JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2155-2159

Mengukur Kewajiban Moral Profesional TI dalam Menanggapi Serangan Ransomware (Studi Kasus PDNS 2 di Indonesia)

Farisa Adhila Nisa[1], Martha Marcella Kerenhapukh Giri[2], Andreansyah Errisa[3], Ahmad Irsyad Rosyadi[4], Annisa Elfina Augustia[5]

[1,2,3,4,5]Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1]farisaadhila12@gmail.com, [2]marthamarcella07@gmail.com, [3]errisa1705@gmail.com, [4]irsydrsydi8@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS 2) Indonesia pada tahun 2024 tidak hanya menimbulkan gangguan layanan publik dan kerugian finansial, tetapi juga mengungkap kegagalan fundamental dalam penerapan etika profesi teknologi informasi. Penelitian ini menganalisis penerapan etika profesi dan kewajiban moral profesional keamanan siber dalam penanganan insiden PDNS 2. Menggunakan pendekatan kualitatif deskriptif dengan studi pustaka terhadap data sekunder dari laporan resmi pemerintah, literatur akademik, kode etik profesi, dan publikasi media, penelitian ini menemukan bahwa penanganan insiden menunjukkan pelanggaran terhadap prinsip-prinsip etika profesi utama. Analisis mengidentifikasi kegagalan dalam menerapkan prinsip "menghindari bahaya" (ACM *Code of Ethics*) melalui non-aktifnya sistem keamanan dan ketiadaan *backup* data yang memadai, serta keterbatasan dalam prinsip "kepentingan publik di atas kepentingan pribadi" (IEEE *Code of Ethics*) dalam aspek transparansi komunikasi. Penelitian ini juga mengungkap dilema etis kompleks yang dihadapi profesional TI, termasuk konflik antara pembayaran tebusan versus pemulihan data, serta trade-off antara keamanan dan aksesibilitas sistem. Implikasi etis dari insiden ini menunjukkan erosi kepercayaan publik terhadap layanan digital pemerintah dan menguatnya kekhawatiran terhadap perlindungan data pribadi. Kesimpulan penelitian menekankan perlunya penguatan regulasi keamanan siber, investasi dalam kapabilitas teknis dan SDM, serta peningkatan kesadaran etika profesi di kalangan profesional TI Indonesia untuk memulihkan kepercayaan publik dan memperkuat ketahanan siber nasional.

Kata Kunci: *ransomware*; etika profesional TI; kewajiban moral profesional; Pusat Data Nasional Sementara (PDNS 2); keamanan siber

Abstract−*The ransomware attack on Indonesia's Temporary National Data Center (PDNS 2) in 2024 not only caused public service disruptions and financial losses, but also revealed fundamental failures in the application of information technology professional ethics. This study analyzes the application of professional ethics and the moral obligations of cybersecurity professionals in handling the PDNS 2 incident. Using a descriptive qualitative approach with a literature review of secondary data from official government reports, academic literature, professional codes of ethics, and media publications, this study found that the handling of the incident violated key professional ethical principles. The analysis identified failures in applying the principle of "avoiding harm" (ACM Code of Ethics) through the deactivation of security systems and the absence of adequate data backups, as well as limitations in the principle of "public interest over private interest" (IEEE Code of Ethics) in terms of transparency of communication. This study also reveals the complex ethical dilemmas faced by IT professionals, including the conflict between ransom payments versus data recovery, as well as the trade-off between security and system accessibility. The ethical implications of this incident indicate an erosion of public trust in government digital services and heightened concerns about personal data protection. The study concludes that there is a need to strengthen cybersecurity regulations, invest in technical capabilities and human resources, and raise awareness of professional ethics among Indonesian IT professionals in order to restore public trust and strengthen national cybersecurity.*

Keywords: *ransomware*; *IT professional ethics; professional moral obligations*; Pusat Data Nasional Sementara (PDNS 2); *cybersecurity*

1. PENDAHULUAN

Perkembangan teknologi informasi membawa kemajuan sekaligus tantangan keamanan siber yang kompleks, salah satunya *ransomware* yang mengenkripsi data penting dan menuntut tebusan. Serangan ini tidak hanya menimbulkan kerugian finansial, tetapi juga mengancam keamanan nasional dan kepercayaan publik terhadap sistem digital pemerintah.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2155-2159

Serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS 2) Indonesia tahun 2024 menjadi kasus nyata yang berdampak luas pada layanan publik seperti imigrasi, pendidikan, dan administrasi kependudukan. Insiden ini mengekspos kerentanan infrastruktur digital nasional dan menegaskan pentingnya kesiapsiagaan, profesionalisme, serta etika kerja tenaga ahli TI dalam menghadapi situasi darurat.

Etika profesi keamanan siber berperan krusial memastikan tindakan profesional TI didasarkan pada nilai moral seperti tanggung jawab, integritas, keadilan, dan kerahasiaan data. Profesional TI tidak hanya dituntut mengatasi serangan secara teknis, tetapi juga mempertimbangkan aspek etis dalam pengambilan keputusan—mulai dari pelaporan insiden, penanganan data korban, hingga komunikasi publik.

Kasus PDNS 2 menggambarkan dilema etika: di satu sisi profesional TI harus melindungi data dan menjaga kerahasiaan sistem, di sisi lain berkewajiban moral bertindak transparan, cepat, dan bertanggung jawab dalam pemulihan. Keseimbangan aspek teknis dan etis inilah yang menjadi inti profesionalisme keamanan siber.

Penelitian ini bertujuan menganalisis penerapan etika profesi dan kewajiban moral profesional TI dalam menanggapi serangan *ransomware* melalui studi kasus PDNS 2, guna memahami peran etika profesi dalam menjaga kepercayaan publik dan memperkuat keamanan digital nasional.

2. METODE

2.1 Jenis dan Pendekatan Penelitian

Kajian ini menggunakan metode kualitatif dengan jenis penelitian deskriptif. Metode ini digunakan mengingat relevansinya terhadap menggambarkan, memahami, dan menganalisis fenomena sosial secara mendalam dalam konteks naturalnya, khususnya mengenai penerapan etika profesi teknologi informasi dalam penanganan insiden serangan *ransomware* pada PDNS 2 di Indonesia. Penelitian deskriptif kualitatif memungkinkan peneliti untuk mengeksplorasi kompleksitas peristiwa, persepsi, dan implikasi etis yang tidak dapat diukur secara numerik, sehingga dapat memberikan pemahaman yang holistik tentang masalah yang diteliti.

2.2 Sumber Data

Jenis data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder dipilih karena penelitian berfokus pada analisis dan interpretasi fenomena yang sudah terjadi. Sumber data diperoleh dari berbagai dokumen terpercaya yang dapat dikelompokkan sebagai berikut:

a. Dokumen Resmi Pemerintah: Laporan publik dan keterangan pers dari Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), serta instansi terkait lainnya mengenai kronologi, dampak, dan langkah penanganan insiden.
b. Literatur Akademik: Jurnal ilmiah, artikel penelitian, dan buku teks yang membahas etika profesi TI, keamanan siber, manajemen insiden, dan tanggung jawab moral profesional.
c. Kode Etik Profesi: Dokumen panduan etika profesional dari organisasi internasional dan nasional, seperti ACM *Code of Ethics*, IEEE *Code of Ethics*, serta pedoman yang dikeluarkan oleh asosiasi profesi TI di Indonesia.
d. Publikasi Media dan Analisis Daring: Berita dari media terpercaya, laporan analisis dari firma keamanan siber, dan publikasi online lain yang menyoroti dampak sosial dan ekonomi dari insiden PDNS 2.
e. Dokumen Regulasi: Peraturan perundang-undangan terkait, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta kebijakan nasional di bidang keamanan siber dan perlindungan data pribadi.

2.3 Metode Pengumpulan Data

Teknik utama yang digunakan untuk mengumpulkan data adalah studi pustaka (literatur, berita resmi, laporan BSSN, jurnal ilmiah). Teknik ini dilakukan dengan cara menelusuri, mengumpulkan, menyeleksi, dan mendokumentasikan berbagai sumber data sekunder yang relevan, seperti yang telah dijelaskan pada bagian sumber data. Proses ini melibatkan pencarian sistematis melalui database jurnal akademis, situs web resmi instansi pemerintah, dan platform berita

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2155-2159

terpercaya untuk mengakses data dan keterangan yang akurat serta dapat dipertanggungjawabkan validitasnya.

3. ANALISA DAN PEMBAHASAN

3.1 Penerapan Etika Profesi Teknologi Informasi dalam Penanganan Insiden PDNS 2

Berdasarkan analisis terhadap data sekunder yang terkumpul, penerapan etika profesi TI dalam penanganan insiden *ransomware* PDNS 2 dapat dievaluasi melalui beberapa prinsip utama:

3.1.1 Evaluasi Berdasarkan Prinsip "Hindari Bahaya" (*Avoid Harm* - ACM)

Kegagalan dalam Penerapan Prinsip Keamanan Dasar: Insiden ini mengungkap kegagalan sistematis dalam menerapkan prinsip dasar keamanan siber. Fakta bahwa Windows Defender dinonaktifkan pada 17 Juni 2024 pukul 23.15 WIB menunjukkan kelalaian dalam menjaga sistem pengamanan tetap aktif dan terkini, yang secara langsung bertentangan dengan prinsip "menghindari bahaya" bagi masyarakat yang bergantung pada layanan publik.

Ketiadaan *Backup* Data yang Memadai: Tidak tersedianya data cadangan *(backup)* yang memadai merupakan bentuk pelanggaran terhadap kewajiban profesional untuk meminimalkan kerugian. Kondisi ini memperparah dampak serangan karena menghambat proses pemulihan dan memaksa pemerintah harus menyiapkan sistem *backup* berlapis pasca-insiden.

3.1.2 Evaluasi Berdasarkan Prinsip “Kepentingan Publik di Atas Kepentingan Pribadi” (IEEE)

Transparansi dan Komunikasi yang Terbatas: Meskipun BSSN dan Kominfo memberikan keterangan pers, analisis menunjukkan bahwa komunikasi kepada publik mengenai skala sebenarnya dari kebocoran data dan dampak jangka panjang masih terbatas. Hal ini menimbulkan pertanyaan mengenai keseimbangan antara kepentingan publik untuk mengetahui informasi dengan pertimbangan strategis instansi pemerintah.

Prioritas Pemulihan Layanan Publik: Upaya pemulihan dengan mengaktifkan Pusat Pemulihan Bencana *(Disaster Recovery Center)* di Tangerang menunjukkan komitmen untuk mengutamakan kepentingan publik dengan memulihkan layanan vital seperti imigrasi. Langkah ini selaras dengan prinsip mengutamakan kesejahteraan publik.

3.2 Kewajiban Moral Profesional Keamanan Siber dalam Merespons Serangan *Ransomware*

Analisis terhadap kewajiban moral profesional keamanan siber mengungkap dimensi etika yang kompleks dalam penanganan insiden ini:

3.2.1 Tanggung Jawab Moral terhadap Integritas Data

Kewajiban untuk Melindungi Data Sensitif: Profesional TI memiliki kewajiban moral mutlak untuk melindungi data sensitif warga negara, termasuk data pendaftar KIP Kuliah (sekitar 800 ribu data) dan data strategis dari Badan Intelijen, TNI, dan Polri. Kebocoran data ini ke *darkweb* menunjukkan kegagalan dalam memenuhi kewajiban fundamental ini.

Komitmen terhadap Transparansi dan Akuntabilitas: Pernyataan Wapres K.H. Ma'ruf Amin yang mengakui perlunya perbaikan industri siber merefleksikan bentuk tanggung jawab moral di tingkat institusi. Namun, evaluasi menyeluruh terhadap akuntabilitas individual dan kolektif dari para profesional yang terlibat masih diperlukan.

3.2.2 Dilema Etis dalam Pengambilan Keputusan

Dilema Pembayaran Tebusan: Tuntutan tebusan sebesar 8 juta USD (Rp 131 miliar) menempatkan pihak berwenang pada dilema etis yang kompleks antara mempertimbangkan pembayaran untuk memulihkan data secara cepat (dengan risiko mendanai kegiatan kriminal) versus penolakan pembayaran yang dapat memperpanjang gangguan layanan publik.

Konflik antara Keamanan dan Aksesibilitas: Investigasi forensik menemukan bahwa serangan memanfaatkan celah keamanan, kemungkinan karena *trade-off* antara kemudahan akses bagi pengguna *(tenant)* dan penerapan protokol keamanan yang ketat. Hal ini menyoroti kegagalan dalam menyeimbangkan prinsip keamanan dengan kebutuhan operasional.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2155-2159

3.3 Implikasi Etis Penanganan Serangan PDNS 2 terhadap Kepercayaan Publik dan Tanggung Jawab Profesional

Penanganan insiden PDNS 2 memiliki implikasi etis yang mendalam terhadap kepercayaan publik dan tanggung jawab profesional di bidang TI:

3.3.1 Dampak terhadap Kepercayaan Publik

Erosi Kepercayaan dalam Layanan Digital Pemerintah: Gangguan terhadap 282 penyewa *(tenant)* dan layanan publik seperti imigrasi dan pendidikan secara signifikan menggerakkan kepercayaan masyarakat terhadap kemampuan pemerintah dalam mengelola infrastruktur digital nasional yang aman.

Kekhawatiran terhadap Perlindungan Data Pribadi: Kebocoran data pribadi skala besar menimbulkan kekhawatiran publik yang mendalam mengenai kemampuan negara dalam melindungi privasi warga negara, yang merupakan hak dasar di era digital.

3.3.2 Tanggung Jawab Profesional dan Institusional

Kebutuhan Penguatan Regulasi dan Tata Kelola: Insiden ini mengungkap kelemahan tata kelola keamanan siber nasional, termasuk ketidakjelasan kewenangan dan ego sektoral antar lembaga. Hal ini mempertegas urgensi pengesahan dan implementasi regulasi seperti RUU Keamanan Siber dan UU PDP.

Pentingnya Investasi dalam Kapabilitas Teknis dan SDM: Pernyataan Wapres mengenai perlunya perbaikan dalam pembiayaan dan SDM TI yang mumpuni mengindikasikan pengakuan atas tanggung jawab institusional untuk berinvestasi dalam penguatan kapabilitas teknis (seperti Next-Generation Firewall, EDR, XDR) dan pengembangan kompetensi profesional secara berkelanjutan.

Berdasarkan analisis di atas, dapat disimpulkan bahwa insiden *ransomware* PDNS 2 tidak hanya merupakan kegagalan teknis, tetapi lebih mendasar sebagai kegagalan dalam menerapkan prinsip-prinsip etika profesi dan memenuhi kewajiban moral profesional di bidang teknologi informasi dan keamanan siber.

4. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan mengenai penerapan etika profesi teknologi informasi dalam penanganan insiden serangan *ransomware* pada PDNS 2 di Indonesia, dapat disimpulkan sebagai berikut:

4.1 Kesimpulan Umum

Insiden serangan *ransomware* terhadap PDNS 2 pada dasarnya bukan hanya merupakan kegagalan teknis semata, melainkan merepresentasikan kegagalan yang lebih mendasar dalam menerapkan prinsip-prinsip etika profesi dan memenuhi kewajiban moral profesional di bidang teknologi informasi dan keamanan siber. Kegagalan ini tercermin mulai dari fase pencegahan, respons insiden, hingga proses pemulihan, yang pada akhirnya berdampak signifikan terhadap erosi kepercayaan publik terhadap layanan digital pemerintah.

4.2 Kesimpulan Khusus

4.2.1 Berdasarkan Penerapan Etika Profesi TI

Teridentifikasi pelanggaran terhadap prinsip *"Avoid Harm"* dari Kode Etik ACM, yang ditunjukkan dengan tidak berfungsinya sistem keamanan (Windows Defender) dan tidak tersedianya cadangan data yang memadai, sehingga memperparah dampak serangan.

Penerapan prinsip "Kepentingan Publik di Atas Kepentingan Pribadi" (IEEE) berjalan tidak konsisten. Di satu sisi, upaya pemulihan layanan publik diutamakan, namun di sisi lain, tingkat transparansi informasi kepada publik mengenai skala sebenarnya dari kebocoran data masih terbatas.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2155-2159

4.2.2 Berdasarkan Kewajiban Moral Profesional

Terjadi kegagalan dalam memenuhi kewajiban moral inti untuk melindungi integritas dan kerahasiaan data sensitif warga negara, yang dibuktikan dengan bocornya data strategis dan data pribadi ke *dark web*.

Profesional dan institusi terkait dihadapkan pada dilema etis yang kompleks, seperti pertimbangan pembayaran tebusan dan konflik antara menerapkan keamanan ketat versus menjaga kemudahan akses operasional.

4.2.3 Berdasarkan Implikasi terhadap Kepercayaan Publik dan Tanggung Jawab Profesional

Penanganan insiden PDNS 2 telah menggerus kepercayaan publik terhadap kompetensi pemerintah dalam mengelola infrastruktur digital nasional yang aman dan melindungi data pribadi.

Insiden ini mengungkap kelemahan tata kelola keamanan siber nasional dan mendesak perlunya penguatan regulasi, peningkatan investasi dalam teknologi keamanan, dan pengembangan kapabilitas SDM profesional TI yang beretika.

REFERENCES

Adristi, F. I., & Ramadhani, E. (2024). Analisis dampak kebocoran data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan matriks budaya keamanan siber dan dimensi budaya nasional Hofstede. Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen, 2(6), 196–212. https://journal.uii.ac.id/selma/article/view/35529

Ghalib, Y. W., Gilang, E. F., Zumi, M., Abdhe, F., Nanda, A., Serly, D. A., & Zurkiyah, A. (2025). Analisis perkembangan keamanan siber dampak dari kebocoran data Pusat Data Nasional Sementara 2 Surabaya. JISCO: Journal of Information System and Computing, 2(1), 27–41. https://doi.org/10.30631/jisco.v2i1.100

Harahap, N. M. (2024). Resiko kejahatan teknologi informasi dan komunikasi cyber crime dan analisi inovasi pencegahan resiko cyber crime di Indonesia. Jurnal Teknologi dan Manajemen Sistem Industri, 3(1), 52–60.

Idzhand, A. N., Harahap, A. I., Yudisthira, T. R., & Amiruddin, A. (2024). Penerapan etika profesi di bidang keamanan cyber untuk mencegah kejahatan dunia maya. VISA: Journal of Vision and Ideas, 4(3), 1792–1799. https://doi.org/10.47467/visa.v4i3.3482

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772. https://doi.org/10.7717/peerj-cs.1772

Jaelani, S. (2024). Peran klasifikasi serangan sistem informasi dalam memperkuat keamanan nasional dan memerangi cyberwarfare. Jurnal Intelek dan Cendikiawan Nusantara, 1(3), 4634–3538. https://jicnusantara.com/index.php/jicn

Pitman, L., & Crosier, W. (2024). On the scale from ransomware to cyberterrorism: The cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine. Journal of Cyber Policy, 9(2), 179–199. https://doi.org/10.1080/23738871.2024.2377670

Prasetyo, D. A., Setiawan, F. D., Kapoyos, J. M., Gusnaldi, M. R., Fadholi, W. H. N., & Nurfiyah. (2024). Pentingnya etika siber pada era digital. Nusantara Journal of Multidisciplinary Science, 2(5), 1130–1137. https://jurnal.intekom.id/index.php/njms/article/view/976

Simorangkir, A., Sihombing, H., Parhusip, J., Yos, J., & Palangka, S. (2024). Ransomware pada data PDN: Implikasi etis dan tanggung jawab profesional dalam pengelolaan keamanan siber. Jurnal Sains Student Research, 2(6), 324–331. https://doi.org/10.61722/jssr.v2i6.2966

Tommy, S., & Nasution, M. I. P. (2025). Evaluasi manajemen risiko keamanan siber pada infrastruktur digital pemerintah: Studi kasus Pusat Data Nasional (PDN). Jurnal Manajemen Ekonomi dan Bisnis (JMEB), 4(1).