TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 278-282

Analisis Pelanggaran Etika Profesi TI dalam Kebocoran Data 279 Juta Pengguna Indihome: Studi Kasus Tanggung Jawab Perlindungan Data Pribadi

Elsa Halizah[1*], Ridwan Ismail[2], Aryaputra Daffa Mujsi[3], Farrel Elshida Riordan[4], Annisa Elfina Augustia[5]

[1-5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1*]elsahalizah4@gmail.com, [2]rdwnism2@gmail.com, [3]aryaputradaffa19@gmail.com, [4]farrelriordan87@gmail.com, [5]annisa12elfina@gmail.com
(* : coressponding author)

Abstrak−Kebocoran data 279 juta pengguna *Indihome* yang terjadi pada tahun 2024 merupakan salah satu insiden keamanan siber terbesar dalam sejarah Indonesia. Insiden ini tidak hanya menimbulkan kerugian materiil bagi korban, tetapi juga menyoroti kegagalan fundamental dalam penerapan etika profesi Teknologi Informasi (TI) dan tanggung jawab perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis pelanggaran prinsip-prinsip etika profesi TI dalam kasus kebocoran data *Indihome* dan menilai tanggung jawab penyedia layanan dalam melindungi data pengguna. Metode penelitian yang digunakan adalah kualitatif deskriptif melalui studi literatur dan analisis kasus. Data diperoleh dari pemberitaan media, laporan resmi, serta kode etik profesi seperti ACM, IEEE, dan APTIKOM. Hasil penelitian menunjukkan adanya pelanggaran terhadap prinsip kejujuran, akuntabilitas, dan tanggung jawab profesional. Penelitian ini menyimpulkan bahwa integritas profesional dan kepatuhan terhadap regulasi data pribadi, seperti UU PDP, merupakan elemen kritis untuk mencegah terulangnya insiden serupa di masa depan.

Kata Kunci: Etika Profesi TI; Kebocoran Data; Perlindungan Data Pribadi; Keamanan Siber; Indihome; Akuntabilitas

Abstract−*The leakage of 279 million Indihome users' data in 2024 was one of the largest cybersecurity incidents in Indonesia's history. This incident not only caused material losses for the victims but also highlighted a fundamental failure in the application of Information Technology (IT) professional ethics and the responsibility of personal data protection. This study aims to analyze the violations of IT professional ethics principles in the Indihome data breach case and assess the service provider's responsibility in protecting user data. The research method used is descriptive qualitative through literature study and case analysis. Data were obtained from media coverage, official reports, and professional codes of ethics such as ACM, IEEE, and APTIKOM. The results show violations of the principles of honesty, accountability, and professional responsibility. This study concludes that professional integrity and compliance with personal data regulations, such as the Personal Data Protection Law, are critical elements to prevent the recurrence of similar incidents in the future.*

Keywords: *IT Professional Ethics; Data Breach; Personal Data Protection; Cybersecurity; Indihome; Accountability*

1. PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mentransformasi berbagai aspek kehidupan masyarakat, termasuk dalam hal akses informasi dan layanan. Dalam ekosistem digital ini, data pribadi telah menjadi aset yang sangat berharga, sekaligus rentan terhadap berbagai ancaman keamanan (Wahyudi & Sari, 2023). Ancaman tersebut termanifestasi dalam bentuk *data breach* atau kebocoran data, yang frekuensi dan skalanya semakin meningkat belakangan ini.

Insiden kebocoran data 279 juta pengguna layanan *Indihome* yang dilaporkan pada awal tahun 2024 menjadi bukti nyata betapa rentannya data pribadi yang dikelola oleh entitas besar (Kompas, 2024). Data yang bocor dilaporkan mencakup informasi sensitif seperti *full name*, nomor telepon, alamat *email*, nomor KTP, dan detail layanan. Skala insiden yang masif ini tidak hanya menjadikannya salah satu yang terbesar di Indonesia, tetapi juga menimbulkan kekhawatiran publik yang luas mengenai keselamatan data digital mereka.

Di balik persoalan teknis keamanan siber, insiden ini menyimpan dimensi etika yang lebih dalam. Setiap profesional di bidang Teknologi Informasi (TI), baik sebagai *system developer*, *database administrator*, ataupun *cybersecurity analyst*, terikat oleh kode etik profesi yang

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 278-282

menjunjung tinggi prinsip integritas, akuntabilitas, dan tanggung jawab untuk melindungi kepentingan publik (*public good*) (ACM, 2018). Kebocoran data dalam skala sedemikian besar mempertanyakan komitmen dan implementasi nyata dari prinsip-prinsip etika tersebut dalam praktik pengelolaan data.

Landasan normatif bagi perlindungan data pribadi di Indonesia telah dikuatkan dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Regulasi ini menegaskan kewajiban bagi setiap Pengendali Data Pribadi untuk menjamin keamanan data yang dikelolanya. Oleh karena itu, kegagalan dalam mencegah kebocoran data tidak hanya dapat dipandang sebagai kelalaian teknis, tetapi juga sebagai bentuk pelanggaran terhadap etika profesi dan ketentuan hukum yang berlaku (Fahrudi, 2023).

Berdasarkan uraian di atas, penelitian ini akan menganalisis kasus kebocoran data *Indihome* melalui lensa etika profesi TI. Fokus penelitian adalah untuk mengidentifikasi bentuk-bentuk pelanggaran prinsip etika yang terjadi, menganalisis tanggung jawab profesional penyedia layanan, dan merekomendasikan langkah-langkah strategis untuk memperkuat perlindungan data pribadi di masa depan.

2. METODE PENELITIAN

2.1 Tahapan Model Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Pendekatan ini dipilih untuk mendapatkan pemahaman yang mendalam dan kontekstual mengenai dinamika pelanggaran etika profesi TI dalam insiden kebocoran data *Indihome* (Creswell & Poth, 2018).

2.2 Sumber Data dan Teknik Analisis

Sumber data yang digunakan dalam penelitian ini terdiri dari:

1. Data Primer: Sumber data primer meliputi dokumen-dokumen formal seperti Kode Etik Profesi dari *Association for Computing Machinery* (ACM, 2018), *Institute of Electrical and Electronics Engineers* (IEEE, 2025), dan *Asosiasi Pendidikan Tinggi Informatika dan Komputer* (APTIKOM), serta dokumen regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP).
2. Data Sekunder: Sumber data sekunder diperoleh dari artikel berita online terpercaya (seperti Kompas dan DetikINET), laporan investigasi dari instansi resmi seperti Badan Siber dan Sandi Negara (BSSN), dan jurnal-jurnal ilmiah terkait *cybersecurity*, manajemen risiko data, dan etika profesi TI.

2.3 Teknik Analisis Data

Teknik analisis data yang digunakan adalah analisis isi (*content analysis*). Tahapan analisis dilakukan secara sistematis sebagai berikut:

1. Identifikasi Fakta Kasus: Tahap ini melibatkan pengumpulan dan penyusunan kronologi, skala, jenis data yang bocor, dan pernyataan resmi dari pihak terkait mengenai insiden kebocoran data *Indihome* dari berbagai sumber terpercaya.
2. Identifikasi Prinsip Etika: Peneliti menelaah prinsip-prinsip kunci dalam kode etik profesi ACM, IEEE, dan APTIKOM yang relevan dengan isu privasi, keamanan data, dan tanggung jawab profesional.
3. Analisis Pelanggaran: Fakta-fakta yang telah diidentifikasi kemudian dibandingkan dengan prinsip-prinsip etika untuk menemukan titik-titik kesenjangan atau pelanggaran, seperti kegagalan dalam menjaga kerahasiaan (*confidentiality*), kurangnya transparansi, dan lemahnya akuntabilitas.
4. Triangulasi: Untuk memastikan validitas dan reliabilitas temuan, dilakukan triangulasi data dengan membandingkan informasi dari berbagai sumber, seperti pemberitaan media, laporan BSSN, dan literatur akademis.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 278-282

3. ANALISA DAN PEMBAHASAN

3.1 Kronologi dan Dampak Kebocoran Data Indihome

Menurut laporan yang beredar, kebocoran data diduga terjadi akibat celah keamanan pada sebuah *Application Programming Interface* (API) yang tidak diamankan dengan baik, sehingga memungkinkan akses tidak sah ke basis data berisi informasi pelanggan (DetikINET, 2024). Data yang terekspos mencapai 279 juta *record*, mencakup informasi personal yang sangat lengkap. Dampak dari insiden ini bersifat multifaset dan serius. Dari sisi pengguna, muncul risiko nyata seperti penipuan (*fraud*), *phishing*, *spam*, pemerasan, hingga penyalahgunaan identitas untuk pinjaman online ilegal. Bagi perusahaan, insiden ini merusak reputasi dan mengikis kepercayaan publik, yang merupakan modal utama dalam bisnis layanan digital. Secara makro, insiden ini mengganggu ekosistem digital nasional dan menjadi ujian bagi ketahanan siber Indonesia (BSSN, 2024).

3.2 Pelanggaran Prinsip Etika Profesi TI

Berdasarkan analisis terhadap kode etik profesi, teridentifikasi beberapa pelanggaran prinsip etika yang signifikan:

a. Prinsip *'Avoid Harm'* (ACM) dan *'Hold Paramount the Safety, Health, and Welfare of the Public'* (IEEE): Prinsip paling fundamental dalam etika profesi TI adalah menghindari menyebabkan bahaya. Kegagalan dalam mengamankan data pengguna yang sedemikian sensitif telah menimbulkan bahaya yang nyata dan langsung bagi jutaan orang, seperti potensi kerugian finansial dan psikologis. Ini merupakan pelanggaran serius terhadap kewajiban moral untuk melindungi kepentingan publik (*public good*).
b. Prinsip Kejujuran dan Keterbukaan (*Honesty and Transparency*): Kode etik ACM menekankan pentingnya kejujuran dan keterbukaan. Dalam penanganan insiden, sering kali terdapat keterlambatan dan kurangnya transparansi dari pihak penyedia layanan dalam mengkomunikasikan secara jelas dan cepat kepada pengguna tentang apa yang terjadi, data apa yang bocor, dan langkah mitigasi yang diambil. Kurangnya komunikasi yang proaktif ini dapat dikategorikan sebagai pelanggaran terhadap prinsip kejujuran.
c. Prinsip Akuntabilitas (*Accountability*) dan Tanggung Jawab Profesional (*Professional Responsibility*): Sebagai Pengendali Data Pribadi, penyedia layanan bertanggung jawab penuh (*accountable*) atas keamanan data yang dikelolanya. Kebocoran ini menunjukkan kegagalan dalam memenuhi tanggung jawab profesional tersebut. Kode etik menuntut profesional TI untuk memastikan bahwa sistem yang mereka rancang dan kelola memenuhi standar keamanan yang memadai.

3.3 Tanggung Jawab Perlindungan Data Pribadi dalam Bingkai UU PDP

Undang-Undang PDP memberikan mandat yang jelas mengenai kewajiban Pengendali Data Pribadi. Pasal 20 UU PDP menyatakan bahwa Pengendali Data wajib melindungi Data Pribadi yang dikelolanya. Perlindungan ini mencakup aspek teknis dan manajerial. Kegagalan memenuhi kewajiban ini, seperti yang terjadi pada kasus *Indihome*, dapat berimplikasi hukum berat, mulai dari sanksi administratif (teguran tertulis, denda administratif, hingga penghentian pemrosesan data), ganti rugi perdata, hingga sanksi pidana (Pasal 57 - 76 UU PDP). Kasus ini menjadi preseden penting dan ujian nyata pertama bagi efektivitas penegakan UU PDP di Indonesia (Makarim & Asmara, 2023).

3.4 Analisis Berdasarkan Teori Etika

Untuk memperdalam analisis, kasus ini juga ditinjau dari perspektif teori etika normatif:

1. Deontologi: Teori deontologi menekankan pada kewajiban dan aturan moral yang harus dipatuhi, terlepas dari konsekuensinya. Dari sudut pandang ini, melindungi data pribadi pengguna adalah kewajiban moral mutlak bagi setiap profesional TI dan organisasi pengendali data. Kegagalan melindungi data, dengan demikian, adalah pelanggaran langsung terhadap kewajiban deontologis tersebut, tanpa memandang apakah kebocoran itu akhirnya dimanfaatkan untuk kejahatan atau tidak (Tavani, 2020).

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 278-282

2. Utilitarianisme: Teori utilitarianisme menilai etis tidaknya suatu tindakan berdasarkan konsekuensinya, yaitu apakah tindakan tersebut memaksimalkan kebahagiaan atau *utility* bagi sebanyak mungkin orang. Dalam kasus ini, kerugian dan penderitaan masif yang dialami oleh 279 juta pengguna (risiko penipuan, kecemasan, kerugian finansial) jelas jauh lebih besar dibandingkan dengan manfaat atau penghematan biaya yang mungkin didapat perusahaan dari tidak menginvestasikan sumber daya yang memadai untuk mengamankan sistemnya. Oleh karena itu, kelalaian yang menyebabkan kebocoran ini dinilai tidak etis berdasarkan prinsip utilitarian (Spinello, 2020).

4. KESIMPULAN

Kasus kebocoran data 279 juta pengguna *Indihome* merupakan cerminan nyata dari masih lemahnya penerapan etika profesi TI dan tanggung jawab perlindungan data pribadi di Indonesia. Analisis ini berhasil mengidentifikasi adanya pelanggaran terhadap prinsip-prinsip inti etika profesi, seperti menghindari bahaya (*avoid harm*), kejujuran (*honesty*), transparansi, dan akuntabilitas. Insiden ini juga menyoroti urgensi penerapan UU PDP secara tegas dan konsisten untuk menciptakan efek jera dan memulihkan kepercayaan publik.

Untuk mencegah terulangnya insiden serupa di masa depan, diperlukan langkah-langkah komprehensif dan kolaboratif dari berbagai pemangku kepentingan:

1. Pendidikan dan Budaya Etika: Integrasi nilai-nilai etika profesi TI harus diperkuat dalam kurikulum pendidikan tinggi dan program pelatihan berkelanjutan bagi profesional TI. Perusahaan teknologi perlu membangun budaya organisasi yang menempatkan keamanan dan privasi data sebagai nilai inti (*core value*).
2. Peningkatan Kapasitas Keamanan Siber: Perusahaan harus meningkatkan investasi dan keseriusan dalam manajemen keamanan siber, termasuk menerapkan *security by design*, melakukan *penetration testing* dan audit keamanan yang rutin dan independen, serta membangun *incident response team* yang tanggap.
3. Penguatan Peran Lembaga Profesi dan Regulator: Lembaga profesi seperti APTIKOM dapat berperan lebih aktif dalam mensosialisasikan kode etik dan memberikan sanksi etik bagi anggotanya yang lalai. Sementara itu, regulator seperti BSSN dan Otoritas Pelindungan Data Pribadi perlu dioptimalkan fungsinya untuk melakukan pengawasan, pembinaan, dan penegakan hukum yang efektif.

Pada akhirnya, integritas profesional dan komitmen kuat untuk melindungi data pengguna harus menjadi fondasi utama dalam pengembangan dan operasional setiap layanan digital di Indonesia. Kemajuan teknologi harus berjalan seiring dengan tanggung jawab etis

UCAPAN TERIMA KASIH

Dengan penuh rasa syukur ke hadirat Tuhan Yang Maha Esa, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya atas rahmat dan karunia-Nya sehingga penulisan jurnal ilmiah dengan judul “Analisis Pelanggaran Etika Profesi TI dalam Kebocoran Data 279 Juta Pengguna Indihome: Studi Kasus Tanggung Jawab Perlindungan Data Pribadi” dapat diselesaikan dengan baik.

Penulis juga mengucapkan terima kasih yang tulus kepada:

1. **Ibu Dosen Pengampu Mata Kuliah Etika Profesi** atas bimbingan, ilmu, dan arahan yang sangat berharga selama proses perkuliahan dan penyusunan jurnal ini.
2. **Seluruh pihak dan mitra diskusi** yang telah memberikan dukungan, masukan, serta referensi yang memperkaya analisis dan pembahasan dalam penelitian ini.
3. **Rekan-rekan mahasiswa** yang telah berpartisipasi dalam diskusi serta bertukar pikiran untuk menyempurnakan tulisan ini.

Penulis menyadari bahwa masih terdapat keterbatasan dalam jurnal ini. Oleh karena itu, saran dan kritik yang konstruktif sangat diharapkan untuk penyempurnaan di masa mendatang. Semoga hasil penelitian ini dapat bermanfaat bagi pengembangan ilmu pengetahuan serta meningkatkan kesadaran akan pentingnya etika profesi TI dalam perlindungan data pribadi di Indonesia.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 278-282

REFERENCES

ACM. (2018). ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. https://www.acm.org/code-of-ethics

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Ancaman Siber Indonesia 2024. Jakarta: BSSN.

Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th ed.). SAGE Publications.

DetikINET. (2024). Diduga Bocor, Data Ratusan Juta Pelanggan Indihome Beredar di Forum Hacker. Diakses dari https://inet.detik.com

Fahrudi, A. N. (2023). Implikasi Hukum Undang-Undang Pelindungan Data Pribadi bagi Dunia Usaha di Indonesia. Jurnal Hukum Bisnis, 45(2), 112-125.

IEEE. (2025). IEEE Code of Ethics. Institute of Electrical and Electronics Engineers. https://www.ieee.org/about/corporate/governance/p7-8.html

Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 249.

Kompas. (2024). Data 279 Juta Pengguna Indihome Diduga Bocor, Berikut Kata Telkom. Kompas.com. Diakses dari https://tekno.kompas.com

Makarim, F. A., & Asmara, D. (2023). Penegakan Hukum Undang-Undang Pelindungan Data Pribadi: Tantangan dan Prospek. Jurnal Legislasi Indonesia, 20(1), 55-70.

Spinello, R. A. (2020). Cyberethics: Morality and Law in Cyberspace (7th ed.). Jones & Bartlett Learning.

Tavani, H. T. (2020). Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing (5th ed.). Wiley.

Wahtyudi, A., & Sari, P. N. (2023). Tantangan Keamanan Data Pribadi di Era Ekonomi Digital Indonesia. Jurnal Sistem Informasi dan Teknologi, 11(3), 201-210.

Zahra, A. F., Fatimah, D., & Saritka, R. E. A. (2025). Tren Edit Foto dengan AI, Pakar Siber Ingatkan Risikonya: Termasuk Kemungkinan Masuk Dark Web. Kompas.com. Diakses dari https://www.kompas.com