TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis

Aditya Permana[1], Andika Bagas Ayogi[2], Ananda Luthfi Bagaskara[3], Radika Murifan Saputra[4]

[1,2,3,4]Teknik dan Ilmu Komputer, Jurusan Teknik Informatika, Universitas Indraprasta PGRI
Email: [1]aditiapermanaa9@gmail.com

Abstrak−Kebocoran data pada Bank Syariah Indonesia (BSI) yang terjadi beberapa waktu lalu menjadi salah satu insiden keamanan informasi terbesar di sektor perbankan nasional. Peristiwa ini menimbulkan pertanyaan serius mengenai penerapan etika profesi dalam menjaga keamanan data nasabah, terutama dalam konteks tanggung jawab profesional para ahli teknologi informasi. Penelitian ini bertujuan untuk menganalisis pengaruh etika profesi terhadap keamanan informasi dengan menggunakan studi literatur sistematis terhadap kasus kebocoran data BSI. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif berbasis studi literatur yang mencakup kode etik profesi (ACM, IEEE, dan APTIKOM), peraturan pemerintah tentang keamanan siber, serta artikel ilmiah dan berita terkini terkait kasus BSI. Hasil penelitian menunjukkan bahwa lemahnya penerapan prinsip- prinsip etika profesi, khususnya pada aspek integritas, akuntabilitas, dan tanggung jawab sosial, berkontribusi terhadap rendahnya kesadaran serta pengawasan keamanan informasi. Diperlukan peningkatan penerapan kode etik profesi secara menyeluruh dalam pengelolaan data dan sistem informasi perbankan untuk mencegah insiden serupa di masa depan.

Kata Kunci: Etika Profesi, Keamanan Informasi, Kebocoran Data, Bank Syariah Indonesia, Studi Literatur Sistematis

Abstrack−*The recent data breach at Bank Syariah Indonesia (BSI) represents one of the most significant information security incidents in the national banking sector. This event raises critical questions regarding the application of professional ethics in protecting customer data, particularly concerning the professional responsibilities of information technology specialists. This study aims to analyze the influence of professional ethics on information security through a systematic literature review of the BSI data breach case. The research employs a descriptive qualitative approach based on literature studies, including professional codes of ethics (ACM, IEEE, and APTIKOM), government cybersecurity regulations, and current scholarly articles and news reports related to the incident. The findings indicate that the weak implementation of ethical principles—especially integrity, accountability, and social responsibility—has contributed to low awareness and oversight of information security. Strengthening the application of professional ethics in data management and information systems within the banking industry is essential to prevent similar incidents in the future.*

Keywords*: Professional Ethics, Information Security, Data Breach, Bank Syariah Indonesia, Systematic Literature Review*

1. PENDAHULUAN

Perkembangan pesat dalam bidang teknologi informasi telah memberikan kemudahan bagi berbagai aspek dalam kehidupan manusia, termasuk dalam industri perbankan. Transformasi digital yang dijalankan oleh lembaga keuangan, seperti Bank Syariah Indonesia (BSI), memiliki tujuan untuk meningkatkan efisiensi layanan dan memperluas akses bagi nasabah. Namun, di balik perkembangan ini, muncul tantangan yang signifikan terkait keamanan informasi dan perlindungan data pribadi. Salah satu insiden yang menarik perhatian masyarakat adalah kebocoran data yang menimpa BSI pada tahun 2024, di mana data sensitif nasabah diduga telah diakses dan disebarluaskan oleh pihak yang tidak bertanggung jawab.

Insiden ini mengangkat pertanyaan penting mengenai sejauh mana penerapan etika profesi berperan dalam mencegah dan mengatasi pelanggaran keamanan informasi. Dalam konteks teknologi informasi, etika profesi tidak hanya terkait dengan tindakan individu profesional, tetapi juga melibatkan tanggung jawab moral dan sosial dalam menjaga kepercayaan publik terhadap sistem digital. Berdasarkan *ACM Code of Ethics* (2018) dan *IEEE Code of Ethics* (2025), seorang profesional dalam teknologi informasi harus menjunjung tinggi integritas, melindungi privasi, menghindari risiko bagi publik, dan bertanggung jawab atas dampak sosial dari teknologi yang dikelolanya. Di Indonesia, APTIKOM juga menekankan pentingnya nilai-nilai profesionalisme dan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

tanggung jawab akademis dalam meningkatkan kesadaran etis para lulusan di bidang teknologi informasi.

Masalah kebocoran data BSI menunjukkan adanya kesenjangan antara prinsip etika profesi dan praktik aktual di lapangan. Meskipun lembaga perbankan telah menerapkan berbagai sistem keamanan yang canggih, faktor manusia seperti kelalaian, kurangnya kesadaran etis, atau pelanggaran tanggung jawab professional masih menjadi titik lemah utama dalam sistem keamanan informasi. Ini menunjukkan bahwa keamanan data tidak hanya tergantung pada teknologi, tetapi juga pada integritas dan etika para profesional yang mengelolanya.

Di samping itu, perkembangan ancaman siber yang semakin rumit juga mendorong perlunya pembaruan dalam penerapan etika profesi di era digital. Keamanan informasi kini bukan hanya tanggung jawab teknis, tetapi juga tanggung jawab moral. Ketika etika profesi diabaikan, risiko kebocoran data dapat menimbulkan dampak sosial dan ekonomi yang luas, seperti kehilangan kepercayaan publik, kerugian finansial, dan pelanggaran hak privasi individu.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk mengidentifikasi pengaruh etika profesi terhadap keamanan informasi dalam konteks kebocoran data BSI dengan menggunakan pendekatan studi literatur sistematis. Penelitian ini diharapkan dapat memberikan wawasan mengenai hubungan antara kesadaran etis profesional teknologi informasi dan tingkat keamanan data di industri perbankan. Selain itu, hasil penelitian ini diharapkan dapat menjadi landasan untuk mengembangkan kebijakan etika serta memperkuat tata kelola keamanan informasi di Indonesia.

1.1 Kajian Teoritis

1.1.1 Etika Profesi dalam Teknologi Informasi

Etika profesi adalah kumpulan nilai moral dan tanggung jawab yang mengarahkan tindakan individu saat menjalankan profesinya. Dalam ranah teknologi informasi, etika profesi berperan sebagai panduan bagi para praktisi untuk melaksanakan tugas dengan penuh tanggung jawab, kejujuran, serta mengutamakan keamanan dan privasi pengguna. Berdasarkan *ACM Code of Ethics* (2018), para profesional dalam bidang teknologi harus berkontribusi pada kesejahteraan publik, menghindari risiko bagi orang lain, bersikap adil dan jujur, serta menghormati hak privasi dan kerahasiaan informasi.

Di saat bersamaan, *IEEE Code of Ethics* (2025) menekankan pentingnya bertindak dengan integritas dan keterbukaan dalam setiap kegiatan yang terkait dengan pengembangan sistem informasi. Di Indonesia, APTIKOM *Code of Ethics* menyoroti nilai-nilai kejujuran, tanggung jawab sosial, serta profesionalisme baik dalam dunia akademik maupun industri teknologi. Tiga kode etik ini berfungsi sebagai pedoman moral yang wajib diterapkan oleh setiap individu untuk menjaga kepercayaan publik terhadap teknologi.

Etika profesi bukan hanya sekadar regulasi formal, tetapi juga mencerminkan komitmen moral untuk mencegah tindakan yang dapat merugikan masyarakat, terutama dalam hal pengelolaan data dan sistem informasi. Minimnya kesadaran akan prinsip etika dapat mengakibatkan penyalahgunaan data, pelanggaran privasi, bahkan kebocoran informasi yang bersifat sensitif.

1.1.2 Keamanan Informasi

Keamanan informasi adalah elemen kunci dalam pengelolaan sistem yang berbasis digital, terutama dalam industri perbankan yang menangani data keuangan serta identitas nasabah. Menurut standar *ISO/IEC* 27001, ada tiga komponen utama dalam keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan. Ketiga komponen ini dirancang untuk memastikan bahwa hanya individu yang berwenang dapat mengakses informasi, bahwa data tidak boleh mengalami perubahan tanpa persetujuan, dan bahwa informasi selalu tersedia saat diperlukan.

Ancaman bagi keamanan informasi dapat muncul dari sumber internal maupun eksternal. Sumber internal meliputi kelalaian staf, lemahnya pengawasan akses, dan kurangnya kesadaran akan etika profesional. Sementara itu, sumber eksternal dapat termasuk serangan siber, peretasan sistem, serta penyalahgunaan data oleh pihak ketiga. Penting untuk diingat bahwa menjaga keamanan informasi memerlukan bukan hanya teknologi yang canggih, tetapi juga integritas dan tanggung jawab para profesional yang mengelolanya.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

1.1.3 Kebocoran Data dalam Konteks Perbankan

Kebocoran data merupakan bentuk pelanggaran keamanan informasi di mana data pribadi atau sensitif diakses dan disebarluaskan tanpa izin. Dalam konteks perbankan, insiden ini dapat menimbulkan konsekuensi serius, seperti pencurian identitas, penyalahgunaan rekening, dan hilangnya kepercayaan publik terhadap lembaga keuangan.

Kasus kebocoran data pada Bank Syariah Indonesia (BSI) menunjukkan bagaimana lemahnya sistem keamanan dan pengawasan internal dapat menimbulkan dampak besar bagi masyarakat. Berdasarkan laporan media dan analisis siber, kebocoran ini melibatkan data nasabah yang bersifat sensitif seperti nomor rekening, KTP, dan informasi keuangan pribadi. Selain kelemahan teknis, aspek etika profesi juga berperan penting dalam kasus ini, di mana kelalaian atau ketidaksadaran etis dari pihak yang bertanggung jawab dapat memperburuk situasi.

1.1.4 Hubungan Etika Profesi dan Keamanan Informasi

Etika profesi memiliki hubungan langsung dengan tingkat keamanan informasi di suatu organisasi. Prinsip-prinsip etis seperti integritas, tanggung jawab, dan transparansi berperan penting dalam membentuk budaya keamanan data. Seorang profesional yang beretika akan menjaga kerahasiaan data pengguna, melaporkan insiden keamanan dengan jujur, dan mematuhi kebijakan perlindungan data yang berlaku.

Sebaliknya, pelanggaran terhadap etika profesi dapat membuka peluang terjadinya kebocoran data. Misalnya, ketika seorang profesional dengan sengaja menyalahgunakan akses sistem, mengabaikan prosedur keamanan, atau gagal melindungi informasi penting, maka risiko serangan siber dan kehilangan data akan meningkat. Oleh karena itu, penerapan etika profesi yang kuat menjadi landasan penting dalam membangun sistem keamanan informasi yang berkelanjutan.

1.1.5 Studi Literatur Sistematis

Metode studi literatur sistematis digunakan untuk mengidentifikasi, meninjau, dan menganalisis berbagai sumber ilmiah yang relevan dengan topik penelitian. Pendekatan ini memungkinkan peneliti memperoleh gambaran yang komprehensif tentang hubungan antara etika profesi dan keamanan informasi. Proses studi literatur dilakukan dengan menelusuri artikel jurnal, laporan kebijakan, kode etik profesi, serta berita terkait kebocoran data BSI.

Dengan pendekatan ini, penelitian tidak hanya meninjau teori, tetapi juga membandingkan hasil temuan dari berbagai sumber untuk mendapatkan kesimpulan yang objektif. Hasil kajian teoritis ini menjadi dasar bagi pembahasan lebih lanjut mengenai bagaimana penerapan etika profesi dapat memengaruhi sistem keamanan informasi, khususnya dalam konteks kebocoran data perbankan.

2. METODE PENELITIAN

Penelitian ini mengadopsi metode kualitatif deskriptif dengan pendekatan kajian literatur sistematis. Pendekatan tersebut dipilih untuk menyelidiki secara mendalam koneksi antara etika profesional dan keamanan data, khususnya dalam konteks pelanggaran data di Bank Syariah Indonesia (BSI). Pemilihan studi literatur sistematis didasarkan pada fokus penelitian yang berorientasi pada analisis teori, regulasi, serta kasus nyata yang telah ada, sehingga menawarkan perspektif menyeluruh mengenai dampak etika profesional terhadap implementasi keamanan informasi di industri perbankan.

Proses penelitian dimulai dengan penentuan isu inti, yakni keterbatasan dalam penerapan etika professional dalam mengelola data perbankan yang dapat mengakibatkan kebocoran informasi. Tahap selanjutnya adalah mengumpulkan referensi dari beragam sumber ilmiah yang dapat diandalkan untuk mendukung proses analisis. Referensi yang digunakan mencakup jurnal akademik, laporan penelitian, kode etik profesi, berita resmi, serta ketentuan pemerintah yang berkaitan dengan perlindungan data pribadi. Proses kajian literatur meliputi mencari referensi, memilih literatur yang relevan, melakukan analisis konten, dan merangkum hasil temuan berdasarkan teori dan praktik yang diketahui di lapangan.

Seluruh data dalam penelitian ini bersumber dari informasi sekunder, yang terbagi dalam tiga

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

kategori utama. Pertama, dokumen kode etik profesi seperti *ACM Code of Ethics* (2018*), IEEE Code of Ethics* (2025), dan APTIKOM *Code of Ethics* (2023) yang berfungsi sebagai panduan etis dalam praktik di bidang teknologi informasi. Kedua, literatur penelitian dan artikel berita yang mengupas isu kebocoran data BSI, keamanan siber, serta penerapan etika dalam pengelolaan sistem informasi. Ketiga, kebijakan serta regulasi pemerintah seperti Undang- Undang No. 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP) dan peraturan dari Otoritas Jasa Keuangan (OJK) yang berkaitan dengan keamanan sistem digital perbankan, yang menjadi dasar hukum dalam menilai penerapan etika profesional dalam lembaga keuangan.

Proses pengumpulan data dilakukan dengan teknik dokumentasi dan studi literatur, di mana peneliti menelusuri sumber melalui platform ilmiah seperti Google Scholar, ResearchGate, dan IEEE Xplore. Rentang waktu publikasi yang digunakan dalam penelusuran literatur adalah tahun 2018 hingga 2025, agar analisis tetap relevan dengan perkembangan teknologi dan kebijakan terkini. Semua sumber kemudian dikelompokkan berdasarkan tema utama, yaitu etika profesi, keamanan informasi, dan kasus kebocoran data di sektor perbankan.

Analisis data dilakukan dengan menggunakan pendekatan analisis isi (content analysis) yang berfokus pada identifikasi nilai-nilai etika seperti integritas, tanggung jawab, dan akuntabilitas dalam praktik keamanan informasi. Analisis ini juga mencakup perbandingan antara prinsip-prinsip etika profesi (ACM, IEEE, dan APTIKOM) dengan praktik aktual dalam kasus kebocoran data BSI. Selanjutnya dilakukan triangulasi sumber data, yaitu proses verifikasi dan penguatan temuan dengan membandingkan informasi dari tiga kategori sumber: jurnal akademik, berita investigatif, dan kebijakan pemerintah. Pendekatan triangulasi ini bertujuan untuk meningkatkan validitas dan reliabilitas hasil penelitian.

Pemilihan metode studi literatur sistematis dalam penelitian ini didasarkan pada beberapa pertimbangan. Pertama, pendekatan ini memungkinkan peneliti mengkaji fenomena secara menyeluruh tanpa memerlukan data primer yang sensitif. Kedua, metode ini mampu menggabungkan hasil penelitian sebelumnya, teori etika profesi, serta kebijakan keamanan informasi untuk membentuk analisis yang komprehensif. Ketiga, pendekatan ini sesuai untuk topik etika dan keamanan data karena mampu menyoroti aspek moral, hukum, dan teknis secara bersamaan.

Melalui metode ini, penelitian diharapkan dapat mengungkap sejauh mana penerapan etika profesi berpengaruh terhadap keamanan informasi di lingkungan perbankan, khususnya dalam kasus kebocoran data Bank Syariah Indonesia. Hasil penelitian diharapkan memberikan kontribusi terhadap peningkatan kesadaran etis bagi para profesional teknologi informasi serta menjadi acuan bagi lembaga keuangan dalam memperkuat tata kelola dan kebijakan keamanan data secara berkelanjutan.

3. ANALISIS DAN PEMBAHASAN

Kebocoran data yang terjadi pada Bank Syariah Indonesia (BSI) menjadi salah satu insiden keamanan informasi terbesar dalam sejarah perbankan nasional. Insiden ini tidak hanya berdampak pada sistem operasional dan kepercayaan nasabah, tetapi juga memunculkan perdebatan mengenai lemahnya penerapan etika profesi di kalangan profesional teknologi informasi. Analisis ini berfokus pada bagaimana etika profesi berpengaruh terhadap keamanan informasi serta sejauh mana prinsip moral dan tanggung jawab profesional diterapkan dalam konteks insiden kebocoran data tersebut.

Kasus kebocoran data BSI menunjukkan adanya kesenjangan antara prinsip etika profesi dan praktik nyata di lapangan. Berdasarkan hasil penelusuran literatur, diketahui bahwa sejumlah data sensitif seperti identitas pribadi, nomor rekening, serta informasi keuangan nasabah beredar di forum daring setelah peretasan terjadi. Hal ini mengindikasikan lemahnya sistem keamanan internal dan pengawasan terhadap akses data. Dari perspektif etika profesi, peristiwa tersebut mencerminkan belum optimalnya penerapan prinsip integritas, akuntabilitas, dan tanggung jawab profesional yang diatur dalam kode etik ACM, IEEE, dan APTIKOM.

Prinsip integritas menuntut setiap profesional untuk menjaga kejujuran dan transparansi dalam bekerja, terutama dalam pengelolaan data digital. Ketika integritas diabaikan, risiko pelanggaran keamanan menjadi semakin besar. Dalam kasus BSI, dugaan kelalaian teknis dan keterlambatan dalam mendeteksi serangan siber menunjukkan kurangnya komitmen terhadap nilai integritas. Hal ini bertentangan dengan prinsip yang tercantum dalam ACM Code of Ethics (2018) yang menegaskan bahwa setiap profesional harus berupaya mencegah bahaya terhadap publik

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

melalui tindakan pencegahan yang etis dan proaktif.

Aspek akuntabilitas juga menjadi titik lemah yang terlihat dalam kasus ini. Akuntabilitas mengharuskan individu maupun organisasi bertanggung jawab atas dampak dari keputusan dan tindakan yang diambil. Namun, dalam banyak kasus kebocoran data, tanggung jawab seringkali tidak jelas dan cenderung dialihkan antara tim teknis, manajemen, dan vendor pihak ketiga. Berdasarkan kajian literatur, kurangnya sistem audit dan pemantauan keamanan secara berkala menjadi faktor yang memperbesar risiko kebocoran data di sektor perbankan. Dalam konteks etika profesi, hal ini menunjukkan belum adanya penerapan mekanisme tanggung jawab yang jelas antara pengembang sistem, administrator jaringan, dan pihak pengelola data.

Selain itu, prinsip tanggung jawab profesional sebagaimana tertuang dalam IEEE Code of Ethics (2025) mengharuskan profesional teknologi untuk menghindari tindakan yang dapat merugikan masyarakat dan selalu mempertimbangkan aspek keselamatan publik. Dalam kasus BSI, konsekuensi dari kebocoran data tidak hanya menimpa institusi, tetapi juga nasabah yang kehilangan rasa aman terhadap data pribadinya. Dampak sosial ini menegaskan bahwa keamanan informasi bukan hanya isu teknis, melainkan juga tanggung jawab moral yang melekat pada setiap profesional di bidang teknologi informasi. Dari perspektif teori etika, peristiwa ini dapat dianalisis menggunakan tiga pendekatan utama: deontologi, utilitarianisme, dan virtue ethics.

Hasil analisis juga menunjukkan bahwa penerapan etika profesi dapat meningkatkan efektivitas sistem keamanan informasi apabila diintegrasikan dengan kebijakan organisasi dan regulasi pemerintah. Misalnya, penerapan Undang- Undang Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022) menuntut setiap lembaga keuangan untuk melaksanakan prinsip transparansi, pembatasan tujuan penggunaan data, serta perlindungan terhadap hak subjek data. Namun, regulasi ini akan sulit diterapkan secara optimal jika para profesional tidak memiliki kesadaran etis dalam mengelola informasi. Etika profesi berfungsi sebagai pondasi moral yang memperkuat penerapan hukum dan teknologi keamanan.

Dalam studi literatur ini, ditemukan bahwa penguatan budaya etis organisasi menjadi faktor kunci dalam menjaga keamanan informasi. Institusi seperti BSI perlu membangun sistem yang tidak hanya berorientasi pada teknologi keamanan (firewall, enkripsi, atau sistem deteksi serangan), tetapi juga pada pembentukan kesadaran etis di kalangan karyawan. Program pelatihan etika profesi, audit internal yang transparan, serta penegakan sanksi terhadap pelanggaran etika dapat membantu memperkecil risiko kebocoran data.

Secara keseluruhan, hasil pembahasan menunjukkan bahwa etika profesi memiliki pengaruh langsung dan signifikan terhadap tingkat keamanan informasi. Ketika prinsip etika dijalankan dengan konsisten, profesional teknologi informasi akan lebih berhati-hati dalam mengelola data, melaporkan kerentanan sistem, dan menjaga kerahasiaan informasi. Sebaliknya, ketika etika diabaikan, maka kebocoran data seperti yang terjadi pada BSI berpotensi terulang kembali di masa mendatang.

Dengan demikian, penerapan etika profesi yang kuat, disertai regulasi yang ketat dan budaya organisasi yang etis, menjadi fondasi utama dalam membangun sistem keamanan informasi yang berkelanjutan di era digital. Kolaborasi antara lembaga keuangan, akademisi, dan pemerintah juga dibutuhkan agar nilai-nilai profesionalisme dan tanggung jawab moral dapat diimplementasikan secara menyeluruh dalam ekosistem keamanan data nasional.

4. KESIMPULAN DAN SARAN

Hasil penelitian ini menunjukkan bahwa penerapan etika profesi memiliki pengaruh yang sangat signifikan terhadap keamanan informasi, khususnya dalam konteks kebocoran data yang terjadi pada Bank Syariah Indonesia (BSI). Melalui studi literatur sistematis, ditemukan bahwa prinsip-prinsip etika profesi seperti integritas, akuntabilitas, transparansi, dan tanggung jawab profesional berperan penting dalam menjaga kepercayaan publik terhadap sistem digital perbankan.

Kasus kebocoran data BSI menggambarkan adanya kesenjangan antara nilai etika profesi dan praktik aktual di lapangan. Meskipun lembaga perbankan telah menerapkan berbagai teknologi keamanan, kelemahan dalam aspek etika dan kesadaran profesional menjadi faktor utama yang memperbesar risiko pelanggaran keamanan informasi. Rendahnya pengawasan internal, kurangnya akuntabilitas, serta minimnya kepatuhan terhadap kode etik profesi berkontribusi terhadap terjadinya insiden kebocoran data.

Dari sisi teori, pendekatan deontologi, utilitarianisme, dan virtue ethics menjelaskan bahwa keamanan informasi tidak hanya merupakan tanggung jawab teknis, tetapi juga kewajiban moral setiap profesional. Dalam pendekatan deontologis, menjaga kerahasiaan data merupakan bentuk tanggung jawab etis yang harus dilakukan tanpa syarat. Pendekatan utilitarian menegaskan bahwa keamanan data harus memberikan manfaat yang lebih besar bagi masyarakat luas dibandingkan dengan keuntungan individu. Sedangkan virtue ethics menekankan pentingnya karakter moral, kejujuran, dan tanggung jawab sebagai dasar profesionalisme di bidang teknologi informasi.

Selain itu, hasil penelitian juga menunjukkan bahwa keberhasilan penerapan keamanan informasi sangat bergantung pada sinergi antara etika profesi, kebijakan organisasi, dan regulasi pemerintah. Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022) dan kebijakan Otoritas Jasa Keuangan (OJK) menjadi landasan hukum yang penting, namun efektivitasnya tetap membutuhkan komitmen etis dari para profesional teknologi informasi di dalam organisasi. Etika profesi berfungsi sebagai pondasi moral yang melengkapi penerapan hukum dan teknologi keamanan siber yang digunakan dalam sistem perbankan.

Dengan demikian, dapat disimpulkan bahwa etika profesi tidak hanya berperan sebagai pedoman moral, tetapi juga menjadi komponen strategis dalam penguatan tata kelola keamanan informasi. Tanpa kesadaran etis dan tanggung jawab profesional, berbagai kebijakan dan sistem keamanan yang diterapkan tidak akan memberikan perlindungan yang optimal terhadap data nasabah.

Sebagai tindak lanjut dari hasil penelitian ini, terdapat beberapa saran yang dapat dijadikan rekomendasi:

1. Lembaga perbankan perlu memperkuat pendidikan dan pelatihan etika profesi bagi seluruh karyawan, terutama bagi mereka yang terlibat langsung dalam pengelolaan data digital. Pelatihan ini harus menekankan nilai integritas, tanggung jawab, dan kewajiban moral terhadap keamanan informasi.
2. Perlu dibangun budaya etis organisasi yang konsisten melalui sistem penghargaan dan sanksi yang jelas terhadap pelanggaran etika. Dengan demikian, nilai etika tidak hanya menjadi norma tertulis, tetapi juga menjadi bagian dari perilaku kerja sehari-hari.
3. Sinergi antara pemerintah, akademisi, dan praktisi teknologi informasi perlu ditingkatkan untuk memperbarui kode etik profesi agar lebih relevan dengan tantangan era digital, termasuk isu-isu seperti keamanan siber, privasi data, dan tanggung jawab sosial teknologi.
4. Bank Syariah Indonesia dan lembaga keuangan lainnya disarankan untuk menerapkan audit etika dan keamanan informasi secara berkala, agar potensi pelanggaran dapat terdeteksi lebih awal dan tindakan pencegahan dapat segera dilakukan.

Akhirnya, penelitian ini menegaskan bahwa kemajuan teknologi harus selalu diimbangi dengan penerapan nilai-nilai etika profesi yang kuat. Hanya dengan integritas dan tanggung jawab moral yang tinggi, sistem keamanan informasi dapat berfungsi secara optimal untuk melindungi hak-hak masyarakat di era digital.

REFERENCES

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

APTIKOM (Asosiasi Pendidikan Tinggi Informatika dan Komputer). (2023).

CNN Indonesia. (2024). Kebocoran Data BSI: Ribuan Data Nasabah Tersebar di Forum Siber. Retrieved from https://www.cnnindonesia.com/teknologi

D'Alessandro, W. (2025). Deontology and Safe Artificial Intelligence.

Della Yunika Zebua & Alfan Pintalius Zebua. (2025). Tantangan Etika dalam Bidang Teknologi Informasi. Jurnal Ilmu Ekonomi, Pendidikan dan Teknik, 2(1), 35–44.

Detik.com. (2024). Analisis Insiden BSI: Tantangan Keamanan Siber di Dunia Perbankan Syariah. Retrieved from https://www.detik.com/teknologi

Dodig-Crnkovic, G., Basti, G., & Holstein, T. (2025). Delegating Responsibilities to Intelligent Autonomous Systems: Challenges and Benefits. Journal of Bioethical Inquiry. https://doi.org/10.1007/s11673-025-10428-5

Gema, A. J. (2022). Perlindungan Data Pribadi dalam Penggunaan Teknologi Informasi di Indonesia. Jurnal Hukum & Pembangunan, 1(1). https://doi.org/10.21143/telj.vol1.no1.1000

Hagendorff, T. (2022). A Virtue-Based Framework to Support Putting AI Ethics into Practice. Philosophy and

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 348-354

Technology, 35(3). https://doi.org/10.1007/s13347-022-00553-z
Hananto, V. A. (2025). Utilitarianisme dan Keseimbangan antara Kepentingan Umum dan Kepentingan Individu. Jurnal Hukum Ius Quia Iustum, 32(1), 72–98. https://doi.org/10.20885/Iustum.Vol32.Iss1.Art4
IEEE (Institute of Electrical and Electronics Engineers). (2025). IEEE Code of Ethics. Retrieved from https://www.ieee.org/about/corporate/governance/ethics.html
Kode Etik Profesi Teknologi Informasi dan Komputer Indonesia. Jakarta: APTIKOM Press.
Kompas.com. (2024). Pakar Siber Ungkap Risiko Serius di Balik Kebocoran Data BSI. Retrieved from https://www.kompas.com/tren
Media Indonesia. (2024). Kebocoran Data Bank Syariah Indonesia Diduga Akibat Serangan Siber LockBit Ransomware. Retrieved from https://www.mediaindonesia.com/teknologi
Otoritas Jasa Keuangan (OJK). (2023). Peraturan OJK tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Jakarta: OJK.
Pant, A., Hoda, R., Spiegler, S. V., Tantithamthavorn, C., & Turhan, B. (2024). Ethics in the Age of AI: An Analysis of AI Practitioners' Awareness and Challenges. ACM Transactions on Software Engineering and Methodology, 33(3). https://doi.org/10.1145/3635715
Philosophical Studies, 182(7), 1681–1704. https://doi.org/10.1007/s11098- 024-02174-Y
Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022). Jakarta: Kementerian Hukum dan HAM Republik Indonesia.