025.
- [5] C. Sorisa, C. L. Kiareni, and J. Parhusip, "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia," *Jurnal Sains Student Research*, vol. 2, no. 6, pp. 586–593, Dec. 2024, doi: 10.61722/jssr.v2i6.2996.
- [6] R. Hikmatulloh and E. Nurmiati, "Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)," *Kosmik Hukum*, vol. 20, no. 2, pp. 121–127, 2020, doi: 10.30595/kosmikhukum.v20i2.6449.
- [7] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2024 Nomor 1, Tambahan Lembaran Negara RI Nomor 6905, 2024.
- [8] R. Firmansyah, "PERAN IT ETHICS AND REGULATION DALAM MENINGKATKAN EFEKTIVITAS CYBERSECURITY DI ERA TEKNOLOGI," *Jurnal Informatika Kaputama (JIK)*, vol. 9, no. 2, Jul. 2025.



- [9] D. Y. Zebua and A. P. Zebua, "TANTANGAN ETIKA DALAM PROFESI TEKNOLOGI INFORMASI," *IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, vol. 2, no. 1, Jan. 2025.
- [10] V. Kumalasari S., *ETIKA PROFESI Dalam Bidang Teknologi Informasi*. Semarang: Yayasan Prima Agus Teknik, 2021.
- [11] Fadli, S. A. Hardiansyah, and T. Sutabri, "Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data," *Jurnal Ilmiah Penelitian Mahasiswa*, vol. 4, no. 1, pp. 666–676, Jan. 2026, doi: 10.61722/jipm.v4i1.1951.
- [12] D. Setiawan, T. Farina, and S. Nugraha, "Fenomena Persekusi Digital dan Cyberbullying: Analisis Hukum Pidana Terhadap Konten Kekerasan Psikis di Internet," *INNOVATIVE: Journal Of Social Science Research*, vol. 5, no. 4, pp. 399–415, 2025.
- [13] M. N. Adlini, A. H. Dinda, S. Yulinda, O. Chotimah, and S. J. Merliyana, "METODE PENELITIAN KUALITATIF STUDI PUSTAKA," *Edumaspul: Jurnal Pendidikan*, vol. 6, no. 1, pp. 974–980, 2022.
- [14] F. Gunawan, A. Fadhilah, and E. M. Sari, "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime," *Jurnal Ilmiah Teknik Informatika (Tekinfo)*, vol. 25, no. 1, Apr. 2024, doi: 10.37817/tekinfo.v25i1.