KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa
Vol.4, No.1 Januari 2026
e-ISSN: 3025-5465; p-ISSN: 3025-7964, Hal 666-676
DOI : https://doi.org/10.61722/jipm.v4i1.1951.

Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data

Fadli[1],Satya Agung Hardiansyah[3],Tata Sutabri
[123]Teknik Elektro, Fakultas Sains Teknologi Universitas Bina Darma
Alamat: Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111
Korespondensi penulis: fadlimarabes05@gmail.com,agungsatia457@gmail.com,tata.sutabri@gmail.com

Abstract. *The rapid development of information technology in Indonesia has been accompanied by various ethical violations that harm society. This research analyzes cases of IT ethics violations in Indonesia and their impacts on users and prevention efforts. Using a qualitative approach with case study methods, data was collected through literature studies, news analysis, and documentation of IT ethics violation cases from 2020-2024. The findings revealed several significant cases including personal data breaches in e-commerce and health applications, misuse of personal data for commercial purposes without permission, and weak data protection across various sectors. The main factors are lack of awareness about IT ethics importance, weak regulations and law enforcement, and minimal investment in data security systems. IT ethics violations in Indonesia require comprehensive handling through regulatory strengthening, digital literacy improvement, and organizational commitment in implementing IT ethics principles.*
Keywords: *data breach; digital privacy; information security; IT ethics; Indonesia*

Abstrak. Perkembangan teknologi informasi di Indonesia mengalami pertumbuhan pesat, namun diikuti dengan berbagai kasus pelanggaran etika yang merugikan masyarakat. Penelitian ini menganalisis kasus-kasus pelanggaran etika IT yang terjadi di Indonesia dan dampaknya terhadap pengguna serta upaya pencegahan yang dapat dilakukan. Menggunakan metode kualitatif dengan pendekatan studi kasus, data dikumpulkan melalui studi literatur, analisis berita, dan dokumentasi kasus pelanggaran etika IT periode 2020-2024. Ditemukan beberapa kasus signifikan seperti kebocoran data pribadi pengguna e-commerce dan aplikasi kesehatan, penyalahgunaan data pribadi untuk kepentingan komersial tanpa izin, serta lemahnya perlindungan data di berbagai sektor. Faktor utama penyebab adalah kurangnya kesadaran pentingnya etika IT, lemahnya regulasi dan penegakan hukum, serta minimnya investasi pada sistem keamanan data. Pelanggaran etika IT di Indonesia memerlukan penanganan komprehensif melalui penguatan regulasi, peningkatan literasi digital, dan komitmen organisasi dalam menerapkan prinsip etika IT.
Kata kunci: etika IT; Indonesia; kebocoran data; keamanan informasi; privasi digital.

Received November 30, 2025; Revised Desember 29, 2025; Januari 03, 2026
* Fadli, fadlimarabes05@email.com

LATAR BELAKANG

Teknologi informasi telah menjadi bagian integral dari kehidupan masyarakat Indonesia. Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai lebih dari 215 juta jiwa pada tahun 2023 (Sadya, 2023). Pertumbuhan pesat ini membawa dampak positif dalam berbagai aspek kehidupan, namun juga menimbulkan permasalahan terkait etika penggunaan teknologi informasi. Etika IT merujuk pada seperangkat prinsip moral yang mengatur penggunaan teknologi informasi secara bertanggung jawab, mencakup privasi, keamanan data, kejujuran, keadilan, dan tanggung jawab sosial.

Badan Siber dan Sandi Negara (BSSN) melalui Lanskap Keamanan Siber Indonesia 2022 menyebutkan bahwa berdasarkan hasil assessment yang dilakukan pada tahun 2022 ditemukan sebanyak 1.950 celah keamanan dari 457 sistem elektronik pada berbagai aplikasi yang digunakan oleh masyarakat secara luas (Yusuf, Arianto, & Amanda, 2022). Berbagai kasus pelanggaran etika IT masih sering terjadi di Indonesia, mulai dari kebocoran data pribadi, penyalahgunaan informasi, hingga kejahatan siber. Beberapa kasus besar yang menarik perhatian publik antara lain kebocoran data 1,3 miliar penduduk Indonesia dari Pusat Data Nasional (PDN) pada tahun 2024, kebocoran data pengguna e-commerce dan aplikasi transportasi online, serta berbagai kasus penipuan online yang memanfaatkan kelemahan sistem keamanan digital.

Penelitian yang dilakukan oleh Ghozali, Kusrini, dan Sudarmawan (2019) dalam mendeteksi kerentanan keamanan aplikasi website sistem informasi dengan metode OWASP menemukan 12 celah keamanan dengan berbagai tingkat risiko. Penelitian lain oleh Aryanti, Nurholis, dan Utamajaya (2021) menggunakan tools Acunetix Web Vulnerability Scanner dalam mengidentifikasi celah keamanan, ditemukan 7 celah keamanan dengan berbagai tingkat risiko. Namun penelitian tersebut hanya sebatas penilaian tingkat risiko keparahan tanpa menggambarkan dampak serta rekomendasi perbaikan dari celah keamanan yang ditemukan secara komprehensif.

Tujuan dari penelitian ini adalah untuk mengidentifikasi bentuk-bentuk pelanggaran etika IT yang terjadi di Indonesia, menganalisis faktor-faktor penyebab pelanggaran etika IT, mengevaluasi dampak pelanggaran etika IT terhadap berbagai pihak, serta merumuskan rekomendasi untuk meningkatkan kesadaran dan kepatuhan

terhadap etika IT. Kebaruan penelitian ini terletak pada analisis komprehensif yang tidak hanya mengidentifikasi jenis pelanggaran, tetapi juga memberikan penilaian dampak risiko yang ditimbulkan dan rekomendasi perbaikan yang aplikatif untuk konteks Indonesia.

KAJIAN TEORITIS

Etika teknologi informasi adalah cabang dari etika terapan yang membahas isu-isu moral yang timbul dari penggunaan teknologi informasi dan komunikasi. Menurut Mason (1986), terdapat empat isu utama dalam etika IT yang dikenal dengan akronim PAPA yaitu Privacy (privasi), Accuracy (akurasi), Property (kepemilikan), dan Accessibility (aksesibilitas). Privacy berkaitan dengan hak individu untuk mengontrol informasi pribadi mereka. Accuracy menyangkut kebenaran, keandalan, dan integritas informasi. Property berkaitan dengan hak kepemilikan intelektual atas informasi dan perangkat lunak. Accessibility menyangkut keadilan dalam akses terhadap teknologi informasi.

Gotterbarn (1999) mengidentifikasi beberapa prinsip etika yang harus dipegang oleh profesional IT mencakup tanggung jawab publik, kompetensi profesional, integritas, kerahasiaan, dan kualitas produk. Dalam konteks keamanan informasi, upaya untuk menghindari kejadian yang tidak diinginkan seperti hilangnya kerahasiaan atau integritas data menjadi sangat penting. Jika aset teknologi informasi mendapat ancaman dan serangan baik dari dalam maupun dari luar maka dapat menimbulkan risiko yang mengganggu dalam proses bisnis bahkan juga dapat menghentikan proses bisnis (Candra, Sari, Iskandar, & Yanto, 2019).

Indonesia telah memiliki beberapa regulasi terkait etika dan keamanan teknologi informasi. UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengatur berbagai aspek penggunaan teknologi informasi termasuk perlindungan data pribadi dan sanksi bagi pelaku kejahatan siber. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) memberikan kerangka hukum yang komprehensif untuk perlindungan data pribadi di Indonesia,

termasuk hak-hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi pelanggaran.

Beberapa penelitian sebelumnya telah membahas topik etika IT di Indonesia. Nurul, Anggrainy, dan Aprelyani (2022) dalam penelitiannya tentang faktor-faktor yang mempengaruhi etika sistem informasi menemukan bahwa moral, isu sosial, dan etika masyarakat memiliki peran penting dalam membentuk perilaku etis dalam penggunaan teknologi informasi. Sutabri, Wijaya, Herdiansyah, dan Negara (2024) melakukan evaluasi risiko celah keamanan aplikasi E-Office menggunakan metode OWASP dan menemukan 38 celah keamanan dengan 18 diantaranya masuk dalam kriteria OWASP Top 10, yang menunjukkan bahwa celah keamanan dalam aplikasi pemerintahan meliputi kerentanan pada tingkat otentifikasi, akses kontrol, konfigurasi, serta proses validasi data.

Wijaya (2024) meneliti implementasi UU Perlindungan Data Pribadi di sektor perbankan Indonesia dan mengidentifikasi berbagai tantangan dalam penerapannya, termasuk keterbatasan sumber daya dan resistensi organisasional. Penelitian-penelitian tersebut menunjukkan bahwa meskipun regulasi telah ada, implementasi dan penegakan masih menjadi tantangan utama di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Pendekatan ini dipilih karena memungkinkan peneliti untuk memahami fenomena pelanggaran etika IT secara mendalam dalam konteks nyata. Data dalam penelitian ini berasal dari data primer yang mencakup dokumentasi kasus pelanggaran etika IT yang dilaporkan di media massa, laporan dari lembaga perlindungan konsumen, dan data dari Kementerian Komunikasi dan Informatika. Data sekunder berasal dari literatur ilmiah, jurnal, buku, artikel, dan penelitian terdahulu yang membahas topik etika IT dan kasus-kasus terkait.

Teknik pengumpulan data yang digunakan meliputi studi literatur untuk mengkaji berbagai sumber tertulis guna memahami konsep etika IT dan kasus-kasus yang terjadi, analisis dokumen untuk menganalisis laporan, berita, dan dokumentasi resmi terkait kasus pelanggaran etika IT, serta content analysis untuk menganalisis isi berita dan laporan untuk mengidentifikasi pola dan tema umum dalam kasus pelanggaran etika IT.

Data yang terkumpul dianalisis menggunakan teknik analisis konten kualitatif dengan langkah-langkah pengumpulan data, reduksi data dengan memilih dan menyederhanakan data yang relevan dengan fokus penelitian, display data dengan menyajikan data dalam bentuk tabel atau narasi untuk memudahkan analisis, kategorisasi dengan mengelompokkan kasus berdasarkan jenis pelanggaran etika IT, interpretasi dengan menganalisis makna dan implikasi dari temuan penelitian, serta verifikasi untuk memastikan validitas temuan melalui triangulasi sumber data. Penelitian ini menggunakan kerangka PAPA dari Mason sebagai dasar analisis kasus pelanggaran etika IT di Indonesia. Setiap kasus yang teridentifikasi dikategorikan berdasarkan aspek etika yang dilanggar.

HASIL DAN PEMBAHASAN

Identifikasi Kasus Pelanggaran Etika IT di Indonesia

Berdasarkan analisis data yang dilakukan, ditemukan beberapa kategori utama pelanggaran etika IT yang terjadi di Indonesia periode 2020-2024. Kategorisasi ini menggunakan framework PAPA (Privacy, Accuracy, Property, Accessibility) dari Mason sebagai dasar analisis.

Kebocoran Data Pribadi (Privacy Violation)

Kasus Kebocoran Data Pusat Data Nasional (2024) merupakan salah satu kasus kebocoran data terbesar dalam sejarah Indonesia. Data 1,3 miliar penduduk Indonesia diduga bocor dan diperjualbelikan di dark web. Data yang bocor mencakup Nomor Induk Kependudikan (NIK), nama lengkap, alamat, dan informasi pribadi lainnya. Kasus ini menunjukkan lemahnya sistem keamanan infrastruktur digital pemerintah. Beberapa platform e-commerce besar di Indonesia juga mengalami kebocoran data pengguna yang mencakup informasi nama, alamat email, nomor telepon, dan riwayat transaksi. Data tersebut kemudian diperjualbelikan secara ilegal dan digunakan untuk penipuan.

Banyak aplikasi pinjaman online ilegal yang menyalahgunakan akses ke data pribadi pengguna, termasuk kontak telepon, foto, dan lokasi. Data ini kemudian digunakan untuk intimidasi dan penagihan yang melanggar privasi. Temuan ini sejalan dengan penelitian Rochman, Salam, dan Maulana (2021) yang mengidentifikasi berbagai celah keamanan dalam sistem informasi rumah sakit yang dapat menyebabkan kebocoran data pasien.

Penyalahgunaan Data (Accuracy & Property Violation)

Beberapa perusahaan teknologi terbukti memanipulasi algoritma dan data pengguna untuk kepentingan bisnis tanpa persetujuan. Hal ini melanggar prinsip akurasi dan kepemilikan data. Platform media sosial menjadi sarana penyebaran informasi yang tidak akurat dan menyesatkan. Meskipun bukan sepenuhnya tanggung jawab platform, lemahnya kurasi konten menunjukkan kurangnya komitmen terhadap prinsip akurasi informasi.

Pembajakan dan Pelanggaran Hak Kekayaan Intelektual

Indonesia masih memiliki tingkat pembajakan software yang tinggi. Banyak organisasi dan individu menggunakan software tanpa lisensi resmi, yang merugikan pemegang hak cipta. Maraknya pencurian konten digital seperti film, musik, dan e-book yang didistribusikan tanpa izin melalui berbagai platform online juga menjadi permasalahan serius.

Kesenjangan Akses Digital (Accessibility Issues)

Masih terdapat kesenjangan akses terhadap teknologi informasi antara wilayah urban dan rural, serta antara kelompok ekonomi berbeda. Hal ini menimbulkan ketidakadilan dalam pemanfaatan teknologi. Banyak layanan digital yang tidak dirancang dengan mempertimbangkan kebutuhan penyandang disabilitas, melanggar prinsip aksesibilitas universal.

Faktor Penyebab Pelanggaran Etika IT

Berdasarkan analisis kasus-kasus di atas, dapat diidentifikasi beberapa faktor penyebab utama yang dikategorikan menjadi faktor teknis, faktor manusia, faktor organisasi, dan faktor regulasi.

Dari segi faktor teknis, banyak organisasi termasuk lembaga pemerintah tidak menerapkan standar keamanan informasi yang memadai. Investasi pada infrastruktur keamanan masih rendah. Data sensitif sering disimpan tanpa enkripsi yang memadai, memudahkan peretas untuk mengakses informasi. Masih banyaknya penggunaan sistem lama yang memiliki celah keamanan dan tidak mendapat update secara berkala. Temuan ini didukung oleh penelitian Sutabri et al. (2024) yang menemukan 38 celah keamanan pada aplikasi E-Office dengan berbagai tingkat risiko yang disebabkan oleh kerentanan teknis.

Faktor manusia mencakup pengguna dan bahkan profesional IT yang masih kurang memahami pentingnya praktik keamanan dasar seperti penggunaan password yang kuat dan two-factor authentication. Pendidikan formal dan pelatihan profesional tentang etika IT masih minim, menyebabkan praktisi tidak memahami implikasi etis dari tindakan mereka. Masih adanya pandangan bahwa pembajakan software adalah hal yang wajar dan dapat diterima menunjukkan budaya permisif yang perlu diubah.

Dari faktor organisasi, banyak organisasi memprioritaskan pertumbuhan bisnis dan profit tanpa mempertimbangkan aspek etika dan perlindungan data pengguna. Tidak semua organisasi memiliki kebijakan yang jelas tentang pengelolaan data dan etika IT. Anggaran untuk keamanan informasi masih dianggap sebagai cost center, bukan investasi strategis. Hal ini sejalan dengan temuan Fachrezi, Cahyono, dan Tanaem (2021) yang mengidentifikasi bahwa manajemen risiko keamanan aset teknologi informasi masih belum optimal di banyak instansi pemerintah.

Faktor regulasi mencakup meskipun regulasi sudah ada, penegakan hukum masih lemah dan sanksi tidak memberikan efek jera. Perkembangan teknologi yang sangat cepat membuat regulasi sering tertinggal dan tidak mampu mengantisipasi isu-isu baru.

Kurangnya koordinasi antara lembaga pemerintah dalam pengawasan dan penegakan aturan terkait IT juga menjadi hambatan.

Dampak Pelanggaran Etika IT

Pelanggaran etika IT menimbulkan dampak yang luas dan serius bagi berbagai pihak. Dampak terhadap individu mencakup kerugian finansial dimana korban kebocoran data sering mengalami kerugian finansial akibat penipuan dan penyalahgunaan informasi. Kehilangan privasi terjadi ketika data pribadi yang bocor dapat disalahgunakan untuk berbagai keperluan tanpa sepengetahuan pemilik. Korban intimidasi dari debt collector pinjol atau korban penipuan online mengalami tekanan psikologis yang berat. Masyarakat menjadi tidak percaya terhadap layanan digital, menghambat adopsi teknologi.

Dampak terhadap organisasi sangat signifikan dimana organisasi yang mengalami kebocoran data mengalami kerusakan reputasi yang sulit dipulihkan. Biaya untuk menangani insiden keamanan, kompensasi kepada korban, dan denda regulasi dapat sangat besar. Pelanggan beralih ke kompetitor yang dianggap lebih dapat menjaga keamanan data. Organisasi dapat menghadapi tuntutan hukum dan sanksi dari regulator.

Dampak terhadap masyarakat dan negara mencakup ketidakpercayaan masyarakat yang menghambat program transformasi digital pemerintah dan ekonomi digital. Pembajakan software dan konten digital merugikan industri kreatif dan teknologi nasional. Kebocoran data skala besar dapat mengancam keamanan nasional dan kedaulatan data. Kurangnya kepercayaan terhadap teknologi digital membuat kesenjangan digital semakin lebar.

Upaya Pencegahan dan Penanganan

Untuk mengatasi permasalahan pelanggaran etika IT, diperlukan upaya komprehensif dari berbagai pihak. Penguatan regulasi dan penegakan hukum menjadi prioritas utama. Pemerintah perlu memastikan UU Perlindungan Data Pribadi diimplementasikan secara efektif dengan sosialisasi, pengawasan, dan penegakan sanksi yang tegas. Menetapkan standar minimum keamanan informasi yang wajib diterapkan oleh semua organisasi yang mengelola data pribadi. Meningkatkan kemampuan aparat penegak hukum dalam menangani kejahatan siber dan pelanggaran etika IT. Memperkuat peran lembaga pengawas seperti Kominfo dan membentuk otoritas independen untuk perlindungan data pribadi.

Peningkatan kesadaran dan literasi digital dapat dilakukan melalui kampanye masif tentang pentingnya keamanan data dan etika IT kepada masyarakat. Memasukkan materi etika IT dalam kurikulum pendidikan formal dari tingkat dasar hingga perguruan tinggi. Mengembangkan program sertifikasi etika IT untuk profesional teknologi informasi. Mendorong organisasi untuk memberikan pelatihan reguler tentang etika dan keamanan IT kepada karyawan. Penelitian Listartha, Mitha, Arta, dan Arimika (2022) menunjukkan bahwa pelatihan dan edukasi tentang keamanan website dapat meningkatkan kesadaran akan pentingnya perlindungan data.

Peningkatan kapasitas teknis meliputi mendorong organisasi untuk meningkatkan investasi pada infrastruktur dan sistem keamanan informasi. Menerapkan standar internasional seperti ISO 27001 untuk manajemen keamanan informasi. Menerapkan prinsip keamanan sejak tahap perancangan sistem, bukan sebagai tambahan di akhir.

Melakukan audit keamanan secara rutin untuk mengidentifikasi dan memperbaiki celah keamanan. Guntoro, Costaner, dan Musfawati (2020) dalam penelitiannya menunjukkan pentingnya penggunaan metode ISSAF dan OWASP dalam menganalisis keamanan web server untuk mengidentifikasi dan memperbaiki celah keamanan.

Penguatan tanggung jawab korporat mencakup setiap organisasi harus memiliki kebijakan etika IT yang jelas dan mengikat. Menunjuk petugas khusus yang bertanggung jawab atas perlindungan data pribadi. Menerbitkan laporan transparansi tentang pengelolaan data dan insiden keamanan. Menyediakan saluran yang aman bagi karyawan dan pengguna untuk melaporkan pelanggaran etika.

Kolaborasi multi-stakeholder sangat diperlukan dengan membangun kerjasama antara pemerintah dan sektor swasta dalam meningkatkan keamanan siber nasional. Melibatkan perguruan tinggi dalam penelitian dan pengembangan solusi keamanan informasi. Memberdayakan organisasi masyarakat sipil untuk mengawasi dan mengadvokasi perlindungan data pribadi. Berkolaborasi dengan negara lain dalam pertukaran informasi dan best practices tentang etika IT. Marzuki, Herdiansyah, Negara, dan Sutabri (2023) menunjukkan pentingnya kolaborasi berbagai pihak dalam implementasi layanan digital e-government yang aman dan efektif.

Analisis dan Diskusi

Hasil penelitian menunjukkan bahwa pelanggaran etika IT di Indonesia merupakan masalah kompleks yang melibatkan berbagai faktor teknis, manusia, organisasi, dan regulasi. Kasus-kasus yang terjadi tidak hanya merugikan individu, tetapi juga mengancam kepercayaan publik terhadap ekosistem digital nasional. Menariknya, meskipun Indonesia telah memiliki kerangka regulasi yang cukup komprehensif dengan adanya UU ITE dan UU PDP, implementasi dan penegakan masih menjadi tantangan utama.

Faktor budaya juga berperan penting. Masih adanya budaya permisif terhadap pembajakan dan pandangan bahwa data adalah komoditas gratis yang dapat dieksploitasi menunjukkan perlunya transformasi mindset yang fundamental. Ini memerlukan pendekatan holistik yang tidak hanya mengandalkan regulasi, tetapi juga edukasi dan pembangunan kesadaran kolektif. Dari perspektif teknis, banyak organisasi di Indonesia masih menganggap keamanan informasi sebagai biaya, bukan investasi strategis. Paradigma ini perlu diubah, terutama mengingat besarnya dampak finansial dan reputasi dari insiden keamanan.

Peran ekosistem digital juga penting. Platform teknologi besar memiliki tanggung jawab tidak hanya kepada pemegang saham, tetapi juga kepada pengguna dan masyarakat luas. Prinsip stakeholder capitalism perlu lebih ditekankan dalam konteks etika IT, di mana kesejahteraan pengguna dan perlindungan data harus menjadi prioritas utama, bukan hanya profit.

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa pelanggaran etika IT di Indonesia mencakup empat kategori utama berdasarkan framework PAPA yaitu pelanggaran privasi seperti kebocoran data, pelanggaran akurasi seperti manipulasi data dan hoaks, pelanggaran kepemilikan seperti pembajakan

software, dan pelanggaran aksesibilitas seperti kesenjangan digital. Pelanggaran terjadi akibat kombinasi faktor teknis seperti sistem keamanan lemah, faktor manusia seperti kesadaran rendah, faktor organisasi seperti prioritas profit, dan faktor regulasi seperti penegakan hukum lemah. Pelanggaran etika IT menimbulkan dampak serius bagi individu berupa kerugian finansial dan privasi, organisasi berupa kerusakan reputasi dan finansial, serta masyarakat dan negara berupa hambatan transformasi digital dan ancaman keamanan nasional. Mengatasi masalah ini memerlukan pendekatan holistik yang melibatkan penguatan regulasi, peningkatan literasi digital, investasi teknis, tanggung jawab korporat, dan kolaborasi multi-stakeholder. Kasus-kasus yang terjadi menunjukkan urgensi tinggi untuk segera mengambil tindakan konkret sebelum kepercayaan publik terhadap ekosistem digital Indonesia semakin terkikis.

Berdasarkan kesimpulan tersebut, beberapa saran direkomendasikan. Untuk pemerintah, perlu mempercepat implementasi UU PDP dengan menerbitkan peraturan pelaksana yang jelas dan operasional, meningkatkan anggaran dan kapasitas lembaga pengawas perlindungan data pribadi, melakukan kampanye nasional tentang literasi digital dan keamanan data, memperkuat koordinasi antar-lembaga dalam penegakan hukum terkait kejahatan siber, serta memberikan insentif bagi organisasi yang menerapkan standar keamanan informasi tinggi. Untuk organisasi atau perusahaan, perlu menjadikan etika IT dan keamanan data sebagai prioritas strategis bukan sekadar compliance, mengalokasikan anggaran memadai untuk investasi sistem keamanan informasi, menerapkan prinsip privacy by design dalam pengembangan produk dan layanan, memberikan pelatihan berkala tentang etika dan keamanan IT kepada seluruh karyawan, serta membangun budaya organisasi yang menghargai privasi dan etika digital. Untuk institusi pendidikan, perlu mengintegrasikan materi etika IT dalam kurikulum program studi teknologi informasi, mengembangkan program sertifikasi etika IT untuk mahasiswa dan profesional, melakukan penelitian lanjutan tentang tren dan tantangan etika IT di Indonesia, membangun kerjasama dengan industri untuk menjembatani gap antara teori dan praktik, serta menyelenggarakan seminar dan workshop tentang etika IT secara berkala. Untuk masyarakat, perlu meningkatkan kesadaran tentang pentingnya melindungi data pribadi, belajar menggunakan fitur keamanan seperti password yang kuat dan two-factor authentication, lebih selektif dalam memberikan izin akses aplikasi terhadap data pribadi, melaporkan dugaan pelanggaran privasi dan keamanan data kepada pihak berwenang, serta mendukung dan menggunakan produk atau layanan yang menghargai privasi pengguna.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan. Cakupan data penelitian fokus pada kasus-kasus yang terpublikasi di media, sehingga kemungkinan ada banyak kasus lain yang tidak terdeteksi. Analisis terbatas pada periode 2020-2024, sehingga tidak mencakup perkembangan terbaru setelah periode tersebut. Keterbatasan metode kualitatif dalam generalisasi hasil ke populasi yang lebih luas juga perlu dipertimbangkan. Tidak semua aspek teknis dari setiap kasus dapat dianalisis secara mendalam karena keterbatasan akses informasi. Untuk memperkaya pemahaman tentang etika IT di Indonesia, penelitian lanjutan dapat dilakukan dengan fokus pada studi kuantitatif tentang tingkat kesadaran etika IT di berbagai sektor industri, analisis komparatif implementasi regulasi perlindungan data antara Indonesia dengan negara lain, penelitian tentang efektivitas program edukasi etika IT di institusi pendidikan, studi longitudinal tentang dampak jangka panjang dari kebocoran data terhadap korban, serta penelitian aksi untuk mengembangkan model pendidikan etika IT yang kontekstual.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Bina Darma yang telah memberikan dukungan dalam pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada semua pihak yang telah membantu dalam proses pengumpulan data dan penyusunan artikel ini.

DAFTAR REFERENSI

Aryanti, D., Nurholis, & Utamajaya, J. N. (2021). Analisis kerentanan keamanan website menggunakan metode OWASP (Open Web Application Security Project) pada Dinas Tenaga Kerja. *Jurnal Nasional Indonesia*, *1*(3), 15–25. https://doi.org/10.54543/fusion.v1i03.53

Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (2019). Sistem manajemen risiko keamanan aset teknologi informasi menggunakan ISO 31000:2018. *Jurnal CoreIT*, *5*(1), 19–28.

Fachrezi, M. I., Cahyono, A. D., & Tanaem, P. F. (2021). Manajemen risiko keamanan aset teknologi informasi menggunakan ISO 31000:2018 Diskominfo Kota Salatiga. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *8*(2), 764–773. https://doi.org/10.35957/jatisi.v8i2.789

Ghozali, B., Kusrini, & Sudarmawan. (2019). Mendeteksi kerentanan keamanan aplikasi website menggunakan metode OWASP (Open Web Application Security Project) untuk penilaian risk rating. *Creative Information Technology Journal*, *4*(4), 264–275. https://doi.org/10.24076/citec.2017v4i4.119

Gotterbarn, D. (1999). How the new software engineering code of ethics affects you. *IEEE Software*, *16*(6), 58-64.

Guntoro, Costaner, L., & Musfawati. (2020). Analisis keamanan web server Open Journal System (OJS) menggunakan metode ISSAF dan OWASP (Studi kasus OJS Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *5*(1), 45–55. https://doi.org/10.29100/jipi.v5i1.1565

Gustian, D. (2023). *Keamanan sistem informasi*. Bandung: Indie Press.

Hidayat, R., & Setiawan, A. (2022). Analisis kesadaran etika teknologi informasi pada mahasiswa program studi informatika. *Jurnal Teknologi Informasi dan Pendidikan*, *15*(2), 145-158.

Kementerian Komunikasi dan Informatika. (2024). *Laporan Insiden Keamanan Siber Indonesia 2023*. Jakarta: Kominfo.

Listartha, I. M. E., Mitha, I. M. A. P., Arta, M. W. A., & Arimika, I. K. W. Y. (2022). Analisis kerentanan website SMA Negeri 2 Amlapura menggunakan metode OWASP (Open Web Application Security Project). *Simkom*, *7*(1), 23–27. https://doi.org/10.51717/simkom.v7i1.63

Marzuki, M., Herdiansyah, M. I., Negara, E. S., & Sutabri, T. (2023). Analisis layanan digital SP4N LAPOR e-government pada pemerintahan Kota Pagaralam

menggunakan model Delone and McLean. *Jurnal Teknologi Informatika dan Komputer*, *9*(2), 1189–1203. https://doi.org/10.37012/jtik.v9i2.1787

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5-12.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi etika sistem informasi: Moral, isu sosial dan etika masyarakat (Literature review SIM). *Jurnal Ekonomi Manajemen dan Sistem Informasi*, *3*(2), 520–529. https://doi.org/10.38035/jmpis.v3i2.1115

Pratama, D., Wijaya, S., & Kusuma, H. (2023). Kebocoran data e-commerce di Indonesia: Analisis faktor penyebab dan dampak. *Jurnal Sistem Informasi dan Keamanan*, *8*(1), 22-35.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Sekretariat Negara.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Sekretariat Negara.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jakarta: Sekretariat Negara.

Rochman, A., Salam, R. R., & Maulana, S. A. (2021). Analisis keamanan website dengan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di Rumah Sakit XYZ. *Jurnal Indonesia Sosial Teknologi*, *2*(4), 506–519. https://doi.org/10.36418/jist.v2i4.124

Sadya, S. (2023). APJII: Pengguna internet Indonesia 215,63 juta pada 2022-2023. Diakses dari https://dataindonesia.id/internet/detail/apjii-pengguna-internet-indonesia-21563-juta-pada-20222023

Sayuthi. (2021). Konsep pengendalian intern untuk keamanan sistem informasi. *Al-Buhuts*, *17*(2), 290–308. https://doi.org/10.30603/ab.v17i2.2370

Spinello, R. A. (2020). *Up and out of poverty: The social marketing solution* (6th ed.). Burlington: Jones & Bartlett Learning.

Sutabri, T., Wijaya, A., Herdiansyah, M. I., & Negara, E. S. (2024). Evaluasi risiko celah keamanan aplikasi E-Office menggunakan metode OWASP. *Edumatic: Jurnal Pendidikan Informatika*, *8*(1), 113-122. https://doi.org/10.29408/edumatic.v8i1.25463

Tavani, H. T. (2016). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (5th ed.). Hoboken: John Wiley & Sons.

Wijaya, B. (2024). Implementasi undang-undang perlindungan data pribadi di sektor perbankan Indonesia: Tantangan dan strategi. *Jurnal Hukum Teknologi*, *12*(1), 78-94.

Yusuf, A., Arianto, T., & Amanda, C. D. (2022). *Lanskap Keamanan Siber Indonesia 2022*. Jakarta: Badan Siber dan Sandi Negara (BSSN).