# TANTANGAN ETIKA DALAM PROFESI TEKNOLOGI INFORMASI

**Della Yunika Zebua[1)], Alfan Pintalius Zebua[2)]**
[1)] Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Nias, Gunungsitoli, Indonesia
Email: yuyudella4@gmail.com
[2)] Teknik Sipil, Fakultas Teknik, Universitas Nommensen HKBP, Medan, Indonesia
Email: alfanzebua2@gmail.com

**Abstract**

The profession in Information Technology (IT) poses many challenges, especially related to ethics, especially in privacy and data security. In working, IT professionals must face ethical dilemmas. They must balance between using innovative technology and protecting users' personal information. Professional ethics in IT are rules that determine how a professional should act, including maintaining integrity and honesty. This is important to maintain public trust in the technology services provided. However, with the increasing number of digital activities and data usage, the risk of data misuse and privacy violations is also increasing. In addition, the use of the internet as a modern communication tool also raises concerns about increasing privacy violations. This study focuses on the study of ethical principles in IT work and the issues that arise in data protection and privacy in the digital age. By understanding ethical rules and regulations on privacy, hopefully awareness of ethics will increase and data security practices can be improved to reduce the risk of privacy violations.

**Keywords:** Professional ethics, Information technology, Privacy, Data security, Code of Ethics

**Abstrak**

Profesi dalam Teknologi Informasi (TI) menimbulkan banyak tantangan terutama terkait etika, khususnya dalam privasi dan keamanan data. Dalam bekerja, para profesional di bidang Teknologi Informasi harus menghadapi dilema etis. Mereka harus seimbang antara menggunakan teknologi inovatif dan melindungi informasi pribadi pengguna. Etika profesi di bidang Teknologi Informasi adalah aturan yang menentukan bagaimana seorang profesional harus bertindak, termasuk menjaga integritas dan kejujuran. Ini penting untuk mempertahankan kepercayaan masyarakat terhadap layanan teknologi yang disediakan. Namun, dengan semakin banyaknya kegiatan digital dan penggunaan data, risiko penyalahgunaan data dan pelanggaran privasi juga semakin meningkat. Selain itu, penggunaan internet sebagai alat komunikasi modern juga menimbulkan kekhawatiran akan pelanggaran privasi yang semakin meningkat. Penelitian ini memfokuskan pada studi tentang prinsip-prinsip etika dalam pekerjaan di bidang Teknologi Informasi dan masalah-masalah yang muncul dalam perlindungan data dan privasi di zaman digital. Dengan memahami aturan etika dan regulasi tentang privasi, semoga kesadaran akan etika meningkat dan praktik keamanan data bisa ditingkatkan untuk mengurangi risiko pelanggaran privasi.

**Kata Kunci:** Etika profesi, Teknologi informasi, Privasi, Keamanan data, Kode Etik

## PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah mengubah banyak hal dalam kehidupan kita. Salah satunya adalah bagaimana orang mencari, menggunakan, dan berbagi informasi. Di zaman digital seperti sekarang, data menjadi sangat berharga bagi individu, organisasi, dan pemerintah. Meningkatnya interaksi manusia melalui internet, media sosial, dan aplikasi web menghasilkan banyak data beragam seperti data pribadi, finansial, dan informasi sensitif. Teknologi yang terus berkembang, seperti cloud computing, big data, dan kecerdasan buatan, membantu data menjadi lebih bermanfaat, namun juga menimbulkan masalah terkait privasi dan keamanan data.

Privasi adalah hak penting setiap individu untuk mengontrol informasi pribadi dan menentukan siapa yang bisa mengakses data tersebut. Namun, di dunia digital, menjaga privasi semakin sulit. Aktivitas online seperti browsing, transaksi digital, dan media sosial meninggalkan jejak digital yang dapat dimanfaatkan oleh orang lain untuk berbagai tujuan, seperti komersial, politik, atau kriminal. Privasi sering terancam oleh tindakan seperti pengumpulan data tanpa izin, pelacakan lokasi, dan penyebaran informasi pribadi yang seharusnya dilindungi. Profesional di bidang teknologi informasi harus memahami aturan dan etika dalam pengelolaan data pengguna serta mematuhi peraturan privasi.

Keamanan data juga penting dalam profesi teknologi informasi. Dengan serangan siber semakin meningkat, seperti pencurian data, ransomware, dan serangan terhadap infrastruktur kritis, profesional TI harus memiliki kemampuan dan kejujuran dalam melindungi data dari akses yang tidak sah. Keamanan data melibatkan langkah-langkah teknis dan administratif yang bertujuan untuk menjaga data tetap aman dan hanya dapat diakses oleh orang yang diberi izin. Ketidakmampuan untuk melindungi data tidak hanya merugikan orang atau perusahaan, tetapi juga menurunkan kepercayaan masyarakat terhadap teknologi dan layanan digital. Karenanya, penting bagi para profesional TI untuk mematuhi standar keamanan yang ketat, memahami regulasi perlindungan data, dan menggunakan praktik terbaik untuk mencegah pelanggaran keamanan.

Menurut (Jeffry Yuliyanto Waisapi, 2022) kode etik profesi merupakan kriteria prinsip profesional yang telah digariskan, sehingga diketahui dengan pasti kewajiban profesional anggota lama, baru, ataupun calon anggota kelompok profesi. Kode etik profesi telah menentukan standarisasi kewajiban profesional anggota kelompok profesi. Etika profesi dalam bidang teknologi informasi melibatkan prinsip-prinsip yang mengatur perilaku seorang profesional dalam menjalankan tugasnya. Etika ini penting untuk menjaga kejujuran dan keadilan dalam hubungan profesional serta untuk melindungi hak privasi dan keamanan data. Di sejumlah negara, peraturan tentang privasi dan keamanan data, seperti GDPR di Uni Eropa dan UU ITE di Indonesia, menetapkan kerangka hukum yang harus diikuti oleh para profesional TI. Meskipun demikian, undang-undang seringkali hanya menetapkan standar minimum. Oleh karena itu, peran kode etik dan norma profesional sangat penting untuk menjaga agar privasi pengguna terlindungi sebaik mungkin. Kode etik ini, sering dibuat oleh asosiasi profesional TI, membantu menjaga standar profesional dan mencegah penyalahgunaan teknologi yang membahayakan data atau hak individu.

Meskipun etika profesi TI terus berkembang, masih ada berbagai tantangan yang muncul dalam penerapannya. Salah satu masalah besar adalah benturan antara kepentingan bisnis dan perlindungan privasi. Contohnya, dalam bisnis yang fokus pada data, data pengguna sering digunakan untuk analisis dan iklan. Seringkali, kondisi ini melanggar hak privasi individu yang seharusnya dilindungi oleh penyedia layanan. Selain itu, penggunaan teknologi baru seperti pengenalan wajah dan pelacakan lokasi juga telah memunculkan perdebatan etis karena dapat membahayakan privasi yang berlebihan. Para profesional di bidang TI harus memikirkan bagaimana teknologi yang mereka kembangkan dapat memengaruhi masyarakat, termasuk risiko terhadap privasi dan keamanan.

Penelitian ini ingin menyoroti berbagai masalah etika yang dihadapi oleh para profesional di bidang teknologi informasi, terutama terkait privasi dan keamanan data. Dengan memahami masalah yang rumit, kita harap bahwa para profesional TI dapat lebih bertanggung jawab dalam pekerjaan mereka dan turut serta dalam melindungi hak-hak pengguna. Penelitian ini juga menekankan betapa pentingnya kesadaran etis dalam mengelola data, serta langkah-langkah pencegahan yang bisa dilakukan untuk

mempertahankan kepercayaan masyarakat terhadap teknologi dan layanan digital.

## METODE PENELITIAN

Penelitian ini mengandalkan sumber-sumber literatur yang relevan untuk mempelajari tantangan etika dalam profesi teknologi informasi, terutama tentang privasi dan keamanan data. Metode yang digunakan adalah metode kepustakaan yang bertujuan untuk menggali, menganalisis, dan menyintesiskan informasi yang diperlukan. Metode ini bertujuan untuk memahami prinsip-prinsip etika yang harus diikuti oleh para profesional teknologi informasi dan masalah yang dihadapi dalam menerapkan prinsip-prinsip tersebut di zaman digital.

Sumber informasi untuk penelitian ini berasal dari jurnal yang terdapat di perpustakaan digital yang terkenal secara internasional, seperti IEEE Xplore, ScienceDirect, dan Google Scholar. Jurnal-jurnal ini membahas perkembangan teknologi, peraturan privasi, dan keamanan data yang berlaku di beberapa negara. Beberapa situs web dengan integritas tinggi di bidang teknologi digunakan sebagai referensi untuk mempelajari etika dan praktik terbaik dalam menjaga keamanan dan privasi data. Analisis literatur dilakukan dengan mengelompokkan sumber berdasarkan tema utama: (1) konsep dasar etika dalam profesi teknologi informasi, (2) privasi dan tantangan dalam menjaga hak-hak pengguna di dunia digital, dan (3) aspek teknis dan hukum dalam menjaga keamanan data. Setiap tema diteliti secara menyeluruh untuk memahami dampaknya terhadap tanggung jawab dan praktik profesional dalam teknologi informasi.

Studi kepustakaan ini diharapkan dapat memberikan informasi tentang tantangan etika yang dihadapi oleh para profesional dalam bidang tersebut, dan memberikan rekomendasi terkait praktik etis untuk melindungi privasi dan keamanan data. Pendekatan ini membantu peneliti untuk mendapatkan perspektif luas dan membandingkan hasil dari berbagai sumber. Dengan demikian, peneliti dapat membuat kesimpulan yang lebih komprehensif dan mendalam.

## HASIL DAN PEMBAHASAN

### A. Konsep Dasar Etika Dalam Profesi Teknologi Informasi

Menurut (Zarkasyi, 2022) kode etik merupakan pola aturan atau tata cara sebagai pedoman berperilaku dan berbudaya. Tujuan kode etik agar profesionalisme memberikan jasa sebaik-baiknya kepada pemakai jasa atau nasabahnya. Adanya kode etik akan melindungi perbuatan yang tidak profesional. Dalam bidang teknologi informasi (TI), kode etik sangat penting karena mengatur tindakan dan perilaku seorang profesional TI dalam bekerja. Etika dalam bidang ini melibatkan nilai-nilai seperti integritas, kejujuran, keadilan, dan tanggung jawab. Nilai-nilai ini penting untuk membangun kepercayaan antara penyedia layanan teknologi dan pengguna atau masyarakat umum.

Profesi di bidang teknologi informasi, seperti pengembang perangkat lunak, analis sistem, hingga ahli keamanan siber, dapat mengakses dan mengelola data sensitif milik individu dan perusahaan. Mereka harus mengikuti aturan etika yang ketat, termasuk melindungi privasi, keamanan data, dan transparansi dalam kegiatan mereka. Kode etik profesi TI melindungi pengguna dan membangun reputasi profesional yang dapat diandalkan. Tenaga profesional di bidang Teknologi Informasi (TI) yang mematuhi etika kerja yang baik akan menjaga keamanan data pengguna, tidak menyalahgunakan hak akses, serta menjaga kerahasiaan informasi yang mereka tangani. Selain itu, konsep dasar etika dalam profesi TI juga mencakup kemandirian dan tanggung jawab profesional dalam mengambil keputusan. Setiap profesional IT diharapkan memahami risiko dan dampak teknologi yang mereka gunakan atau kembangkan. Maka, kode etik menekankan pentingnya pengambilan keputusan yang bertanggung jawab, yaitu keputusan yang memperhitungkan kepentingan pengguna dan masyarakat. Contohnya, saat mengembangkan sistem berbasis data pengguna, para ahli TI harus memikirkan privasi sejak tahap perancangan (privacy by design). Mereka harus memastikan bahwa data pengguna terlindungi dengan mekanisme keamanan yang sesuai.

Seiring dengan kemajuan teknologi, seperti kecerdasan buatan dan internet of things (IoT), tantangan terhadap etika dalam profesi TI semakin

meningkat. Teknologi-teknologi ini dapat mengumpulkan data dalam jumlah besar dan menganalisis pola perilaku pengguna dengan lebih detail. Walaupun ada banyak keuntungan, para profesional TI harus memastikan bahwa penggunaan data dilakukan dengan etika dan tidak melanggar privasi individu. Kode etik membantu kita untuk mengerti batasan-batasan etis dalam menggunakan teknologi baru agar tidak merugikan atau membahayakan pengguna. Etika dalam bidang TI juga mencakup komitmen untuk terus belajar dan mengikuti perkembangan teknologi yang terus berubah. Seorang ahli Teknologi Informasi harus tahu aturan dan standar terbaru tentang keamanan data dan privasi, seperti General Data Protection Regulation (GDPR) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Dengan mengikuti aturan dan update hukum, para profesional TI bisa memastikan mereka memberikan manfaat yang baik untuk masyarakat dan meningkatkan kepercayaan akan industri teknologi informasi.

Menurut (Dedes et al., 2022) penggunaan teknologi informasi juga tidak bisa terlepas dengan etika-etika yang menjadi pendamping atau pegangan bagi penggunanya. Untuk menerapkan etika teknologi informasi, terlebih dahulu perlu diketahui dan dijelaskan prinsip-prinsip yang terkandung di dalam teknologi informasi, di antaranya adalah:

1. Tujuan teknologi informasi adalah untuk memberdayakan manusia dalam memecahkan masalah, membangkitkan kreativitas, dan memungkinkan manusia untuk melakukan lebih banyak pekerjaan tanpa menggunakan teknologi informasi dan aktivitasnya.
2. Prinsip High–tech–high–touch: jangan mengandalkan teknologi canggih, tetapi yang lebih penting, tingkatkan kemampuan dari aspek “high touch “yaitu “manusia”.
3. Menyesuaikan teknologi informasi dengan manusia: Teknologi informasi harus dapat mendukung semua aktivitas manusia yang harus disesuaikan dengan teknologi informasi.

Secara keseluruhan, etika dalam profesi TI berperan sebagai dasar moral yang menjaga praktik profesional tetap berlandaskan pada prinsip keadilan, integritas, dan tanggung jawab. Kode etik ini membantu profesional TI dan melindungi masyarakat dengan memastikan teknologi digunakan dengan aman, etis, dan bermanfaat bagi semua.

### B. Privasi Dan Tantangan Dalam Menjaga Hak-hak Pengguna Di Dunia Digital

Menurut (Yuwinanto, 2015) privasi adalah tingkatan interaksi atau keterbukaan yang dikehendaki oleh seseorang pada suatu kondisi atau situasi tertentu, dimana situasi yang dirasa sebagai privat atau tidak yang menentukan adalah subjektifitas dan kontrol (ruang interpersonal dan territorial) dari seseorang tersebut . Privasi dalam dunia digital adalah tentang hak individu untuk mengendalikan siapa yang bisa melihat dan menggunakan informasi pribadi mereka. Pada zaman teknologi informasi, informasi pribadi pengguna sangat berharga dan digunakan dalam berbagai hal seperti media sosial, layanan perbankan online, aplikasi kesehatan, dan e-commerce. Privasi ini melibatkan informasi sensitif seperti nama, alamat, nomor identifikasi, informasi keuangan, serta data perilaku dan preferensi pengguna yang tercatat dari aktivitas online.

Perlindungan privasi adalah hak dasar yang penting untuk menjaga kepercayaan antara pengguna dan penyedia layanan digital. Namun, dalam dunia digital, menjaga privasi pengguna bisa menjadi sulit karena teknologi yang terus berkembang dapat membuka celah bagi orang-orang yang ingin mengakses atau menggunakan data pribadi secara ilegal atau tidak etis. Salah satu masalah utama adalah sulitnya melindungi data pengguna yang disimpan melalui berbagai platform, seperti aplikasi media sosial dan perangkat Internet of Things (IoT). Banyak perusahaan teknologi mengumpulkan dan menyimpan data pengguna dalam jumlah besar untuk analitik, personalisasi, atau iklan, mengakibatkan risiko pelanggaran privasi. Contoh, aplikasi yang menggunakan lokasi pengguna untuk memberikan layanan lokal atau memantau aktivitas online bisa menyimpan informasi pribadi yang bisa disalahgunakan jika tidak aman.

1. Privasi dalam Penggunaan Data oleh Perusahaan Teknologi

   Perlindungan privasi saat perusahaan teknologi menggunakan data pengguna sangat penting. Mereka sering menggunakan informasi pribadi ini untuk

meningkatkan layanan mereka, seperti iklan yang sesuai atau rekomendasi konten. Meskipun dapat membuat pengalaman pengguna menjadi lebih baik, penggunaan data dalam jumlah besar juga menimbulkan kekhawatiran tentang seberapa jauh perusahaan bisa mengakses dan menggunakan informasi tanpa melanggar privasi pengguna. Salah satu contoh kasus nyata adalah insiden Cambridge Analytica pada tahun 2018. Data pribadi dari jutaan pengguna Facebook dikumpulkan tanpa izin mereka dan dimanfaatkan untuk kampanye politik. Kasus ini menyoroti bahaya ketika perusahaan teknologi bisa mengakses data pengguna dengan bebas. Ini menunjukkan pentingnya aturan yang jelas untuk melindungi privasi pengguna di zaman digital.

2. Tantangan Privasi dalam Teknologi IoT dan Kecerdasan Buatan

   Perkembangan teknologi Internet of Things (IoT) dan kecerdasan buatan (AI) menimbulkan tantangan privasi baru. Perangkat pintar dan sensor IoT bisa mengumpulkan data dalam jumlah besar dari sekitar dan penggunaannya. Contohnya, perangkat pintar seperti asisten suara (seperti Amazon Alexa atau Google Home) bisa merekam percakapan atau suara di sekitar pengguna. Hal ini menimbulkan kekhawatiran mengenai pelanggaran privasi yang mungkin terjadi. Selain itu, teknologi pengenalan wajah juga sering digunakan di tempat ramai. Ada kekhawatiran bahwa data biometrik ini bisa disalahgunakan oleh orang yang tidak seharusnya, entah untuk keuntungan bisnis atau pengawasan. Perangkat IoT sering memiliki keamanan yang buruk dan rentan terhadap serangan siber yang bisa membocorkan data pribadi pengguna.

3. Risiko Privasi dalam Sistem Keamanan Siber dan Serangan Data

   Tantangan lain untuk privasi adalah ancaman terhadap keamanan data, di mana serangan siber seperti peretasan dan ransomware semakin sering terjadi. Pelanggaran data adalah saat informasi pribadi pengguna dicuri oleh peretas, kemudian dijual di pasar gelap atau digunakan untuk kejahatan seperti penipuan identitas. Contoh, tahun 2017, data Equifax dilanggar, perusahaan kredit AS. Data pribadi 147 juta orang bocor, termasuk nomor jaminan sosial dan info finansial. Insiden ini merugikan individu dan merusak kepercayaan publik terhadap kemampuan perusahaan dalam menjaga privasi dan keamanan data pengguna. Perusahaan harus menerapkan protokol keamanan yang ketat seperti enkripsi data, autentikasi multi-faktor, dan pemantauan serangan untuk mengatasi tantangan keamanan siber.

4. Regulasi untuk Menjaga Privasi dan Perlindungan Hukum

   Dalam mempertahankan privasi, berbagai aturan telah dibuat, seperti General Data Protection Regulation (GDPR) di Uni Eropa yang menangani data pribadi dan memberikan hak kepada individu untuk mengontrol data mereka. Peraturan ini mengharuskan perusahaan untuk jelas dalam mengumpulkan dan menggunakan data, juga memberikan hak kepada pengguna untuk melihat dan menghapus data mereka. Di Indonesia, UU ITE mengatur privasi dalam transaksi digital.

   Namun, tantangan terbesar adalah bahwa teknologi sering lebih cepat berkembang daripada regulasi yang ada. Contohnya, walaupun GDPR melindungi data pribadi, beberapa platform digital dari negara-negara dengan standar perlindungan yang rendah masih dapat menyebabkan data pengguna terancam kebocoran. Selain itu, perusahaan teknologi seringkali memiliki kantor pusat di negara dengan regulasi yang longgar, yang memungkinkan mereka untuk mengambil keuntungan dari celah hukum dalam penggunaan data pribadi.

5. Keterlibatan Pengguna Dalam Menjaga Privasi Mereka Sendiri

   Selain tanggung jawab perusahaan dan pemerintah, pengguna juga memiliki peran penting dalam melindungi privasi

mereka sendiri. Dengan semakin seringnya pelanggaran privasi, pengguna disarankan untuk lebih berhati-hati dalam membagikan informasi pribadi di internet. Contohnya, pengguna bisa menggunakan fitur pengaturan privasi di media sosial atau tidak menyimpan informasi sensitif di perangkat yang mudah diakses. Menurut penelitian, banyak orang masih belum menyadari konsekuensi dari jejak digital mereka, sehingga penting untuk memberikan pendidikan tentang literasi digital agar mereka lebih sadar akan privasi.

6. Tantangan Etis bagi Profesional TI dalam Menjaga Privasi Pengguna

   Etika berperan penting dalam penanganan data pengguna. Para profesional TI bertanggung jawab untuk memastikan data pengguna diproses dan disimpan dengan aman. Contohnya, mereka harus mengikuti aturan perilaku yang benar dalam mengumpulkan, menyimpan, dan menggunakan data, serta memastikan bahwa data tersebut tidak disalahgunakan atau diakses oleh orang yang tidak diizinkan. Tantangan etis ini termasuk tanggung jawab dalam mengembangkan teknologi yang bisa memengaruhi privasi, misalnya memastikan bahwa algoritma AI tidak punya bias atau merugikan hak privasi individu.

   Secara keseluruhan, menjaga privasi di era digital adalah tantangan yang rumit dan melibatkan peran dari perusahaan, pemerintah, dan individu. Saat teknologi terus maju, cara terbaik untuk menjaga privasi adalah dengan menerapkan aturan yang ketat dan mengikuti kode etik yang baik. Hal ini dapat membantu menciptakan lingkungan online yang aman dan etis bagi semua orang.

## C. Aspek Teknis Dan Hukum Dalam Menjaga Keamanan Data

Di tengah era digital yang pesat, data pribadi individu semakin rentan terhadap potensi penyalahgunaan dan pelanggaran privasi. Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati (Anggen Suari and Sarjana, 2023). Keamanan data penting dalam teknologi informasi. Data adalah aset berharga bagi individu dan organisasi. Perlindungan data penting untuk menjaga kerahasiaan informasi dan mencegah kerugian dari kebocoran atau penyalahgunaan data, baik yang bersifat materiil maupun non-materiil. Data pribadi sangat berharga, pelanggaran privasi dapat menyebabkan kerugian ekonomi dan melanggar hak individu.

Para profesional di bidang teknologi informasi harus memahami aspek teknis dalam menjaga data dan mematuhi aturan hukum untuk memastikan tindakan mereka sejalan dengan prinsip keamanan dan integritas mengingat ancaman keamanan digital yang semakin kompleks. Menjalankan langkah teknis dengan benar dan mengikuti regulasi yang ketat sangat penting untuk menciptakan lingkungan digital yang aman dan bisa diandalkan.

1. Aspek Teknis dalam Menjaga Keamanan Data

   Di dunia digital, ada beberapa langkah teknis yang bisa diambil untuk menjaga keamanan data dari akses yang tidak sah atau serangan siber:

   - Enkripsi

     Enkripsi adalah langkah dasar dan penting dalam melindungi data. Menurut (Alfarist and Indonesia, 2023) enkripsi data adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca atau dimengerti tanpa kunci enkripsi yang sesuai. Tujuannya adalah untuk melindungi kerahasiaan dan integritas data. Dengan enkripsi, data hanya dapat dibaca oleh pihak yang memiliki kunci enkripsi. Hal ini dapat membantu melindungi data dari akses yang tidak sah, baik oleh pihak internal maupun pihak eksternal. Enkripsi dapat mengubah data menjadi format yang hanya dapat dibaca oleh orang yang memiliki kunci dekripsi yang tepat. Proses enkripsi digunakan untuk melindungi data ketika disimpan atau ditransfer melalui jaringan. Contohnya, informasi dalam perbankan dan transaksi finansial biasanya diacak agar

terhindar dari akses pihak yang tidak berwenang.

- Otentikasi dan Otorisasi

  Otentikasi adalah cara untuk memeriksa identitas pengguna sebelum diberi izin akses ke sistem, sementara otorisasi memastikan bahwa pengguna hanya dapat mengakses data dan fungsi yang sesuai dengan hak akses yang dimilikinya. Metode autentikasi yang biasa digunakan termasuk menggunakan kata sandi, biometrik, dan autentikasi multi-faktor (MFA), dimana pengguna harus melewati beberapa tahap verifikasi untuk bisa masuk. Dengan melakukan ini, risiko akses yang tidak sah turun secara signifikan.

- Firewall dan Sistem Deteksi Intrusi (IDS)

  (Wicaksono, 2022) Firewall merupakan suatu jenis teknologi keamanan jaringan yang berguna untuk mengatur paket data yang masuk ke dalam jaringan dan paket data yang di blokir. Firewall juga digunakan untuk melindungi, membatasi maupun menolak jaringan pribadi dengan jaringan luar yang berbahaya. Firewall bertindak sebagai penghalang antara jaringan yang aman dan jaringan luar seperti internet. Firewall bisa memantau dan mengatur lalu lintas masuk serta keluar, hanya memperbolehkan lalu lintas yang sudah diverifikasi atau sesuai dengan aturan keamanan yang telah ditetapkan. Sistem Deteksi Intrusi (Intrusion Detection System atau IDS) adalah metode tambahan untuk mengawasi aktivitas mencurigakan atau abnormal dalam jaringan. IDS memberikan pemberitahuan tentang kemungkinan serangan sebelum kerusakan terjadi.

- Penambalan Sistem (Patching)

  Sistem perangkat lunak yang jarang diperbarui sering kali menjadi sasaran serangan karena rentannya. Pembaruan sistem secara teratur diperlukan untuk memperbaiki celah keamanan yang bisa disusupi oleh peretas. Dengan melakukan patching, organisasi bisa memastikan mereka gunakan versi perangkat lunak teraman, kurangi risiko serangan yang memanfaatkan kerentanan yang sudah diketahui.

- Back-Up Data dan Pemulihan Bencana

  Backup adalah kegiatan menyalin atau membuat file database cadangan, sehingga file database salinan atau cadangan tersebut disimpan dan dapat dipanggil kembali untuk mengganti file asli apabila terdapat kerusakan atau kehilangan. Backup bertujuan untuk menyalin data asli sebagai data cadangan yang disimpan di tempat yang berbeda dalam rangka mengantisipasi terjadinya kerusakan dan kehilangan data yang diakibatkan oleh bencana maupun kerusakan alat dan media penyimpanan utama (Setiawan et al., 2021). Dalam menjaga keamanan data, penting punya sistem cadangan yang bisa diakses jika terjadi serangan atau bencana yang menyebabkan data hilang. Melakukan back-up data secara teratur dan merencanakan pemulihan bencana akan membantu organisasi untuk mengembalikan data dengan cepat dan mengurangi gangguan operasional.

- Blockchain

  Untuk memperkuat keamanan data, teknologi blockchain menawarkan solusi yang inovatif dan tahan gangguan (tamper-resistant) dalam menjaga privasi dan integritas data. Blockchain adalah struktur data terdesentralisasi yang terdiri dari blok-blok berisi informasi yang dihubungkan secara berantai. Setiap blok mengandung hash unik yang mengamankan data, sehingga sulit bagi pihak luar untuk memodifikasi informasi tanpa deteksi.

  Menurut (Suryawijaya, 2023) teknologi blockchain dapat meningkatkan keamanan data dengan

beberapa cara. Pertama, blockchain memungkinkan data untuk disimpan secara terdesentralisasi dan terenkripsi, sehingga meningkatkan keamanan data. Karena data tidak disimpan secara sentral, maka sulit bagi orang untuk mencuri data atau mengubahnya tanpa persetujuan dari seluruh jaringan blockchain. Kedua, dalam teknologi blockchain, setiap transaksi dan data dapat diverifikasi oleh semua pihak yang terlibat. Hal ini meningkatkan transparansi dan mengurangi risiko penipuan. Ketiga, proses verifikasi dan validasi dalam teknologi blockchain sangat efisien dan cepat, karena tidak memerlukan perantara atau pihak ketiga. Blockchain juga dapat meningkatkan transparansi dan akuntabilitas dalam pengelolaan data.

2. Aspek Hukum yang Berlaku di Indonesia dalam Menjaga Keamanan Data

Selain hal-hal teknis, aspek hukum juga sangat penting untuk memastikan perlindungan data di Indonesia. Beberapa peraturan dan hukum yang berlaku memberikan panduan bagi para profesional teknologi informasi dan organisasi mengenai standar keamanan yang harus dipatuhi:

- Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE adalah salah satu undang-undang penting di Indonesia yang mengatur tentang keamanan data dan privasi dalam transaksi elektronik. Pasal 26 Undang-Undang ITE menjamin perlindungan data pribadi individu. Individu berhak menuntut secara hukum jika data pribadi mereka disalahgunakan. Selain itu, UU ITE juga mengatur tentang keamanan data, melarang penyadapan atau peretasan yang dilakukan tanpa izin, dan menetapkan sanksi bagi pelanggaran privasi yang terjadi di ruang digital.
- Peraturan Pemerintah No. Undang-undang Nomor 71 Tahun 2019 mengatur cara pengelolaan data pribadi oleh penyelenggara sistem elektronik. Termasuk di dalamnya adalah aspek keamanan data. Peraturan ini menyatakan bahwa penyelenggara wajib melaksanakan langkah-langkah teknis, seperti enkripsi dan autentikasi, untuk melindungi keamanan data. Pengguna layanan berhak mendapatkan informasi tentang data yang dikumpulkan, digunakan, dan dilindungi oleh penyedia layanan. Mereka juga berhak untuk menghapus data pribadi mereka jika diperlukan.
- Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. Peraturan tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik memusatkan perhatian pada cara melindungi data pribadi yang disimpan dan diproses secara elektronik. Peraturan dari Kementerian Komunikasi dan Informatika meminta penyelenggara sistem elektronik untuk melindungi data dan memastikan pengguna bisa mengakses, mengoreksi, atau menghapus data pribadi mereka. Peraturan Komunikasi dan Informatika juga menegaskan betapa pentingnya izin pengguna sebelum data pribadi mereka diolah, dan perlunya pemberitahuan jika terjadi pelanggaran data.
- Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang sedang dalam proses perumusan bertujuan untuk meningkatkan aturan terkait keamanan dan kerahasiaan data di Indonesia. Dengan dasar yang sama dengan GDPR di Uni Eropa, RUU PDP diharapkan memberikan hak yang lebih luas kepada individu atas data pribadi mereka, seperti hak untuk mengakses, mengoreksi, dan menghapus data mereka. RUU ini juga akan mewajibkan organisasi untuk melindungi data pengguna dengan lebih ketat dan

memberlakukan sanksi berat bagi pelanggaran.

3. Pentingnya Kepatuhan terhadap Aspek Teknis dan Hukum bagi Profesional TI

Dalam era serangan siber yang semakin meningkat dan kesadaran akan pentingnya privasi data, para profesional TI bertanggung jawab untuk tidak hanya memahami teknis menjaga keamanan data, tetapi juga mematuhi aturan yang berlaku. Menurut (Nasution et al., 2014) perilaku penggunaan teknologi informasi secara sebagian-sebagian, atas alasan karena menguntungkan saja, bukan untuk tujuan perbaikan mutu kehidupan atau pengajaran, merupakan perilaku fatal dalam menegakkan nilai-nilai keadilan. Keamanan dan kerahasiaan data menjadi sangat penting saat data memiliki nilai. Sebagai contoh, data pribadi masyarakat sebagai warga negara perlu dilindungi karena data tersebut dapat digunakan oleh orang yang tidak berhak untuk berbuat kejahatan, akibatnya pemilik data yang harus bertanggung jawab (Mirna et al., 2023). Memahami UU ITE dan peraturan terkait lainnya merupakan hal penting bagi para profesional TI. Hal ini akan membantu mereka untuk melindungi data pengguna dan perusahaan dari risiko hukum yang dapat timbul karena pelanggaran privasi. Selain itu, aturan ini juga membantu para profesional TI agar lebih berhati-hati dalam mengelola data pribadi, sehingga dapat mencegah pelanggaran hukum.

Dengan menggabungkan pengetahuan teknis dan hukum, para profesional TI dapat lebih efektif dalam melindungi data dengan baik. Ketaatan pada hukum juga membantu menciptakan lingkungan digital yang lebih aman dan dapat dipercaya. Hak privasi pengguna dihormati dan dilindungi sesuai dengan standar yang berlaku.

## KESIMPULAN

Jurnal ini mengatakan bahwa pertumbuhan pesat dalam teknologi informasi (TI) menimbulkan tantangan etika yang semakin rumit, terutama tentang privasi dan keamanan data. Para profesional TI harus menjaga keseimbangan antara inovasi teknologi dan perlindungan data pribadi pengguna dalam menghadapi dilema etis. (Aldiansyah, 2023) Etika profesi TI menekankan pada tanggung jawab sosial para profesional dalam menggunakan teknologi informasi untuk kebaikan masyarakat. Mereka harus mempertimbangkan dampak sosial, lingkungan, dan budaya dalam pengembangan dan implementasi solusi TI juga bertanggung jawab untuk menciptakan teknologi yang efisien dan menjaga keamanan serta keandalan informasi pengguna. Etika profesi di bidang TI mencakup nilai-nilai seperti integritas, kejujuran, dan tanggung jawab. Etika ini penting untuk melindungi privasi pengguna dan memastikan transparansi dalam aktivitas profesional. Tujuannya adalah untuk membangun dan mempertahankan kepercayaan masyarakat terhadap layanan digital.

Di era digital saat ini, privasi individu semakin rentan karena pengumpulan data tanpa izin untuk kepentingan komersial, politik, atau kriminal. Penggunaan Internet of Things (IoT) dan kecerdasan buatan (AI) memungkinkan perusahaan dan penyedia layanan untuk mengumpulkan dan menganalisis data pengguna dengan lebih efisien. Ini berguna untuk memahami pola perilaku pengguna secara mendalam. Walaupun teknologi ini berguna untuk meningkatkan efisiensi dan inovasi, ada risiko besar terkait penyalahgunaan data dan pelanggaran privasi. Profesional TI harus memahami etika dan melindungi privasi individu dalam pengembangan dan penggunaan teknologi. Ini termasuk pendekatan "privacy by design" yang memasukkan perlindungan privasi sejak tahap awal desain sistem.

Langkah-langkah teknis seperti enkripsi, otentikasi, firewall, dan teknologi blockchain penting untuk melindungi data dari serangan dan akses yang tidak sah. Teknologi blockchain memberikan keuntungan transparansi dan keamanan data melalui sistem desentralisasi yang sulit untuk dimanipulasi. Meskipun langkah-langkah ini penting, tetapi tidak akan efektif tanpa adanya aturan yang jelas seperti yang terdapat dalam UU ITE di Indonesia atau GDPR di Uni Eropa. Regulasi ini melindungi pengguna dan

menuntut perusahaan serta profesional TI agar mematuhi standar keamanan data yang ketat. Meski demikian, salah satu masalah utama adalah perkembangan teknologi yang cepat melebihi kemampuan aturan untuk menyesuaikan diri. Oleh karena itu, para profesional TI harus komitmen untuk terus meningkatkan pengetahuan dan praktik mereka dalam mengelola data dengan cara yang etis dan bertanggung jawab.

Secara keseluruhan, kesadaran etis dan kepatuhan terhadap peraturan hukum penting dalam menciptakan lingkungan digital yang aman, etis, dan dapat dipercaya. Tenaga IT sangat penting dalam mengembangkan teknologi yang tidak hanya efisien dan inovatif, tetapi juga memperhatikan privasi dan keamanan pengguna. Dengan menggabungkan keahlian teknis, pemahaman etika, dan kepatuhan terhadap peraturan, para profesional TI bisa membantu menjaga kepercayaan masyarakat terhadap teknologi. Mereka bisa memastikan bahwa teknologi baru tidak hanya bermanfaat untuk semua orang, tapi juga melindungi hak-hak individu. Hal ini membantu mencegah privasi yang bisa terancam dan memberikan rasa aman bagi pengguna di era digital yang terus maju.

**DAFTAR PUSTAKA**

Aldiansyah, R., 2023. Etika Profesi Teknologi Informasi: PelanggaranKeamanan Data 4–9. https://doi.org/10.13140/RG.2.2.25804.18567

Alfarist, A.N., Indonesia, U.K., 2023. Penerapan Enkripsi untuk Meningkatkan Keamanan Data di Cloud Computing.

Anggen Suari, K.R., Sarjana, I.M., 2023. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. J. Anal. Huk. 6, 132–142. https://doi.org/10.38043/jah.v6i1.4484

Dedes, K., Prasetya, A., Laksana, E.P., Ramadhani, L., Setia, V., 2022. Peran Etika dalam Teknologi Informasi. Peran Etika dalam Teknol. Inf. 2, 11–19. https://doi.org/10.17977/um068v2i12022p11-19

Jeffry Yuliyanto Waisapi, 2022. Kode Etik dan Etika Profesi. Formosa J. Soc. Sci. 1, 275–284. https://doi.org/10.55927/fjss.v1i3.1287

Mirna, M., Judhariksawan, Maskum, 2023. Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. J. Ilm. Living Law 15, 16–30. https://doi.org/10.30997/jill.v15i1.4726

Nasution, M.K.M., Sitompul, O.S., Nasution, S., 2014. Perspektif Hukum Teknologi Informasi. Dies Natalis ke-60 Fak. Huk. USU 1, 23. https://doi.org/10.13140/RG.2.2.25583.15520

Setiawan, B.A., Sutanto, N.H., Rahman, G.F., Utami, E., Mustafa, M.S., 2021. Pengamanan Backup dan Restore Basis Data dengan Penambahan Enkripsi Advanced Encryption Standard (Studi Kasus: Analisis Jabatan Bagian Organisasi Kabupaten Balangan). J. Sist. Komput. dan Inform. 2, 277. https://doi.org/10.30865/json.v2i3.2940

Suryawijaya, T.W.E., 2023. Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. J. Stud. Kebijak. Publik 2, 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Wicaksono, D., 2022. Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering. JATISI (Jurnal Tek. Inform. dan Sist. Informasi) 9, 1380–1392. https://doi.org/10.35957/jatisi.v9i2.2103

Yuwinanto, H.P., 2015. Privasi online dan keamanan data. Palimpsest (Iowa. City). 11.

Zarkasyi, Z., 2022. Etika Profesi Dalam Bidang Teknologi Informasi. J. Teknol. Terap. Sains 4.0 3, 719. https://doi.org/10.29103/tts.v3i1.8870