Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer
Volume. 6 Nomor. 2 Juli 2026
E-ISSN :2827-7953; P-ISSN : 2827-8135, Hal 525-537
DOI: https://doi.org/10.55606/juisik.v6i2.2541
Tersedia: https://journal.sinov.id/index.php/juisik

Analisis Pelanggaran Etika Profesi TI dalam Penyalahgunaan Data Pengguna pada Aplikasi Mobile

Nadwa Meilan Iffa[1*], Evy Nurmiati[2]
[1-2]Universitas Islam Negeri Syarif Hidayatullah, Indonesia
Email: nadwa.meilan24@mhs.uinjkt.ac.id [1], evy.nurmiati@uinjkt.ac.id [2]
[*]*Penulis Korespondensi: nadwa.meilan24@mhs.uinjkt.ac.id*

Abstract. *Rapid growth of mobile applications in the digital era has significantly improved public access to various services. However, this development has simultaneously increased the risk of personal data misuse within the digital ecosystem. This study aims to identify and analyze various forms of violations of Information Technology (IT) professional ethics that are likely to occur throughout the processes of collecting, processing, storing, and sharing user data on mobile application platforms. This research employed a qualitative descriptive approach through a literature review. The analysis was conducted by comprehensively examining data management practices based on the fundamental principles of IT professional ethics, the provisions of Indonesia's Personal Data Protection Law (PDP Law), and internationally recognized mobile application security standards. The findings reveal that the most common ethical violations include excessive or unnecessary data collection beyond the application's primary functions, non-transparent and misleading user consent mechanisms, unauthorized sharing of personal data with third parties, inadequate data storage protection leading to security breaches, and large-scale exploitation of user data to manipulate user behavior for commercial purposes. These unethical practices directly violate the principles of responsibility, integrity, confidentiality, fairness, and information security. Consequently, to maintain public trust and minimize the risk of cybercrime, mobile application developers and service providers are strongly encouraged to adopt privacy-by-design principles, implement strict data minimization practices, strengthen multilayered technical security controls, and establish privacy policies that are transparent, accessible, and easily understood by all users.*

Keywords: *Accountability; Data Misuse; Information Technology Ethics; Mobile Applications; User Privacy.*

Abstrak. Pertumbuhan pesat aplikasi mobile di masa digital dikala ini sudah bawa kemudahan akses layanan untuk warga luas, tetapi secara bertepatan keadaan ini pula tingkatkan resiko penyalahgunaan informasi individu pengguna secara signifikan di ekosistem digital. Riset ini bertujuan buat mengenali serta menganalisis bermacam wujud pelanggaran etika profesi Teknologi Data (TI) yang rentan terjalin dalam aplikasi pengumpulan, pemrosesan, penyimpanan, sampai pembagian informasi pengguna pada platform aplikasi mobile. Pendekatan yang digunakan dalam riset ini merupakan riset literatur dengan tipe kualitatif- deskriptif. Analisis dicoba secara mendalam dengan mengevaluasi aplikasi pengelolaan informasi di lapangan bersumber pada prinsip bawah etika profesi TI, syarat Undang- Undang Pelindungan Informasi Individu (UU PDP), dan standar keamanan teknis aplikasi mobile secara global. Hasil kajian secara komprehensif menampilkan kalau pelanggaran etika yang gempar terjalin meliputi pengumpulan informasi yang dinilai kelewatan ataupun tidak cocok guna utama, mekanisme persetujuan pengguna yang tidak transparan serta membingungkan, distribusi informasi kepada pihak ketiga tanpa bawah izin yang legal, lemahnya sistem proteksi penyimpanan yang merangsang kebocoran, dan eksploitasi informasi yang masif buat manipulasi sikap pengguna demi keuntungan komersial. Praktik- praktik negatif tersebut secara langsung mencederai prinsip tanggung jawab, kejujuran, kerahasiaan, keadilan, serta keamanan data. Selaku implikasinya, buat melindungi keyakinan warga serta meminimalisasi resiko kejahatan digital, para pengembang dan pengelola aplikasi mobile sangat dituntut buat mengadopsi prinsip desain berbasis pribadi, mempraktikkan minimalisasi informasi yang ketat, tingkatkan kontrol keamanan teknis secara berlapis, dan menyusun kebijakan pribadi yang sangat transparan serta gampang dimengerti oleh segala golongan pengguna.

Kata kunci: Aplikasi Mobile; Etika Profesi TI; Penyalahgunaan Data; Privasi Pengguna; Tanggung Jawab.

1. LATAR BELAKANG

Aplikasi mobile telah muncul sebagai aspek penting dari fungsi masyarakat saat ini. Pengguna terlibat dengan aplikasi ini untuk memfasilitasi komunikasi, pengadaan transportasi, melaksanakan transaksi keuangan, mengejar peluang pendidikan, berbelanja, dan mendapatkan

Naskah Masuk: 15 April 2026; Revisi:28 Mei 2026; Diterima: 02 Juni 2026; Terbit: 09 Juli 2026

layanan kesehatan. Frekuensi pemanfaatan aplikasi yang meningkat membuat data pribadi menjadi aset penting dalam ekosistem digital. Di Indonesia, Asosiasi Penyedia Layanan Internet Indonesia

(APJII) melaporkan bahwa pada tahun 2024, jumlah pengguna internet mencapai 221.563.479 orang, mencerminkan tingkat penetrasi sebesar 79,5%. Keadaan ini menggarisbawahi potensi besar data yang diproses oleh platform digital, termasuk aplikasi mobile.

Data pengguna dalam aplikasi mobile dapat mencakup berbagai informasi seperti nama, nomor telepon, alamat email, lokasi geografis, daftar kontak, riwayat transaksi, perilaku pencarian, spesifikasi perangkat, data biometrik, dan informasi keuangan. Sangat penting bahwa data tersebut diproses dengan uji tuntas, karena memiliki kapasitas untuk mengidentifikasi individu, baik secara langsung maupun tidak langsung melalui penggabungannya dengan data lain. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menggambarkan data pribadi sebagai informasi yang berkaitan dengan individu yang dapat diidentifikasi, baik secara independen maupun dalam hubungannya dengan informasi lainnya. Perlindungan Data pribadi merupakan hak asasi manusia sebagai bagian dari hak *privacy* yang mendapatkan jaminan perlindungan baik instrument hukum internasional dan konstitusi negara (Arrasuli & Fahmi, 2023).

Berdasarkan regulasi tersebut, data pribadi dibagi menjadi dua kategori utama, yaitu data yang bersifat umum dan data yang bersifat spesifik. Pembagian ini didasarkan pada besarnya dampak atau risiko kerugian yang mungkin timbul apabila data tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab (Kristanto, n.d.).

Tantangan muncul ketika data yang dikumpulkan oleh aplikasi mobile digunakan dengan cara yang tidak konsisten dengan maksud awalnya, disebarluaskan ke pihak ketiga tanpa transparansi yang sesuai, atau disimpan tanpa protokol keamanan yang memadai. Penyalahgunaan data melampaui komplikasi teknis belaka dan merupakan dilema etika yang mendalam untuk profesi teknologi informasi (TI). Profesional TI memiliki kewajiban etis untuk memastikan bahwa sistem yang mereka kembangkan tidak menimbulkan kerugian, tidak mengeksploitasi kurangnya kesadaran pengguna, dan tidak mengabaikan hak privasi.

Kode Etik dan Perilaku Profesional Asosiasi untuk Mesin Komputasi (ACM) menekankan bahwa profesional komputasi harus memprioritaskan kepentingan publik, menghindari bahaya, menjaga kejujuran dan kepercayaan, dan menjunjung tinggi privasi dan kerahasiaan. Akibatnya, praktik aplikasi mobile yang mengaburkan tujuan pemrosesan data, meminta izin akses asing, atau memanipulasi perilaku pengguna melalui eksploitasi data dapat

ditafsirkan sebagai pelanggaran etika profesional TI.

Mengingat konteks ini, artikel ini membahas manifestasi pelanggaran etika dalam profesi TI mengenai penggunaan data pengguna yang tidak tepat dalam aplikasi mobile, faktor penyebab yang mendasari, dampak yang dihasilkan, serta strategi pencegahan yang dapat diadopsi oleh pengembang, perusahaan, dan pengguna.

2. KAJIAN TEORITIS

Bagian ini menguraikan teori- teori relevan yang mendasari topik riset menimpa pelanggaran etika profesi TI dalam penyalahgunaan informasi pengguna, dan membagikan pembahasan tentang sebagian riset lebih dahulu yang relevan serta membagikan acuan dan landasan untuk riset ini dicoba.

Teori- Teori Relevan Etika Profesi Teknologi Data

Profesi di bidang TI dihadapkan pada dilema etis buat menyeimbangkan pemakaian inovasi teknologi dengan upaya melindungi data individu pengguna. Etika profesi mengendalikan sikap seseorang handal dalam melaksanakan tugasnya supaya berlandaskan pada prinsip keadilan, integritas, serta tanggung jawab. Prinsip etika ini sangat krusial diterapkan sebab handal TI mengelola peninggalan tidak berwujud berbentuk informasi, di mana kegagalan pengelolaannya bisa membagikan akibat yang masif. Secara umum, perilaku etis yang mutlak diharapkan dari para profesional komputer meliputi sikap jujur, adil, serta mampu memelihara kerahasiaan. Mereka juga diwajibkan untuk selalu menghargai dan melindungi kerahasiaan pribadi pengguna demi mencegah kerugian pada pihak lain (Zarkasyi, 2021).

Seorang profesional di bidang TI wajib menempatkan kepentingan masyarakat di atas kepentingan pribadi dan mematuhi standar moral yang tinggi. Hal ini mutlak diperlukan guna mencegah terjadinya penyimpangan atau tindakan kriminal berbasis teknologi seperti pembobolan situs rahasia dan pencurian data rekening konsumen (Rahman et al., 2024).

Pribadi di dunia digital ialah hak krusial tiap orang buat mengatur siapa saja yang diperbolehkan mengakses serta memakai data individu mereka. Dalam praktiknya, Penyelenggara Sistem Elektronik(PSE) mempunyai kewajiban hukum buat mematuhi prinsip-prinsip proteksi informasi dalam tiap tahapan, mulai dari pengumpulan, pemrosesan, sampai penghapusan informasi.

Hak privasi ini pada dasarnya merupakan hak konstitusional warga negara yang telah dijamin secara tegas dalam Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pasal tersebut menjamin bahwa setiap orang berhak atas perlindungan

diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang ada di bawah kekuasaannya (Pertiwi et al., 2022).

Tinjauan Riset Sebelumnya

Penelitian- penelitian lebih dahulu sudah menyoroti bermacam sisi dari tantangan etika serta keamanan informasi dalam ekosistem digital. Zebua & Zebua, (2025) menegaskan kalau kenaikan kegiatan digital berbanding lurus dengan meningkatnya resiko penyalahgunaan informasi, sehingga kepatuhan terhadap kode etik oleh handal TI sangat berarti buat mempertahankan keyakinan warga. Persaingan di dunia bisnis yang terus menjadi kompetitif pula kerap merangsang pelanggaran etika; oleh karena itu, pelaksanaan etika handal yang kokoh absolut diperlukan buat memencet resiko kecurangan serta melindungi kredibilitas sesuatu entitas.

Terpaut dengan pangkal pemicu pelanggaran, Andari & Nurmiati, (2026) meningkatkan Kerangka Tanggung Jawab Etis- Teknis (KTET) serta menciptakan kalau sebagian besar insiden kebocoran informasi di Indonesia(semacam informasi kesehatan serta pajak) bersumber dari kegagalan etis, bukan sekedar kegagalan teknis. Perihal ini diperkuat oleh analisis Hardiansyah et al. (2026)yang memakai kerangka PAPA(*Privacy, Accuracy, Property, Accessibility*) buat merumuskan kalau pelanggaran etika TI di Indonesia sangat dipengaruhi oleh minimnya pemahaman pengguna, lemahnya regulasi serta penegakan hukum, dan sedikitnya investasi pada sistem keamanan informasi organisasi.

Dalam konteks aplikasi digital serta e- commerce, (Rista Maharani & Andria Luhur Prakoso, 2024)menyoroti kalau kepatuhan penyelenggara layanan dalam melindungi informasi individu merupakan harus; kelalaian dalam perihal ini tidak cuma berujung pada sanksi administratif, namun pula berakibat parah berbentuk hilangnya keyakinan konsumen. Kasus keamanan ini terus menjadi menekan bila memandang tingginya pencurian informasi yang terjalin lewat platform media sosial ataupun transaksi digital, yang mewajibkan terdapatnya proteksi hukum yang khusus serta tegas.

Di masa kecerdasan buatan(AI) dikala ini, tantangan etis tersebut jadi terus menjadi lingkungan. Saprizal et al. (2025) mencatat kalau AI mengumpulkan serta memproses informasi dalam skala masif, yang secara signifikan tingkatkan resiko pelanggaran pribadi. Buat mengamankan informasi tersebut, handal TI dituntut buat mempraktikkan perpaduan pemecahan teknis (semacam enkripsi, backup informasi, serta teknologi *blockchain*) dengan kepatuhan yang ketat terhadap regulasi semacam UU Proteksi Informasi Individu(UU PDP).

Sintesis serta Landasan Penelitian

Tinjauan dari bermacam literatur di atas membagikan landasan kokoh kalau penyalahgunaan informasi pengguna pada aplikasi mobile tidaklah semata- mata isu teknis kerentanan sistem, melainkan wujud pelanggaran mendasar terhadap etika profesi TI. Bersumber pada acuan tersebut, riset ini dibentuk atas pemikiran kalau bila pengembang serta pengelola aplikasi mobile mempraktikkan standar keamanan yang sejalan dengan prinsip etika profesi TI, hingga kemampuan eksploitasi informasi serta resiko pelanggaran hak pribadi pengguna bisa ditekan secara signifikan.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif melalui metode studi literatur. Pemilihan metode ini didasari oleh fokus penelitian yang ingin mendalami fenomena penyalahgunaan data serta aspek etika melalui tinjauan konsep, peraturan, dan standar yang berlaku, tanpa melakukan pengujian teknis langsung pada perangkat lunak.

Landasan teori dan referensi penelitian ini mencakup literatur etika profesi teknologi informasi, regulasi perlindungan data, serta standar keamanan aplikasi mobile. Secara spesifik, penelitian ini merujuk pada:

a. Undang-Undang Nomor 27 Tahun 2022 sebagai instrumen hukum perlindungan data pribadi.
b. ACM *Code of Ethics and Professional Conduct* sebagai acuan prinsip etika. Standar global seperti yang dikembangkan oleh *Association for Computing Machinery* (ACM) dan *Institute of Electrical and Electronics Engineers* (IEEE) telah memberikan panduan terperinci terkait etika profesi TI. Standar tersebut secara khusus sangat menekankan pada prinsip tanggung jawab sosial, kejujuran, privasi data, serta pencegahan bahaya (R. A. Rahman et al., 2026).
c. ISO/IEC 27001:2022 untuk standar tata kelola keamanan informasi di tingkat organisasi (seperti manajemen risiko dan kontrol akses).
d. OWASP Mobile *Application Security Verification Standard* (MASVS) sebagai panduan teknis untuk mengidentifikasi celah keamanan aplikasi, seperti enkripsi komunikasi dan perlindungan privasi.

Proses penelitian dilakukan secara sistematis, mulai dari identifikasi masalah, pengumpulan data literatur, hingga klasifikasi bentuk pelanggaran. Analisis dilakukan dengan membandingkan praktik penyalahgunaan data dengan nilai-nilai tanggung jawab profesional, kejujuran, serta keamanan informasi guna menghasilkan rekomendasi pencegahan yang tepat.

Kerangka Analisis Etika

Analisis etika dalam penelitian ini berlandaskan pada lima pilar utama:

a. Tanggung Jawab: Kewajiban praktisi TI untuk memastikan sistem tidak merugikan pengguna.
b. Kejujuran: Transparansi dalam memberikan informasi mengenai pengumpulan dan pemanfaatan data.
c. Kerahasiaan: Komitmen untuk menjaga data dari akses yang tidak sah.
d. Keadilan: Memastikan pengguna diperlakukan secara wajar tanpa adanya eksploitasi.
e. Keamanan: Implementasi kontrol organisasi dan teknis yang mumpuni.

Kelima prinsip ini menjadi tolok ukur untuk mengevaluasi manajemen data pada aplikasi mobile. Praktik seperti pengumpulan data yang berlebihan, kebijakan privasi yang membingungkan, atau penyimpanan data sensitif tanpa proteksi yang kuat dikategorikan sebagai pelanggaran etika profesi, meskipun dampak teknisnya mungkin tidak terlihat secara langsung di permukaan.

4. HASIL DAN PEMBAHASAN

Bentuk Penyalahgunaan Data Pengguna

Pengumpulan data yang berlebihan adalah bentuk penyalahgunaan data yang pertama dari tiga yang umum. Beberapa aplikasi meminta izin lebih banyak daripada yang mereka butuhkan. Contohnya, sebuah aplikasi yang dirancang untuk mencatat aktivitas harian meminta izin untuk mengumpulkan lokasi pengguna, mengakses kamera ponsel mereka, mikrofon, dan daftar kontak. Ini bertentangan dengan prinsip minimalisasi data, di mana sebuah aplikasi seharusnya hanya mengumpulkan data yang diperlukan untuk layanan tersebut.

Sebagai contoh nyata di lapangan, banyak aplikasi layanan digital mewajibkan calon pengguna untuk memberikan persetujuan akses terhadap histori perangkat, kontak di dalam handphone, dan penyimpanan eksternal sebelum aplikasi tersebut dapat diinstal dan digunakan (Zamrud & Syarifuddin, 2022).

Bentuk kedua dari tiga ini mencakup pengumpulan persetujuan pengguna yang kurang transparan. Beberapa aplikasi menjelaskan kebijakan data mereka secara panjang lebar dengan bahasa yang kurang menguntungkan, rumit, atau bahkan bahasa hukum, meninggalkan pengguna bingung dan harus menekan tombol persetujuan. Mendapatkan izin untuk pengumpulan data ini, jika dianalisis, lebih merupakan etika penipuan daripada *exercising of user's free will.*

Bentuk terakhir dari tiga ini melibatkan pemrosesan data yang tidak beralasan, di mana aplikasi memberikan data pengguna kepada perusahaan lain. Perusahaan yang mengolah data pengguna untuk analitik atau sebagai strategi pemasaran, yang tidak menjelaskan kepada pengguna rincian pemrosesan mereka, penerima data, dan siapa yang akan mengakses data tersebut serta berapa lama, secara inheren merupakan penyalahgunaan data. Praktik pengumpulan informasi dalam jumlah besar ini sering disebut sebagai *digital dossier*, di mana data pribadi tersebut dipandang memiliki nilai ekonomi yang sangat tinggi sehingga rentan dimanfaatkan dan diperjualbelikan oleh kalangan bisnis (Perlindungan & Dewi, 2021).

Jenis keempat meliputi penyimpanan data tanpa perlindungan yang cukup. Misalnya, aplikasi seluler mungkin menyimpan token otentikasi, lokasi, riwayat transaksi, atau informasi lain di penyimpanan perangkat atau server aplikasi. OWASP MASVS mengidentifikasi perlunya menyimpan data sensitif secara aman dengan menerapkan kriptografi, otentikasi, otorisasi, dan komunikasi jaringan yang aman. Pengembang yang mengabaikan aspek penyimpanan data mungkin dianggap tidak kompeten secara teknis, dan sebagai akibatnya, kelalaian ini menjadi masalah etika, yang membahayakan keamanan dan integritas pengguna.

Jenis kelima mencakup penggunaan data yang disimpan untuk manipulasi perilaku. Set data perilaku agregat dapat digunakan untuk membangun profil pengguna yang komprehensif, membuat konten kustom, atau mempengaruhi keputusan pembelian. Analitik data meningkatkan kualitas layanan. Namun, saat analitik data ini digunakan tanpa pengetahuan pengguna untuk mengeksploitasi kelemahan mereka, hal itu melampaui batas penggunaan yang tidak etis.

Tabel 1. Bentuk Pelanggaran Etika dan Dampaknya.

Bentuk pelanggaran	**Prinsip etika yang dilanggar**	**Risiko utama**	**Upaya pencegahan**
Pengumpulan data berlebihan	Minimalisasi data dan keadilan	Privasi pengguna terganggu	Batasi izin akses sesuai fungsi aplikasi
Persetujuan tidak transparan	Kejujuran dan tanggung jawab	Pengguna tidak memahami konsekuensi	Gunakan kebijakan privasi yang ringkas dan jelas
Pembagian data tanpa izin	Kerahasiaan dan penghormatan hak pengguna	Profiling dan penyalahgunaan pihak ketiga	Terapkan persetujuan eksplisit dan kontrak pemrosesan data
Keamanan penyimpanan lemah	Keamanan dan profesionalisme	Kebocoran data dan pencurian identitas	Enkripsi, kontrol akses, audit, dan pengujian keamanan
Manipulasi perilaku berbasis data	Keadilan dan menghindari kerugian	Eksploitasi psikologis atau komersial	Transparansi algoritmik dan pembatasan pemrofilan

Analisis Berdasarkan Etika Profesi TI

Penyalahgunaan data pengguna merupakan pelanggaran yang jelas terhadap kepercayaan pengguna terhadap aplikasi. Pengembang aplikasi menyalahgunakan keterampilan teknologi mereka untuk mengumpulkan, memproses, dan menyimpan data secara besar-besaran. Pengguna tidak memiliki pengetahuan yang cukup untuk menilai potensi risiko tersebut. Oleh karena itu, para profesional TI memiliki tanggung jawab untuk memastikan pengguna tidak dimanfaatkan.

Dalam kasus desain aplikasi yang buruk, tanggung jawab sosial pengembang aplikasi akan menjawab apakah mereka merancang aplikasi dengan niat yang benar. Pengembang aplikasi seharusnya merancang aplikasi yang tidak mengumpulkan data untuk alasan ilegal, tidak menimbulkan kekhawatiran keamanan data, dan tidak menciptakan peluang penyalahgunaan data. Ketidakpahaman tentang tanggung jawab sosial dari sistem digital adalah kegagalan yang serius dari sebuah profesi.

Dari sudut pandang kejujuran, aplikasi yang menyembunyikan tujuan pengumpulan data melemahkan kemampuan pengguna untuk membuat keputusan yang tepat. Orang perlu mampu membaca sesuatu dan memahami jenis, tujuan, dan justifikasi hukum dari data tersebut, prosesnya, serta durasi penyimpanan data, dan kepada siapa data akan dikirim.

Dari sudut pandang kerahasiaan, semua data pengguna bersifat sensitif dan harus dijaga demikian. Profesional TI tidak boleh melampaui posisi dan akses mereka, menyalin, mengungkapkan data pengguna, dan sebagainya. Hal ini juga sesuai dengan Kode Etik ACM. Mereka harus melindungi dan menjaga data tersebut untuk mencegah kerugian yang tidak disengaja atau kerugian informasi. Apabila profesional TI atau pihak pengelola aplikasi terbukti memperoleh, mengungkapkan, atau menggunakan data pribadi tanpa izin, mereka dapat dijerat sanksi administratif hingga pidana. Berdasarkan Pasal 67 Undang-Undang Nomor 27 Tahun 2022, pelaku pelanggaran ini dapat diancam dengan hukuman pidana penjara maksimal lima tahun dan denda hingga lima miliar rupiah (Fritiana et al., 2025).

Dari sudut pandang keamanan, standar ISO/IEC 27001:2022 menawarkan kerangka kerja untuk membangun, mengimplementasikan, memelihara, dan meningkatkan pengelolaan sistem manajemen keamanan informasi. Kerangka kerja ini penting karena mencakup kekurangan, di mana pelanggaran data tidak selalu merupakan hasil dari niat jahat pengguna; kadang-kadang mereka adalah hasil dari kurangnya manajemen, proses, dan pengendalian keamanan yang sesuai.

Faktor Penyebab Pelanggaran

Faktor pertama adalah perilaku bisnis yang berorientasi data secara berlebihan. Dalam ekonomi digital, data pengguna adalah sumber daya berharga. Data dapat dimonetisasi melalui iklan tertarget, rekomendasi personal, atau bahkan penjualan wawasan data. Tanpa etika, upaya ekonomi akan mengabaikan hak pengguna. Kondisi ini memicu munculnya dilema antara inovasi teknologi dan tanggung jawab etis yang harus diemban oleh perusahaan. Sering kali, perusahaan teknologi lebih memprioritaskan kepentingan bisnis serta efisiensi operasional dibandingkan dengan perlindungan hak privasi para penggunanya (Aljuhdy et al., 2025).

Faktor kedua adalah kurangnya pengetahuan etika dari pengembang dan manajer. Banyak yang lebih memilih menganggap privasi sebagai masalah hukum. Kepatuhan digunakan untuk menghindari jangkauan dan pengawasan hukum, tetapi perlindungan hukum diabaikan, dan pengguna secara empatik diabaikan.

Faktor ketiga adalah kurangnya perhatian terhadap privasi selama tahap awal perancangan dan pengembangan. Fitur, jika belum final, diutamakan selama proses perancangan dan privasi hampir selalu diabaikan. Ini meningkatkan risiko dibandingkan mengintegrasikan privasi sejak proses perencanaan. Bagaimanapun, perbaikan yang dilakukan terlambat dalam proses selalu lebih menantang dan mahal.

Faktor keempat adalah pengawasan internal yang kurang memadai. Data sering kali tidak terlindungi. Tidak semua organisasi memiliki akses terhadap data dan informasi. Bahkan jika ada catatan log, mereka tidak diaudit, dan insiden tidak dikelola serta dievaluasi. Karyawan internal dan mitra bisnis memiliki akses, dan data juga dapat disalahgunakan. Sebagai contoh, kasus kebocoran data berskala nasional sering kali dipicu oleh pemberian akses data kepada pihak ketiga tanpa diikuti dengan pemantauan dan audit yang ketat. Hal ini mencerminkan bahwa pengelolaan data yang meremehkan aspek keamanan merupakan bentuk lemahnya kepatuhan terhadap etika profesi (Safira et al., 2025).

Faktor kelima adalah ketimpangan literasi digital pengguna. Banyak pengguna kurang inisiatif atau kebiasaan untuk memeriksa izin dan kebijakan privasi dari aplikasi yang mereka gunakan, dan mereka tidak menilai risiko berbagi informasi mereka. Penyedia aplikasi tidak dapat menggunakan ini sebagai alasan untuk tidak beretika. Aplikasi, seharusnya, menyediakan kontrol yang mudah dipahami dan informatif. Selain itu, tingkat kesadaran keamanan informasi dan privasi data juga sangat dipengaruhi oleh faktor sosiodemografi pengguna, seperti jenis kelamin dan usia, serta sejauh mana frekuensi mereka dalam menggunakan aplikasi tersebut sehari-hari (Pangaribuan et al., 2023).

Dampak Penyalahgunaan Data

Terdapat banyak dampak penyalahgunaan data yang jelas. Bagi subjek data individu saat ini, banyak pengguna telah melihat data mereka digunakan untuk kehilangan privasi, kehilangan identitas mereka, kehilangan uang, kehilangan akun mereka... Dengan kehilangan kendali atas bagaimana data mereka digunakan, pengguna menyalahgunakan kehilangan kendali tersebut untuk perusahaan. Bagi subjek, kehilangan data meliputi kehilangan kendali atas data pelacakan mereka, lokasi, pencarian, dan data alasan. Pengguna yang menjadi subjek pelacakan data paling takut kehilangan kendali mereka. Data dapat kehilangan kendali pelacakan.

Bagi bisnis, banyak aplikasi menjadi tidak berguna atau tidak berharga dan banyak aplikasi tidak mampu mempertahankan dukungan pelanggan.

Dampak penyalahgunaan data terhadap masyarakat adalah hilangnya dukungan terhadap perubahan dunia digital. Pengguna masyarakat takut kehilangan kendali mereka. Sistem data masyarakat adalah kehilangan kendali paling besar.

Upaya Pencegahan

Upaya pencegahan pertama melibatkan penerapan privasi melalui desain. Ini menentukan bahwa privasi tidak bisa dihapus dari desain sebuah sistem dan tidak boleh pernah menjadi hal yang dipikirkan belakangan. Setiap fitur dari sebuah aplikasi harus dinilai terkait kebutuhan data, risiko, dan manfaat pengguna.

Upaya kedua melibatkan minimalisasi data. Aplikasi tidak boleh diizinkan untuk meminta data yang bernilai di atas ambang batas tertentu. Jika layanan masih dapat berfungsi tanpa akses ke data lokasi, maka permintaan akses lokasi sebaiknya tidak diizinkan. Selain itu, jika data hanya diperlukan sementara, data tersebut harus dihapus. Ini untuk memastikan bahwa data hanya disimpan selama tujuan pemrosesan belum terpenuhi.

Upaya ketiga melibatkan kemampuan pengguna untuk melakukan kontrol. Kebijakan privasi harus bebas dari bahasa hukum, jelas, ringkas, dan mudah dipahami oleh pengguna. Pengguna juga harus diberi izin untuk menolak ketentuan, serta hak untuk mencabut persetujuan, memperbarui data, dan meminta penghapusan data, sesuai ketentuan hukum. Ketersediaan kebijakan privasi yang transparan dan mudah dipahami terbukti berkorelasi positif dengan tingkat kepercayaan pengguna terhadap platform digital. Kepercayaan yang terbangun ini pada akhirnya akan memotivasi pengguna untuk lebih proaktif dalam mengambil langkah-langkah perlindungan terhadap data pribadi mereka sendiri (Fathni et al., 2023).

Upaya keempat adalah peningkatan keamanan teknis. Para pengembang wajib memastikan bahwa data selama penyimpanan, transmisi, dan pemrosesan terlindungi untuk menciptakan lingkungan yang aman dan terlindungi. Pendekatan keamanan yang baik adalah mengikuti standar yang ditetapkan oleh OWASP.

Upaya terakhir adalah peningkatan budaya organisasi dan etika. Tanggung jawab organisasi adalah mengadopsi budaya kolaborasi yang etis dan meningkatkan pelatihan profesional bagi staf TI. Profesional TI harus memahami bahwa kebijakan dan keputusan teknis selalu membawa tanggung jawab sosial. Pendekatan berbasis etika menjadi sangat krusial untuk menciptakan budaya keamanan yang berkelanjutan, mengingat ancaman peretasan sistem tidak cukup diatasi hanya dengan kontrol teknis semata. Oleh karena itu, penguatan kapasitas etika melalui kebijakan, pelatihan, dan komunikasi strategis harus menjadi bagian tidak terpisahkan dari tata kelola keamanan informasi yang profesional (Anugrah et al., 2025).

5. KESIMPULAN DAN SARAN

Penyalahgunaan data konsumen oleh aplikasi seluler menunjukkan kurangnya etika bagi profesional TI karena tindakan mereka tidak mematuhi prinsip utama akuntabilitas, kejujuran, kerahasiaan, keadilan, atau keamanan. Pelanggaran yang paling umum dikenal sebagai eksploitasi data di mana data dikumpulkan secara berlebih, dibagikan dengan pihak ketiga, disimpan secara tidak baik, dan digunakan untuk modifikasi perilaku pengguna berbasis data. Pelanggaran berbasis data disebabkan oleh etika yang buruk, privatisasi etika, dan rancangan pengawasan etika yang berdebu serta ketidakseimbangan antara desain privasi rendah, pengawasan rendah, dan literasi digital pengguna yang rendah. Pencegahan harus melibatkan desain dan minimisasi data, kebijakan yang jelas, dan budaya organisasi.

UCAPAN TERIMA KASIH

Artikel ilmiah ini disusun untuk memenuhi Tugas Ujian Akhir Semester (UAS) pada mata kuliah Etika Profesi Teknologi Informasi. Oleh karena itu, penulis, Nadwa Meilan Iffa dari Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, mengucapkan terima kasih yang sebesar-besarnya kepada Evy Nurmiati, S.Kom, M.MSI selaku dosen pengampu atas bimbingan, arahan, dan ilmu yang telah diberikan selama satu semester ini. Penulis juga mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan moril maupun materiil sehingga penyusunan artikel ini dapat diselesaikan dengan baik.

DAFTAR REFERENSI

Agung Hardiansyah, S., Sutabri, T., Palembang, K., & Selatan, S. (2026). Analisis pelanggaran etika teknologi informasi di Indonesia: Studi kasus kebocoran data. *Jurnal Ilmiah Penelitian Mahasiswa, 4*(1), 666–676. https://doi.org/10.61722/jipm.v4i1.1951

Andari, A. S. S., & Nurmiati, E. (2026). Peran dan tanggung jawab etis profesional TI dalam mencegah kebocoran data privasi. *Jejak Digital: Jurnal Ilmiah Multidisiplin, 2*(3), 3856–3863. https://doi.org/10.63822/kpy62w91

Anesya Fritiana, Daishahwa, & Wiraguna, S. A. (2025). Penyalahgunaan data pribadi pada layanan pinjaman online: Analisis perlindungan dan sanksi hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3*(2), 523–529. https://doi.org/10.61104/alz.v3i2.1082

Anugrah, S., Qalby, N. R., Himawan, M. Z., & Nurmiati, E. (2025). Pengaruh etika profesi terhadap keamanan informasi dalam konteks kebocoran data BSI (Bank Syariah Indonesia): Studi literatur sistematis. *Jurnal Teknologi dan Teknologi Informasi, 11*(2), 106–112. https://doi.org/10.34010/jtk3ti.v11i2.17033

Dean Safira, S., Setyaningrum, R. P., Anwar, N. R., Aldrin, M., Noto, I. M. C. D., & Fathihah, M. A. N. (2025). Analisis kepatuhan etika profesi dan keamanan sistem: Studi kasus kebocoran data BPJS Kesehatan. *Jurnal Informasi Interaktif, 10*(2).

Fathni, I., Zulaika, S., & Dewi, R. S. (2023). Pengaruh kebijakan privasi dan tingkat kepercayaan pada platform digital terhadap perilaku pengguna dalam melindungi privasi online di Indonesia. *Sanskara Hukum dan HAM, 2*(2), 118–126. https://doi.org/10.58812/shh.v2i02.305

Kharisma Arrasuli, B., & Fahmi, K. (2023). Perlindungan hukum positif Indonesia terhadap kejahatan penyalahgunaan data pribadi. *UNES Journal of Swara Justisia, 7*(2). https://doi.org/10.31933/ujsj.v7i2

Kristanto, A. P. (n.d.). Perlindungan terhadap data pribadi dalam aplikasi digital sebagai bentuk perlindungan hak asasi manusia. *UNES Law Review*. https://doi.org/10.31933/unesrev.v5i3

Ode Zamrud, W., & Syarifuddin, M. (2022). Perlindungan hukum terhadap data pribadi konsumen pengguna jasa ojek online. *Jurnal Ilmu Hukum Kanturuna Wolio, 3*(2). https://doi.org/10.55340/jkw.v3i2.787

Pangaribuan, T., Sari, D., Takariani, C. S. D., & Simatupang, O. (2023). Kesadaran keamanan dan privasi data pengguna WhatsApp (studi kasus di Provinsi Jawa Barat). *Jurnal Studi Komunikasi dan Media, 27*(1), 93–108. https://doi.org/10.17933/jskm.2023.5129

Perlindungan, K., & Dewi, S. (2021). Konsep perlindungan hukum atas privasi dan data pribadi dikaitkan dengan penggunaan cloud computing di Indonesia. *Yustisia, 5*(1). http://www.telkomcloud.com/

Pertiwi, E., Nuraldini, D. D., Buana, G. T., & Arthacerses, A. (2022). Analisis yuridis terhadap penyalahgunaan data pribadi pengguna media sosial. *Rechten*. https://doi.org/10.52005/rechten.v3i3.65

Rahman, A., Tanjung, M. I., Sirait, M. Z., & Ritonga, S. J. (2024). Etika profesional dalam menghadapi tantangan teknologi informasi. *Journal of Social Science Research, 4*, 8118–8125.

Rahman, R. A., Nurmiati, E., & Diterima, R. A. (2026). Tinjauan etika profesi TI pada standar ACM-IEEE dan SKKNI: Systematic literature review. *Jurnal Ilmiah Sistem Informasi, 2*(2). https://doi.org/10.69533/2w2exa64

Rista Maharani, & Prakoso, A. L. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *Jurnal Hukum dan HAM Wara Sains, 7*(1), 333–346. https://doi.org/10.58812/jhhws.v2i05.354

Saprizal, A. M., Pebriana, R., Margaret, T., & Swastina, L. (2025). Etika profesi TI di era AI: Tantangan perlindungan data dan privasi pengguna. *Methoda, 15*(3), 231–238. https://doi.org/10.46880/methoda.Vol15No3.pp231-238

Yunika Zebua, D., & Zebua, A. P. (2025). Tantangan etika dalam profesi teknologi informasi. *Identik*. https://doi.org/10.70134/identik.v2i1.162

Zarkasyi. (2021). Etika profesi dalam bidang teknologi informasi. *Techno Training and Society, 3*(1). https://doi.org/10.29103/tts.v3i1.8870

Zidan Aljuhdy, M., Abdillah, D. H., Fauzan, R., Aryanto, F. N., & Augustia, A. E. (2025). Etika profesi IT dalam penggunaan data lokasi oleh aplikasi *ride-hailing*: Kajian privasi dan tanggung jawab sosial. *Teknobis, 3*, 355–359.