Vol. 8 No.01 2026
E-ISSN: 2685-6921
Universitas Ma'arif Nahdlatul Ulama Kebumen

Tanggung Jawab Profesional dalam Keamanan *Cyber* Perspektif Etika dan Hukum

Amiruddin Amiruddin[1]*, Mohd Wildan Qasthari[2], Muhammad Nazar[2], Nov Indra Adiwira Suryantyo[2], Rahmadani Rahmadani[2], Raja Rahmad Hafizhul Manik[2], M. Fadil Nasution[2]

[1]*Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia*

[2]*Universitas Islam Negeri Sumatera Utara, Medan, Indonesia*

mohdwildanqasthari@gmail.com*

Received: 13/06/2026 | *Revised: 29/06/2026* | *Accepted: 30/06/2026*

Abstrak

Keamanan siber merupakan aspek penting dalam menjaga keamanan data dan infrastruktur digital di era transformasi teknologi yang semakin pesat. Peningkatan ancaman siber menuntut adanya tanggung jawab 351rofessional yang tidak hanya berfokus pada aspek teknis, tetapi juga mempertimbangkan dimensi etika dan hukum. Penelitian ini bertujuan untuk mengkaji tanggung jawab 351rofessional dalam keamanan siber dari perspektif etika dan hukum serta menganalisis tantangan yang dihadapi dalam implementasinya. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur dan studi kasus. Data diperoleh melalui analisis jurnal ilmiah, regulasi keamanan siber, serta kebijakan organisasi, disertai wawancara semi-terstruktur dengan 351rofessional keamanan siber seperti administrator 351 rofes, analis keamanan informasi, dan praktisi *IT security*. Analisis data dilakukan menggunakan 351 rofes analisis tematik untuk mengidentifikasi pola tanggung jawab 351 rofessional dalam praktik keamanan siber. Hasil penelitian menunjukkan bahwa tanggung jawab 351rofessional dalam keamanan siber mencakup perlindungan data pribadi, kepatuhan terhadap regulasi seperti *General Data Protection Regulation* (GDPR) dan *California Consumer Privacy Act* (CCPA), serta penerapan kode etik 351rofessional seperti ISC² Code of Ethics dan EC-Council Code of Ethics. Selain itu, ditemukan bahwa tantangan utama terletak pada praktik *ethical hacking*, pemantauan aktivitas pengguna, serta pengelolaan kerentanan 351rofes yang memunculkan 351rofess antara keamanan, privasi, dan kepatuhan hukum. Penelitian ini menyimpulkan bahwa integrasi antara etika, hukum, dan kebijakan organisasi sangat penting dalam menciptakan ekosistem keamanan siber yang aman dan bertanggung jawab. Kode etik 351 rofessional berperan sebagai pedoman utama dalam membentuk perilaku 351rofessional yang berintegritas dalam menghadapi ancaman siber yang semakin kompleks.

Kata Kunci : keamanan siber, etika, hukum, perlindungan data, ancaman siber

Abstract

Cybersecurity is an essential aspect of protecting data and digital infrastructure in the era of rapid technological transformation. The increasing number of cyber threats requires professional responsibility that goes beyond technical aspects and considers ethical and legal dimensions. This study aims to examine professional responsibility in cybersecurity from ethical and legal perspectives and to analyze the challenges in its implementation. This research employs a qualitative approach using literature review and case study methods. Data were collected through the analysis of scientific journals, cybersecurity regulations, and organizational policies, as well as semi-structured interviews with cybersecurity professionals, including system administrators, information security analysts, and IT security practitioners. Data analysis used thematic analysis to identify patterns of professional responsibility in cybersecurity practices. The findings indicate that professional responsibility in cybersecurity includes the protection of personal data, compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and the implementation of professional codes of ethics such as the ISC² Code of Ethics and the EC-Council Code of Ethics. In addition, the study reveals that the main challenges lie in ethical hacking practices, user activity monitoring, and vulnerability management, which create dilemmas between security, privacy, and legal compliance. This study concludes that integrating ethics, law, and organizational policies is essential to creating a secure and responsible cybersecurity ecosystem. Professional codes of ethics play a crucial role in guiding ethical behavior and maintaining integrity in facing increasingly complex cyber threats.

Keywords: cybersecurity, ethics, law, data protection, cyber threats

Pendahuluan

Keamanan siber merupakan salah satu aspek penting dalam konteks keamanan nasional. Dalam era modern, infrastruktur digital telah menjadi bagian vital dalam mendukung fungsi pemerintahan, ekonomi, dan layanan publik, sehingga perlindungan terhadap sistem digital menjadi hal yang sangat penting (Rosy, 2020). Selain itu, data kini dipandang sebagai aset strategis yang harus dijaga keamanannya untuk memastikan keberlangsungan berbagai aktivitas digital di masyarakat.

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan, seperti komunikasi, transaksi daring, pendidikan, kesehatan, dan layanan pemerintahan. Transformasi ini menyebabkan ketergantungan yang tinggi terhadap sistem digital yang saling terhubung, sehingga meningkatkan risiko terhadap gangguan keamanan siber (Vimy et al., 2022). Kondisi ini menunjukkan bahwa keamanan siber tidak lagi bersifat opsional, melainkan menjadi kebutuhan utama dalam era digital.

Seiring dengan meningkatnya digitalisasi, ancaman keamanan siber juga mengalami peningkatan baik dari segi jumlah maupun kompleksitas. Berbagai bentuk ancaman seperti

malware, *phishing*, *ransomware*, hingga pencurian data pribadi semakin sering terjadi dan memberikan dampak signifikan bagi individu, organisasi, maupun negara. Laporan keamanan global menunjukkan bahwa insiden serangan siber terus meningkat setiap tahun, baik dalam skala kecil maupun serangan yang menargetkan infrastruktur kritis (Ramayanti & Lubis, 2023).

Dampak dari pelanggaran keamanan siber tidak hanya bersifat teknis, tetapi juga ekonomi, sosial, dan hukum. Kerugian yang ditimbulkan dapat berupa hilangnya data penting, kerusakan reputasi organisasi, hingga kerugian finansial dalam jumlah besar. Oleh karena itu, keamanan siber perlu dipahami sebagai sistem yang tidak hanya berfokus pada aspek teknis, tetapi juga mencakup aspek regulasi dan tanggung jawab profesional dalam pengelolaannya.

Dari perspektif hukum, Undang-Undang Dasar 1945 menjadi landasan utama dalam pengaturan keamanan nasional di Indonesia, termasuk perlindungan terhadap sistem informasi dan data digital. Namun, perkembangan teknologi yang sangat cepat sering kali tidak sejalan dengan regulasi yang ada, sehingga menimbulkan tantangan dalam penegakan hukum di bidang siber. Hal ini menunjukkan perlunya penguatan regulasi yang lebih adaptif terhadap perkembangan teknologi digital.

Selain aspek hukum, dimensi etika juga memiliki peran penting dalam keamanan siber. Profesional di bidang teknologi informasi memiliki akses terhadap data sensitif sehingga dituntut untuk menjunjung tinggi nilai integritas, tanggung jawab, dan kerahasiaan. Pelanggaran etika dapat berdampak luas tidak hanya pada organisasi, tetapi juga pada masyarakat secara umum. Oleh karena itu, kode etik seperti ISC² Code of Ethics dan EC-Council menjadi pedoman penting dalam menjaga profesionalisme di bidang keamanan siber.

Berdasarkan penelitian terdahulu, kajian mengenai keamanan siber umumnya masih berfokus pada aspek teknis dan sistem keamanan, sedangkan integrasi antara aspek etika dan hukum masih relatif terbatas. Kesenjangan ini menunjukkan perlunya kajian yang lebih komprehensif mengenai tanggung jawab profesional dalam keamanan siber. Oleh karena itu, penelitian ini bertujuan untuk mengkaji tanggung jawab profesional dalam keamanan siber dari perspektif etika dan hukum serta menganalisis implikasi dan tantangan yang dihadapi dalam implementasinya.

Metodologi Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis literatur dan studi kasus. Studi literatur dilakukan dengan mengkaji jurnal ilmiah, regulasi, serta kebijakan terkait keamanan siber dan perlindungan data. Sementara itu, studi kasus dilakukan pada organisasi yang bergerak di bidang teknologi informasi dan keamanan data yang telah menerapkan praktik keamanan siber berbasis etika dan hukum.

Organisasi yang menjadi fokus studi kasus dalam penelitian ini adalah institusi atau perusahaan yang memiliki kebijakan keamanan informasi, seperti penerapan standar keamanan data dan kode etik profesi di bidang teknologi informasi. Adapun aspek hukum yang dianalisis meliputi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), regulasi perlindungan data pribadi, serta kebijakan internal organisasi terkait keamanan informasi.

Pengumpulan data dilakukan melalui wawancara semi-terstruktur kepada profesional keamanan siber, seperti administrator sistem, analis keamanan informasi, dan praktisi IT security. Instrumen wawancara disusun berdasarkan indikator utama yang mencakup aspek

etika profesi (integritas, tanggung jawab, dan kerahasiaan), serta kepatuhan terhadap regulasi hukum keamanan siber. Selain itu, dilakukan juga analisis dokumen berupa kebijakan keamanan, standar operasional prosedur (SOP), dan kode etik profesi seperti ISC² Code of Ethics dan EC-Council.

Analisis data dilakukan menggunakan teknik analisis tematik dengan cara mengelompokkan data berdasarkan kategori etika, hukum, dan praktik keamanan siber. Proses ini bertujuan untuk mengidentifikasi pola tanggung jawab profesional dalam menghadapi ancaman keamanan siber serta keterkaitannya dengan kepatuhan hukum dan etika profesi.

Hasil dan Pembahasan

Hasil penelitian menunjukkan bahwa tanggung jawab profesional dalam keamanan siber mencakup beberapa aspek utama, salah satunya adalah perlindungan data pribadi. Perlindungan data pribadi dalam konteks global merujuk pada regulasi *General Data Protection Regulation* (GDPR), yaitu peraturan perlindungan data yang diterapkan di Uni Eropa untuk mengatur pemrosesan, penyimpanan, dan perlindungan data pribadi individu. Selain itu, terdapat *California Consumer Privacy Act* (CCPA), yaitu regulasi privasi data di negara bagian California, Amerika Serikat, yang memberikan hak kepada pengguna untuk mengakses, menghapus, dan mengontrol penggunaan data pribadi mereka oleh organisasi. Setelah disebutkan secara lengkap, kedua regulasi tersebut selanjutnya digunakan dalam penelitian ini sebagai acuan utama dalam analisis kepatuhan hukum keamanan siber.

Berdasarkan hasil wawancara semi-terstruktur dengan profesional keamanan siber (administrator sistem, analis keamanan informasi, dan praktisi *IT security*) serta analisis studi kasus pada beberapa organisasi yang telah menerapkan kebijakan keamanan informasi, ditemukan bahwa tanggung jawab profesional tidak hanya bersifat teknis, tetapi juga mencakup kepatuhan terhadap etika dan hukum. Hasil wawancara menunjukkan bahwa organisasi yang memiliki kebijakan keamanan formal cenderung lebih disiplin dalam menerapkan prinsip *confidentiality, integrity, and availability* (CIA) dalam pengelolaan data dan sistem informasi. Selain itu, studi kasus menunjukkan bahwa implementasi kode etik profesional berkontribusi terhadap peningkatan kesadaran keamanan dan pengurangan risiko pelanggaran data.

Kode etik profesional seperti ISC² Code of Ethics dan EC-Council Code of Ethics menjadi pedoman utama dalam menjaga integritas profesional keamanan siber. Berdasarkan hasil studi kasus, organisasi yang secara konsisten menerapkan kode etik tersebut memiliki mekanisme pengawasan internal yang lebih kuat dalam mengendalikan akses data, menjaga kerahasiaan informasi, serta memastikan kepatuhan terhadap kebijakan keamanan. Salah satu tantangan utama yang ditemukan dalam hasil wawancara dan studi kasus adalah penerapan *ethical hacking* atau pengujian penetrasi. Praktik ini dinilai efektif dalam mengidentifikasi kerentanan sistem sebelum dieksploitasi pihak tidak bertanggung jawab. Namun, beberapa responden menyatakan bahwa tanpa kebijakan yang jelas, aktivitas ini dapat menimbulkan dilema etika dan risiko pelanggaran privasi.

Selain itu, aspek pelacakan dan pemantauan aktivitas pengguna juga menjadi isu yang sering muncul dalam praktik keamanan siber. Hasil wawancara menunjukkan adanya perbedaan pandangan antar organisasi, di mana sebagian organisasi mengutamakan keamanan sistem, sementara yang lain lebih menekankan perlindungan privasi pengguna. Hal ini menunjukkan pentingnya penerapan prinsip proporsionalitas dalam setiap aktivitas pemantauan. Tantangan

lain yang teridentifikasi adalah pengungkapan kerentanan (*vulnerability disclosure*). Studi kasus menunjukkan bahwa organisasi yang memiliki prosedur pelaporan kerentanan yang jelas lebih cepat dalam melakukan mitigasi risiko keamanan. Namun, pengungkapan yang tidak terkontrol dapat meningkatkan risiko eksploitasi oleh pihak eksternal sebelum perbaikan dilakukan.

Selain aspek teknis, hasil penelitian juga menunjukkan pentingnya etika penggunaan internet dalam praktik profesional. Profesional keamanan siber dituntut untuk menjaga etika digital, termasuk tidak menyebarkan konten yang mengandung unsur SARA maupun konten yang melanggar hukum dan norma sosial. Selain itu, tanggung jawab dalam penggunaan data juga menjadi aspek penting, khususnya dalam memastikan bahwa data pribadi tidak disalahgunakan serta tetap sesuai dengan regulasi GDPR dan CCPA yang telah disebutkan sebelumnya.

Adopsi teknologi yang bertanggung jawab juga menjadi temuan penting dalam penelitian ini. Hasil wawancara menunjukkan bahwa organisasi yang mempertimbangkan dampak sosial dan etika dalam penerapan teknologi cenderung memiliki tingkat kepercayaan publik yang lebih tinggi. Oleh karena itu, pengembangan teknologi keamanan siber tidak hanya berorientasi pada aspek teknis, tetapi juga harus mempertimbangkan aspek sosial dan etika. Secara keseluruhan, hasil penelitian menunjukkan bahwa tanggung jawab profesional dalam keamanan siber merupakan kombinasi antara aspek teknis, etika, dan hukum. Integrasi antara regulasi seperti GDPR dan CCPA, kode etik profesional, serta kebijakan organisasi menjadi faktor utama dalam menciptakan sistem keamanan siber yang aman, terpercaya, dan berkelanjutan.

Kesimpulan

Tanggung jawab profesional dalam keamanan siber merupakan konsep yang kompleks karena melibatkan keseimbangan antara aspek etika dan kepatuhan hukum. Hasil penelitian menunjukkan bahwa penerapan kode etik profesional serta regulasi hukum yang berlaku menjadi faktor penting dalam membangun lingkungan keamanan siber yang aman, terpercaya, dan berkelanjutan. Dalam konteks ini, organisasi dituntut untuk terus mengembangkan kebijakan keamanan yang adaptif terhadap perkembangan teknologi serta meningkatnya ancaman siber. Kode etik profesional seperti ISC² *Code of Ethics* dan *EC-Council Code of Ethics* memiliki peran penting dalam membentuk perilaku profesional di bidang keamanan siber. Nilai-nilai utama seperti integritas, tanggung jawab, dan kerahasiaan menjadi dasar dalam pengambilan keputusan profesional, khususnya dalam menghadapi tekanan, konflik kepentingan, serta tantangan etika dalam praktik keamanan siber. Secara keseluruhan, kepatuhan terhadap kode etik dan regulasi hukum tidak hanya meningkatkan profesionalisme, tetapi juga berkontribusi dalam membangun budaya keamanan digital yang berlandaskan tanggung jawab, integritas, dan perlindungan data dalam ekosistem teknologi yang terus berkembang.

Daftar Pustaka

A. Anggono and M. Riskiyadi, "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review," J. Manaj. dan Organ., vol. 12, no. 3, pp. 239–251, 2021.

A.B. Wiranata, I Gede. *Dasar-dasar Etika dan Moralitas*, (Bandung: PT Citra Aditya Bakti, 2005)

Alfreda, I.J., Permata, R.R., & Ramli, T.S. (2021). Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang. *Jurnal Sains Sosio Humaniora*.

Ardiyanti, H. (2016). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. *Jurnal DPR RI*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*.

D. I. Sukmawan and D. P. Setyawan, "Peretas, Ketakutan, Dan Kerugian: Pelanggaran Data dan Keamanan Nasional," pp. 153–182.

Fachrudin, R., Respaty, E., Adilah I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, 95.

Fauzi, A., Akbar, R., Rizkha, A., Putri, S. T., Fadhilah, I., Iskandar, N. P., & Agung, G. N. (2023). Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna. *Jurnal Ilmu Multidisiplin*.

Ginting, S.B. (2018). Pentingnya Profesionalitas Dan Integritas Dalam Penegakan Hukum Dari Perspektif Etika.

I. S. Indartik, "*Pengaruh Etika Dalam Teknologi Informasi*," pp. 1–61, 2004.

Kementerian Pertahanan. (2016). PEDOMAN PERTAHANAN CYBER. kemenhan.

Mayola, C. A., Megasari, D. S., Dwiyanti, S., & Lutfiati, D. (2021). STRATEGI PEMASARAN MARKETING MIX PRODUK BULU MATA PALSU ELLASHES.PRO. e-journal UNESA.

Napitupulu, D. (2017). *Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional*. Universitas Budi Luhur.

Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, & Nurlela, S. (2023). Pentingnya Manajemen Security di Era Digitalisasi. *Jurnal Ilmu Multidisiplin*.

Rahmawati, C. (2019). Tantangan Dan Ancaman Keamanan CyberIndonesia Di Era Revolusi Industri 4.0. *Seminar Nasional Sains Teknologi dan Inovasi Indonesia*.

Ramayanti, H., & Lubis, A. F. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional. *Jurnal Hukum dan HAM*.

Rosy, A. F. (2020). Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan cyber. *Jurnal Ilmu Pemerintahan*.

Semiawan, C. (2010). *Metode Penelitian Kulitatif*. GRASINDO.

Simorangkir, B., Legionosuko, T., & Waluyo, S. D. (2023). *CYBER SECURITY DALAM STUDI KEAMANAN NASIONAL: POLITIK, HUKUM DAN STRATEGI*. Media Bina Ilmiah.

Susanto, E., Antira, L., Kevin, Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Jurnal Bisnis dan Kewirausahaan.

Vimy, T., Wiranto, S., Rudiyanto, W., P., & Suwarno, P. (2022). ANCAMAN SERANGAN CYBER PADA KEAMANAN NASIONAL INDONESIA. *Jurnal Kewarganegaraan*.

Wahyono, T. (2011). *Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi Edisi 1*.

Wahyono, Teguh. *Etika Komputer dan Tanggung Jawab Profesional di bidangTeknologi* Informasi (Yogyakarta: Andi Offset, 2006)