Teknik: Jurnal Ilmu Teknik dan Informatika
Volume 4 Nomor 2 Oktober 2024
e-ISSN: 2798-2513; p-ISSN: 2808-8751, Hal 53-56
DOI: https://doi.org/10.51903/teknik
Available online at: https://journal.stiestekom.ac.id/index.php/TEKNIK

Analisis Pelanggaran Etika Profesi Keamanan Siber (Studi Kasus Kebocoran Data Pajak di Indonesia)

Fransciko Pritama[1], Ekat Rueh Daya Leluni[2], Yovita[3], Jadiaman Parhusip[4]
[1234]Universitas Palangka Raya, Indonesia
Email : fransciko.pritama02@gmail.com[1], ekatruehdayaleluni22@gmail.com[2], yopitaipit1301@gmail.com[3], parhusip.jadiaman@it.upr.ac.id[4]

Alamat: Jl. Yos Sudarso, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah
Korespondensi penulis: fransciko.pritama02@gmail.com

Abstract. *Violation of professional ethics in cyber security is a critical issue that affects public trust in the management of sensitive data. This study analyzes ethical violations that occurred in cases of tax data leaks in Indonesia, using an emphasis on the main causes, impacts and consequences. The research method used involves literature analysis and case studies. The research results show that there are weaknesses in the data security system, minimal application of professional ethical principles, and lack of supervision of the authorized parties. This research aims to analyze violations of cyber security professional ethics related to tax data leaks in Indonesia.*

Keywords: *Professional Ethics, Cybersecurity, Tax Data, Leaks*

Abstrak. Pelanggaran etika profesi pada keamanan siber adalah gosip kritis yg memengaruhi kepercayaan publik terhadap pengelolaan data sensitif. Studi ini menganalisis pelanggaran etika yg terjadi dalam perkara kebocoran data pajak pada Indonesia, menggunakan penekanan dalam penyebab utama, dampak, & akibat. Metode penelitian yg dipakai melibatkan analisis literatur dan studi perkara. Hasil penelitian memperlihatkan adanya kelemahan pada sistem pengamanan data, minimnya penerapan prinsip etika profesi, dan kurangnya supervisi terhadap pihak yg berwenang. Penelitian ini bertujuan untuk menganalisis pelanggaran etika profesi keamanan siber terkait kebocoran data pajak di Indonesia.

Kata kunci: Etika Profesi, Keamanan Siber, Data Pajak, Kebocoran

1. LATAR BELAKANG

Perkembangan teknologi informasi telah memberikan pengaruh besar terhadap berbagai bidang kehidupan, termasuk dalam pengelolaan data dan informasi di dunia pemerintahan. Salah satu bidang yang sangat membutuhkan teknologi ini adalah perpajakan, di mana data pribadi masyarakat dan entitas bisnis dikelola secara digital. Akan tetapi, kemajuan ini juga menimbulkan risiko yang cukup besar, terutama berkaitan dengan ancaman keamanan siber yang dapat berakibat pada kebocoran data.

Kejadian kebocoran data perpajakan di Indonesia merupakan salah satu insiden yang merusak kepercayaan masyarakat terhadap sistem keamanan data pemerintah. Peristiwa ini tidak hanya menyoroti kelemahan teknis dalam pengelolaan data, tetapi juga menimbulkan pertanyaan mengenai kepatuhan terhadap etika profesi dalam bidang keamanan siber. Dalam hal ini, etika profesi berperan penting dalam menghindari tindakan-tindakan yang dapat merugikan masyarakat dan merusak reputasi institusi.

Pelanggaran etika dalam keamanan siber, seperti penyalahgunaan akses, kurangnya transparansi, dan kelalaian dalam perlindungan, menjadi masalah yang memerlukan perhatian serius. Selain itu, efek dari kebocoran data ini tidak hanya merugikan individu yang datanya telah terungkap, tetapi juga mengganggu kestabilan sistem perpajakan

Received: September 11, 2024; Revised: September 18, 2024; Accepted: November 12, 2024; Published: Desember 05, 2024;
fransciko.pritama02@gmail.com

secara keseluruhan. Oleh karena itu, dibutuhkan analisis menyeluruh untuk menemukan akar masalah, mengevaluasi dampak, dan memberikan solusi untuk mencegah kejadian serupa di masa depan.

Studi ini bertujuan untuk meneliti kasus kebocoran data pajak di Indonesia dari sudut pandang pelanggaran etika profesi dalam keamanan siber. Dengan memahami faktor-faktor yang berkontribusi pada pelanggaran ini, penelitian ini diharapkan dapat memberikan rekomendasi yang sesuai untuk meningkatkan keamanan data dan memperkuat kesadaran etika di antara para profesional keamanan siber.

2. KAJIAN TEORITIS

Etika profesional dalam keamanan siber adalah kumpulan prinsip moral yang bertujuan untuk mengatur perilaku profesional di bidang keamanan digital. Prinsip-prinsip ini mencakup kerahasiaan data, kejujuran, tanggung jawab profesional, dan transparansi. Di Indonesia, penguatan etika ini menjadi semakin penting seiring dengan meningkatnya kasus pelanggaran data, seperti kebocoran informasi pajak, yang berdampak pada kepercayaan masyarakat terhadap pengelolaan data oleh lembaga publik dan swasta. Selain itu, regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 berfungsi sebagai pedoman hukum untuk menegakkan etika dan mengatasi kejahatan siber (Linuxhackingid, 2024; Salsabil, 2021).

Kejahatan siber seperti pencurian data sering terjadi akibat penerapan standar etika yang kurang dalam pengelolaan sistem digital. Di Indonesia, etika ini juga dihadapkan pada tantangan untuk memastikan bahwa setiap individu dalam keamanan siber bertindak untuk melindungi data dan tidak menyalahgunakannya. Misalnya, ethical hackers memiliki tanggung jawab untuk melaporkan celah sistem yang mereka temukan kepada pemilik tanpa menyebabkan kerusakan, sesuai dengan prinsip tanggung jawab profesional yang diatur dalam berbagai pelatihan dan sertifikasi internasional seperti Certified Ethical Hacker (CEH) (UTI-TTIS, 2024).

Praktik etika profesional memerlukan integrasi prinsip moral ke dalam setiap tahapan kerja, dari perencanaan sistem hingga pengurangan ancaman. Ini mencakup pemahaman yang mendalam tentang hak privasi, kewajiban untuk mematuhi standar hukum, serta penghindaran konflik kepentingan. Tantangan seperti munculnya ancaman digital baru memerlukan adaptasi terhadap teknologi seperti kecerdasan buatan dan blockchain, sembari tetap berpegang pada norma etika (UTI-TTIS, 2024; Linuxhackingid, 2024).

3. METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif dengan desain studi kasus untuk menganalisis pelanggaran etika profesi dalam keamanan siber yang berkaitan dengan kebocoran data pajak di Indonesia. Metode ini memungkinkan peneliti untuk mengeksplorasi fenomena dengan detail menggunakan data sekunder yang relevan (Salsabil, 2021). Studi kasus dipilih agar dapat memberikan gambaran yang lebih jelas tentang konteks sosial, hukum, dan teknis di balik kebocoran data yang terjadi.

Pengumpulan data dilakukan melalui studi literatur dengan menganalisis sumber-sumber sekunder. Sumber data meliputi dokumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), laporan insiden kebocoran data dari lembaga pemerintah atau swasta, artikel akademis, dan berita dari media (UTI-TTIS, 2024). Metode ini memberikan informasi menyeluruh mengenai regulasi, prinsip etika, serta dampak sosial-ekonomi kebocoran data pajak di Indonesia.

Teknik analisis data yang digunakan adalah analisis tematik. Data dari berbagai sumber diorganisasikan dan diklasifikasikan menurut tema yang relevan, seperti kepatuhan terhadap regulasi keamanan data, prinsip etika dalam profesi keamanan siber, dan dampak dari kebocoran data. Data ini selanjutnya dianalisis dengan menggunakan analisis kualitatif untuk menemukan faktor-faktor yang mempengaruhi pelanggaran etika profesi akuntansi dan cara perusahaan dapat memprediksi serta menangani masalah tersebut (Ariadi et al., 2022). Metode ini diterapkan untuk menemukan pola dan hubungan antara pelanggaran etika dengan dampaknya di masyarakat (Salsabil, 2021).

Strategi ini dipilih karena tidak memerlukan interaksi langsung dengan subjek penelitian dan terbukti efektif dalam memahami konteks kebocoran data pajak berdasarkan informasi yang tersedia untuk umum. Pendekatan ini diharapkan dapat memberikan pemahaman yang mendalam mengenai penyebab, dampak, dan solusi terkait pelanggaran etika profesi dalam keamanan siber di Indonesia.

4. HASIL DAN PEMBAHASAN

Kronologi Kasus

Pada awal tahun 2024, Indonesia dikejutkan oleh insiden kebocoran data pajak yang melibatkan lebih dari 20 juta data pribadi wajib pajak. Data yang bocor mencakup informasi penting seperti nama, alamat, nomor identitas, dan rincian pendapatan. Kebocoran ini terungkap setelah beberapa pihak melaporkan adanya data pribadi yang dijual di internet. Investigasi awal menunjukkan bahwa kebocoran tersebut disebabkan oleh kelemahan dalam sistem keamanan yang digunakan oleh Direktorat Jenderal Pajak (DJP), ditambah dengan kelalaian dalam pengelolaan data oleh beberapa pegawai yang bertugas.

Setelah terungkap, kasus ini menimbulkan kekhawatiran di masyarakat karena data pribadi yang seharusnya dilindungi bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Pemerintah Indonesia segera membentuk tim investigasi untuk menemukan penyebab kebocoran dan menetapkan beberapa pejabat DJP sebagai tersangka terkait kelalaian mereka dalam menjaga data tersebut.

Dampak

Kasus kebocoran data pajak di Indonesia memiliki pengaruh yang besar, baik dari aspek sosial, ekonomi, hingga hukum. Secara sosial, insiden kebocoran ini mengurangi kepercayaan masyarakat terhadap pemerintah serta sistem perpajakan. Warga menjadi lebih waspada terhadap kemungkinan penyalahgunaan data pribadi mereka, yang bisa dimanfaatkan untuk penipuan atau tindak kriminal lainnya. Situasi ini berpotensi menurunkan keterlibatan wajib pajak dalam sistem perpajakan, yang dapat berdampak pada penurunan pendapatan pajak dan mempengaruhi stabilitas ekonomi negara.

Dari aspek ekonomi, efek dari kebocoran data mencakup kerugian finansial yang bersifat langsung dan jangka panjang. Individu yang mengalami kebocoran data berisiko mengalami pencurian identitas atau penipuan finansial, sedangkan perusahaan yang terpengaruh mungkin kehilangan reputasi dan kepercayaan dari pelanggan. Selain itu, pemerintah perlu menanggung biaya untuk pemulihan dan peningkatan sistem keamanan data, yang bisa sangat tinggi. Biaya ini tidak hanya melibatkan perbaikan teknis tetapi juga usaha untuk mengatasi dampak psikologis dan sosial terhadap masyarakat.

Dampak hukum yang ditimbulkan juga cukup berat. Pemerintah dihadapkan pada tuntutan untuk merevisi undang-undang dan regulasi yang berkaitan dengan perlindungan data pribadi. Kebocoran ini menegaskan betapa pentingnya penegakan hukum yang lebih

ketat tentang perlindungan data, serta pengawasan yang lebih intensif terhadap kebijakan dan praktik pengelolaan data pribadi. Di samping itu, individu yang bertanggung jawab atas kebocoran data dapat dikenakan sanksi hukum yang signifikan, baik itu sanksi pidana maupun administratif.

5. KESIMPULAN DAN SARAN

Kasus kebocoran data pajak di Indonesia memperlihatkan pelanggaran terhadap beberapa prinsip etika dalam bidang keamanan siber, yang dapat dijelaskan sebagai berikut:

1. Pelanggaran terhadap Prinsip Confidentiality (Kerahasiaan Data)

   Kebocoran data pajak yang melibatkan informasi pribadi wajib pajak menunjukkan kurangnya kemampuan dalam menjaga kerahasiaan data. Data yang sensitif seharusnya dilindungi dengan baik oleh pihak yang memiliki akses, tetapi dalam hal ini, kebocoran terjadi karena kelalaian dalam pengelolaan data, yang mencerminkan ketidakpatuhan terhadap prinsip mendasar ini.
2. Pelanggaran terhadap Prinsip Integrity (Integritas Data)

   Kebocoran data ini juga menunjukkan kegagalan dalam mempertahankan integritas data. Data pribadi seharusnya tetap aman dan tidak boleh terkena perubahan yang tidak sah, tetapi justru terbuka untuk disalahgunakan. Ini menunjukkan bahwa sistem keamanan yang ada tidak efektif dalam memastikan data tidak dimanipulasi atau disalahgunakan.
3. Pelanggaran terhadap Prinsip Accountability (Pertanggungjawaban)

   Kasus ini juga mencerminkan pelanggaran terhadap prinsip accountability, karena pihak yang bertanggung jawab atas pengelolaan data pajak tidak dapat menjelaskan kelalaian yang menyebabkan kebocoran. Kurangnya pengawasan yang memadai terhadap sistem yang ada mengindikasikan bahwa individu yang terlibat tidak menjalankan tanggung jawab mereka dengan baik.
4. Pelanggaran terhadap Prinsip Transparency (Transparansi)

   Kebocoran ini menunjukkan minimnya transparansi dalam pengelolaan data pribadi oleh lembaga pemerintah. Masyarakat seharusnya mendapatkan penjelasan yang jelas tentang cara data mereka dikelola dan dilindungi. Namun, pengelolaan yang tertutup dalam prosedur keamanan data menyebabkan kurangnya kepercayaan terhadap sistem yang ada.

Pelanggaran-pelanggaran ini menekankan pentingnya penerapan prinsip etika dalam profesi keamanan siber untuk mempertahankan kepercayaan publik dan melindungi data pribadi dari ancaman yang semakin kompleks.

DAFTAR REFERENSI

Linuxhackingid. (2024). Definisi dan Ruang Lingkup Etika Profesi Cybersecurity. Retrieved from https://linuxhacking.or.id

Salsabil, LS (2021). PERKEMBANGAN ETIKA SIBER DAN PENGATURAN CYBERLAW DI INDONESIA. DIALEKTIKA KOMUNIKA: Jurnal Kajian …, ejournal.unis.ac.id, <https://ejournal.unis.ac.id/index.php/DK/article/view/1211>

Universitas Teknokrat Indonesia - CSIRT. (2024). Etika dalam Hacking: Memahami Peran Ethical Hacker. Retrieved from https://csirt.teknokrat.ac.id

Ariadi, D, Husna, GA, & ... (2022). Analisis etika profesi dalam era digitalisasi pada kantor akuntan publik. Jurnal Ilmiah Manajemen …, journal.stiemb.ac.id, <http://www.journal.stiemb.ac.id/index.php/mea/article/view/2187>