ETIKA DALAM ILMU KOMPUTER

Zen Munawar, M.Kom - Nono Heryana, M.Kom
Dr. Bob Subhan Riza, S.T., M.Kom - Hadiansyah Ma'sum, S.Pd., S.T., M.Kom
Ahmad Setiadi, M.Kom - Budi Wijaya Rauf, S.Kom., M.Kom
Dr. Irmawati, S.Kom., MMSI - Marsujitullah, S.Kom., M.T
Dr. Budi Triandi, M.Kom - Subria Mamis, S.I.Kom., M.I.Kom
Dr. Hendi Sama - Dr. Lili Tanti, M.Kom

Penerbit Yayasan Cendikia Mulia Mandiri

ETIKA DALAM ILMU KOMPUTER

Disusun Oleh:
Zen Munawar, M.Kom
Nono Heryana, M.Kom
Dr. Bob Subhan Riza, S.T., M.Kom
Hadiansyah Ma'sum, S.Pd., S.T., M.Kom
Ahmad Setiadi, M.Kom
Budi Wijaya Rauf, S.Kom., M.Kom
Dr. Irmawati, S.Kom., MMSI
Marsujitullah, S.Kom., M.T
Dr. Budi Triandi, M.Kom
Subria Mamis, S.I.Kom., M.I.Kom
Dr. Hendi Sama
Dr. Lili Tanti, M.Kom

Penerbit Yayasan Cendikia Mulia Mandiri

ETIKA DALAM ILMU KOMPUTER

Penulis:
Zen Munawar, M.Kom
Nono Heryana, M.Kom
Dr. Bob Subhan Riza, S.T., M.Kom
Hadiansyah Ma'sum, S.Pd., S.T., M.Kom
Ahmad Setiadi, M.Kom
Budi Wijaya Rauf, S.Kom., M.Kom
Dr. Irmawati, S.Kom., MMSI
Marsujitullah, S.Kom., M.T
Dr. Budi Triandi, M.Kom
Subria Mamis, S.I.Kom., M.I.Kom
Dr. Hendi Sama
Dr. Lili Tanti, M.Kom

Editor:
Paput Tri Cahyono

Penerbit:
Yayasan Cendikia Mulia Mandiri

Redaksi:
Perumahan Cipta No.1
Kota Batam, 29444
Email: cendikiamuliamandiri@gmail.com

ISBN: 978-623-8382-11-8
Terbit: Agustus 2023
IKAPI: 011/Kepri/2022
Exp. 31 Maret 2024

Ukuran:
xii hal + 241 hal;
14,8cm x 21cm

KATA PENGANTAR

Syukur *alhamdulillah* penulis haturkan kepada Allah Swt. yang senantiasa melimpahkan karunia dan berkah-Nya sehingga penulis mampu merampungkan karya ini tepat pada waktunya, sehingga penulis dapat menghadirkannya dihadapan para pembaca. Kemudian, tak lupa *shalawat* dan salam semoga senantiasa tercurah limpahkan kepada Nabi Muhammad Saw., para sahabat, dan ahli keluarganya yang mulia.

Dalam dunia yang semakin terhubung dan didorong oleh teknologi, peran ilmu komputer tidak dapat diragukan lagi. Namun, di tengah kemajuan yang pesat ini, terbangun pula pertanyaan etika yang mendalam.

Buku ini lahir dari keinginan kami untuk merangkai pemahaman tentang etika dalam konteks ilmu komputer, sebuah perpaduan antara etika klasik dan tantangan yang unik di dunia digital. Kami menjelajahi pertanyaan-pertanyaan kompleks tentang privasi data, kecerdasan buatan, keamanan siber, hak kekayaan intelektual, dan dampak sosial dari teknologi informasi.

Kami membuka jendela ke dunia refleksi moral dan keputusan etis yang harus dihadapi oleh para profesional dan pengguna teknologi. Kami berharap

bahwa buku ini akan membantu para pembaca, baik itu mahasiswa ilmu komputer, praktisi teknologi, atau masyarakat umum, untuk menggali sudut pandang yang mendalam tentang implikasi etis dalam dunia yang semakin terhubung ini.

Dalam keperluan itulah, buku **Etika dalam Ilmu Komputer** ini sengaja penulis hadirkan untuk pembaca. Tujuan buku ini adalah sebagai panduan bagi setiap orang yang ingin mempelajari dan memperdalam ilmu pengetahuan.

Penulis menyampaikan terima kasih yang tak terhingga bagi semua pihak yang telah berpartisipasi. Terakhir seperti kata pepatah bahwa" Tiada Gading Yang Tak Retak" maka penulisan buku ini juga jauh dari kata sempurna, oleh karena itu penulis sangat berterima kasih apabila ada saran dan masukkan yang dapat diberikan guna menyempurnakan buku ini di kemudian hari.

……., Juni 2023

Penulis

DAFTAR ISI

BAB I
PENGANTAR ETIKA DALAM ILMU KOMPUTER

1.1. Pendahuluan

Pada saat ini kehidupan lebih nyaman dibandingkan masa lalu, karena dengan adanya perkembangan komputer dengan internetnya yang telah memberikan kontribusi dalam kenyamanan hidup manusia (Munawar and Indah Putri, 2020). Konsep dasar ilmu komputer dimaksudkan sebagai latihan pertama bagi pembaca yang baru memulai belajar ilmu komputer. Komputer dan aplikasi teknologi sekarang menjadi pusat dari banyak aspek kehidupan dan masyarakat, mulai dari industri dan perdagangan, pemerintahan, penelitian, pendidikan, kedokteran, komunikasi hingga sistem hiburan.

Perkembangan teknologi dan inovasi terjadi dengan kecepatan yang lebih cepat daripada debat etika dan moral yang relevan. Sejarah etika komputasi atau etika komputer berjalan seiring dengan sejarah komputer itu sendiri; sejak awal perkembangan komputer digital, ilmuwan komputer perintis, seperti Turing, Wiener dan

Weizenbaum, berbicara tentang tantangan etika yang melekat pada teknologi komputer (Weizenbaum, 1976; Bynum, 2006), tetapi baru pada tahun 1985 etika komputasi mulai muncul sebagai bidang yang terpisah. Terdapat dua publikasi penting diproduksi, buku Deborah Johnson Computer Ethics dan makalah James Moor, "What Is Computer Ethics?" (Moor, 1985; Johnson, 2008).

Etika Komputer Deborah Johnson adalah buku besar pertama yang berkonsentrasi pada kewajiban etis para profesional komputer, dan dengan cermat mengidentifikasi masalah etika yang unik untuk komputer, berlawanan dengan etika bisnis atau etika hukum. Dia juga mencatat penerapan norma moral umum yang kurang untuk masalah dan dilema moral terkait komputer yang baru dan asing. Teknologi telah mengubah cara kita menjalani kehidupan sehari-hari, cara kita berinteraksi satu sama lain, dan telah mengubah arah sejarah kita. Teknologi mempunyai peran penting dalam mengendalikan berbagai permasalahan yang dihadapi manusia (Putri *et al.*, 2021).

Setiap komputer berkomunikasi dengan komputer lain (Sastradipraja and Munawar, 2022). Oleh karena itu, pengetahuan tentang komputer merupakan kebutuhan bagi keberadaan setiap orang di desa global ini.

Penemuan komputer telah mengubah pekerjaan manual kita yang sederhana menjadi pekerjaan otomatis yang canggih untuk memenuhi permintaan global akan produktivitas yang lebih tinggi dan peningkatan efisiensi dengan presisi tinggi. Dalam kehidupan sehari-hari manusia dapat melihat kemudahan dengan bantuan komputer visi, seperti pengenalan sidik jari dan pengenalan wajah (Munawar and Sastradipraja, 2023).

Namun, komputer juga tidak pintar. Terlepas dari penggambaran yang paling fantastik dalam aksi sains dan dan harapan Kecerdasan Buatan, komputer hanya dapat melakukan apa yang diperintahkan. Seni dasar Ilmu Komputer adalah penyelesaian masalah. Komputer tidak pandai memecahkan masalah; Anda adalah pemecah masalah. Terserah Anda, pengguna, untuk mendekati masalah yang kompleks, mempelajarinya, memahaminya, dan mengembangkan solusinya. Komputer hanya bagus dalam mengotomatiskan solusi setelah Anda menyelesaikan masalahnya.

1.2. Etika Komputer

Etika komputer sebagai "analisis sifat dan dampak sosial dari teknologi komputer dan perumusan yang sesuai dan pembenaran kebijakan untuk penggunaan etis dari teknologi tersebut", dan berpendapat bahwa

teknologi komputer memungkinkan bagi orang untuk melakukan banyak hal yang tidak mungkin dilakukan sebelumnya dan karena tidak ada yang bisa melakukannya sebelumnya, pertanyaan mungkin tidak pernah muncul apakah seseorang harus melakukannya (Moor, 1985).

Bidang etika komputasi terus berkembang pada tahun 1990-an, dan konsep "desain komputer peka nilai" muncul, berdasarkan wawasan bahwa potensi masalah etika komputasi dapat dihindari, sementara teknologi baru sedang dikembangkan, dengan mengantisipasi kemungkinan kerusakan pada nilai-nilai kemanusiaan. dan merancang teknologi baru sejak awal dengan cara yang mencegah bahaya tersebut (Flanagan, Howe and Nissenbaum, 2008). Etika komputasi harus dilihat sebagai kode etik profesional yang dikhususkan untuk pengembangan dan peningkatan standar praktik yang baik bagi para profesional komputasi (Gotterbarn, 1991). Hal ini mengakibatkan pengembangan sejumlah kode etik dan kode etik bagi para profesional komputasi. Salah satu contoh penting adalah kode ACM yang pertama kali ditetapkan pada tahun 1966 dengan judul “Pedoman Perilaku Profesional” dengan tujuan menegakkan perilaku etis dalam profesi komputasi (Gotterbarn *et al.*, 2018). Kode tersebut telah melalui

berbagai pembaruan dengan tetap menjaga etika dan dampak sosial sebagai tujuan utamanya. Salah satu pembaruan terpentingnya adalah pada tahun 1992 ketika namanya diubah menjadi "Kode Etik dan Perilaku Profesional ACMC" dan terdiri dari 25 prinsip etika untuk diikuti oleh para profesional (ACM, 2018).

Pada tahun 1996 meramalkan bahwa teori etika global akan muncul dari waktu ke waktu karena sifat global internet. Perkembangan sejak saat itu tampaknya membenarkan hipotesis Gorniak dan telah menghasilkan teori etika informasi metafisik (Floridi and Sanders, 2005). Teori-teori baru ini memperjelas perubahan sosial dan global yang diciptakan oleh teknologi baru dan menyerukan debat antar budaya tentang etika komputasi untuk mendiskusikan secara kritis dampaknya terhadap masyarakat.

1.2.1. Etika Data

Etika data adalah cabang etika komputasi yang relatif baru yang mempelajari masalah moral terkait manajemen data (termasuk pembuatan, perekaman, kurasi, pemrosesan, penyebaran, pembagian, dan penggunaan) serta algoritme (termasuk yang menggunakan AI, agen buatan, pembelajaran mesin, dan robot) untuk

merumuskan dan mendukung solusi yang baik secara moral untuk data (Floridi and Taddeo, 2016).

Data telah menjadi masukan utama untuk mendorong pertumbuhan, memungkinkan bisnis untuk membedakan diri mereka sendiri, dan mempertahankan keunggulan kompetitif. Nilai sangat tinggi dari pengumpulan massal dan agregasi data, terutama oleh perusahaan dengan model bisnis berbasis data. Namun, penggunaan data agregat mendukung risiko terhadap privasi individu pada tingkat yang sangat mendasar.

Gambar 1. Etika Data

Sumber : (Staff, 2020)

Struktur dan isi kode etik bagi perusahaan yang bergerak dalam bisnis berbasis data, yaitu perusahaan yang proposisi nilainya sangat bergantung pada penggunaan data . Dalam kehidupan sehari-hari manusia dapat melihat

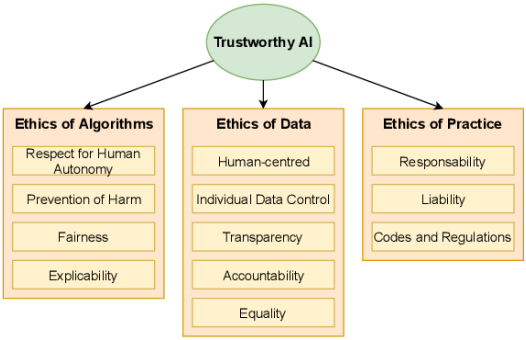
kemudahan dengan bantuan komputer visi, seperti pengenalan sidik jari dan pengenalan wajah (Munawar and Sastradipraja, 2023).

1.3. Etika Kecerdasan Buatan

Kecerdasan buatan (AI) telah muncul sebagai salah satu isu sentral dalam etika komputasi. Masalah terkait dalam etika AI meliputi transparansi; penyertaan; tanggung jawab; ketidakberpihakan; keandalan; keamanan dan Privasi. Sementara banyak peneliti dan pakar teknologi sangat antusias dengan potensi AI, banyak orang lain yang resah karenanya. Penulis menyeimbangkan efek positif AI (mobil self-driving yang mengarah ke keamanan yang lebih baik, asisten digital, robot untuk pekerjaan fisik yang berat; dan algoritme yang kuat untuk mendapatkan wawasan bermanfaat dan penting dari sejumlah besar data) dengan efek negatif dari otomatisasi yang menyebabkan hilangnya pekerjaan, meningkatnya ketidaksetaraan yang dikaitkan dengan AI yang memiliki dan tidak memiliki serta ancaman terhadap privasi (Helbing *et al.*, 2019).

Transparansi dan keadilan algoritma adalah elemen kunci dari sistem AI etis (Webb, Ceppi and Patel, 2018). Sistem AI etis juga harus bekerja untuk menghilangkan bias yang dapat dicapai dengan pemahaman yang lebih

baik tentang data yang digunakan untuk membangun sistem (Floridi and Taddeo, 2016).



Gambar 2. AI Yang Dapat Dipercaya

Sumber : (Kumar and Braud, 2020)

Etika mesin dan robot adalah subbidang penting lainnya dari etika AI. Jika robot bertindak, apakah robot itu sendiri yang bertanggung jawab, bertanggung jawab, atau bertanggung jawab atas tindakannya?

1.4. Etika Komputer dan Informasi

Istilah "etika komputer" dapat ditelusuri kembali ke tahun 1970-an tetapi masalah etika yang timbul dari komputasi digital kembali ke awal perkembangan teknologi (Bynum, 2016). Teknologi ini memiliki potensi untuk mengubah banyak aspek kehidupan yang memiliki kepentingan etis yang krusial. Dia meramalkan perubahan yang relevan secara moral dengan cara kita

berperilaku dalam banyak hal, termasuk peperangan. Pandangan jauh ke depannya sedemikian rupa sehingga, pada awal perkembangan teknologi komputasi, dia mengeksplorasi bagaimana komputer dapat mengubah dunia kerja.

Meskipun ada contoh awal perhatian tingkat tinggi terhadap hubungan antara komputer dan etika, wacana yang lebih luas baru dimulai pada 1980-an dan 1990-an. Selama periode ini, etika komputer berkembang menjadi bidang etika terapan. Pada saat yang sama ketika etika komputer diakui sebagai bidang penyelidikan akademik yang sah, bidang studi—komputer—menjadi kurang dikenal. Meningkatnya integrasi artefak komputasi ke dalam teknologi lain dan lingkungan seperti yang diungkapkan dalam visi teknologi yang ditangkap oleh konsep seperti kecerdasan sekitar Difusi komputer ke lingkungan sekitarnya menimbulkan pertanyaan etis baru terkait dengan isu-isu seperti privasi, pengawasan, otonomi, atau kepemilikan.

1.4.1. Etika Komputasi Pervasif

Istilah "*pervasive computing*", "*ubiquitous computing*", "*ambient intelligence*", dan "*Internet of Things*" mengacu pada visi teknologi yang berbagi satu ide dasar: membuat sumber daya komputasi

tersedia kapan saja dan di mana saja dengan menyematkan perangkat komputasi dalam objek sehari-hari, membebaskan pengguna dari kendala berinteraksi dengan perangkat TIK secara eksplisit melalui keyboard dan layar. Semua program perangkat lunak wajib mematuhi prinsip dan konsep pengkodean tertentu (Munawar, 2023).

Salah satu prinsip utama komputasi pervasif adalah "Memahami dan Mengubah Perilaku", sebuah topik yang jelas memiliki pertimbangan etis yang signifikan (Kranzberg, 2020). Salah satu argumen inti terhadap pengawasan adalah bahwa hal itu menimbulkan ancaman terhadap privasi dan dalam dunia identifikasi otomatis di mana-mana, jumlah data pribadi yang dihasilkan dan diedarkan diperkirakan akan meningkat secara dramatis.

Dalam konteks komputasi, privasi biasanya diartikan sebagai "privasi informasional", yang merupakan keadaan yang ditandai "dengan mengontrol apakah dan bagaimana data pribadi dapat dikumpulkan, disimpan, diproses, atau disebarluaskan secara selektif".

Ada konflik yang jelas antara privasi dan teknologi komputasi pervasif, khususnya teknologi yang berhubungan dengan penginderaan dan

penyimpanan (Jacobs dan Abowd, 2003). Persyaratan yang dihasilkan untuk melindungi privasi individu terhadap penyalahgunaan data memasuki banyak undang-undang dan perjanjian internasional dengan istilah yang berbeda, beberapa di antaranya berfokus pada aspek defensif, seperti "perlindungan data", yang lain menekankan otonomi individu, seperti "penentuan nasib sendiri secara informasi".

1.4.2. Etika Komputer adalah bentuk etika kompensasi

Etika Komputer dianggap membantu karena teknologi berkembang sangat cepat dan masyarakat mungkin menghadapi skenario tak terduga di mana tidak ada kebijakan atau pedoman yang jelas: dalam situasi yang benar-benar baru ini, sangat sulit untuk memutuskan apa yang benar dan apa yang salah. Asumsi dasarnya adalah bahwa teknologi itu netral dan tidak dihasilkan dari interaksi yang kompleks dengan masyarakat, konsekuensi dari pilihan manusia, sebuah artifak yang menanamkan nilai. Dari sudut pandang ini, Etika Komputer adalah bentuk etika kompensasi atau reaktif.

R Namun demikian, pendekatan reaktif ini pun memainkan peran penting sebagai bidang etika terapan dan mendukung definisi banyak kebijakan terkait TIK.

BAB II
DASAR-DASAR ETIKA ILMU KOMPUTER

2.1. Prinsip-Prinsip Etika dalam Ilmu Komputer

Etika dalam ilmu komputer mencakup sejumlah prinsip yang harus dihargai dan diikuti oleh para profesional di bidang ini. Prinsip-prinsip ini mencakup kejujuran dan integritas, kerahasiaan dan privasi, keamanan, serta tanggung jawab dan akuntabilitas.

2.1.1. Prinsip Kejujuran dan Integritas

Kejujuran dan integritas adalah dua prinsip etika kunci dalam ilmu komputer. Kejujuran merujuk pada komitmen untuk selalu memberikan informasi yang benar dan akurat, serta tidak menyesatkan atau menipu orang lain. Dalam konteks ilmu komputer, ini bisa mencakup hal-hal seperti tidak memanipulasi data, tidak mencuri atau menggunakan perangkat lunak secara ilegal, dan tidak menyebarluaskan informasi palsu atau menyesatkan (Gotterbarn dkk, 2001).

Integritas, di sisi lain, adalah komitmen untuk bertindak dengan prinsip moral dan etika yang konsisten, dan untuk selalu melakukan yang benar,

bahkan ketika tidak ada yang melihat. Dalam ilmu komputer, integritas bisa mencakup hal-hal seperti menjaga standar profesional yang tinggi, tidak menyalahgunakan akses atau kekuasaan, dan tidak mengambil keuntungan dari orang lain atau situasi untuk keuntungan pribadi (Floridi, 2010).

2.1.2. Prinsip Kerahasiaan dan Privasi

Prinsip kerahasiaan dan privasi merupakan dua elemen penting dalam etika ilmu komputer. Kerahasiaan merujuk pada perlindungan informasi dari akses yang tidak sah, sedangkan privasi merujuk pada hak individu untuk mengontrol penggunaan dan penyebaran informasi pribadi mereka (Koontz, 2017).

Dalam konteks ilmu komputer, kerahasiaan dan privasi sering kali menjadi isu utama, terutama dalam era digital saat ini di mana data pribadi dan informasi sensitif sering kali disimpan dan diproses secara elektronik. Misalnya, dalam pengembangan perangkat lunak, penting bagi pengembang untuk memastikan bahwa data pengguna dilindungi dari akses yang tidak sah dan penyalahgunaan (Bynum & Rogerson, 2003).

Dalam pengelolaan dan analisis data, profesional ilmu komputer harus memastikan bahwa data pribadi pengguna dihargai dan dilindungi. Ini termasuk memastikan bahwa data tersebut hanya digunakan untuk tujuan yang telah disetujui oleh pengguna dan tidak disebarkan tanpa izin (Ahmad dkk., 2022).

Menjaga kerahasiaan dan privasi dalam ilmu komputer bukanlah tugas yang mudah. Ada banyak tantangan yang dihadapi, seperti ancaman keamanan siber, kebocoran data, dan penyalahgunaan data. Oleh karena itu, penting bagi profesional ilmu komputer untuk terus memperbarui pengetahuan dan keterampilan mereka dalam bidang keamanan informasi dan privasi (Olayinka & Win, 2022).

2.1.3. Prinsip Keamanan

Prinsip keamanan dalam ilmu komputer merujuk pada perlindungan data dan sistem dari akses yang tidak sah, penggunaan yang tidak tepat, pengungkapan, perusakan, modifikasi, atau gangguan (Von Solms & Van Niekerk, 2013). Dalam konteks ini, keamanan tidak hanya berarti menjaga informasi dari ancaman eksternal, tetapi juga

memastikan bahwa data dan sistem tetap aman dari ancaman internal.

Keamanan dalam ilmu komputer melibatkan berbagai aspek, termasuk keamanan fisik, keamanan jaringan, keamanan aplikasi, dan keamanan data. Keamanan fisik melibatkan perlindungan terhadap perangkat keras dan infrastruktur fisik. Keamanan jaringan berfokus pada perlindungan terhadap data saat transit, sedangkan keamanan aplikasi berfokus pada perlindungan terhadap perangkat lunak dan aplikasi dari eksploitasi dan serangan. Keamanan data, di sisi lain, berfokus pada perlindungan data dan informasi dari akses dan penggunaan yang tidak sah (Bishop, 2005).

Prinsip keamanan juga mencakup pemahaman tentang ancaman dan risiko yang mungkin dihadapi oleh sistem dan data, serta langkah-langkah yang perlu diambil untuk mengurangi risiko tersebut. Ini melibatkan proses identifikasi dan penilaian risiko, serta pengembangan dan implementasi kontrol dan langkah-langkah mitigasi yang tepat (Stallings & Brown, 2013).

2.1.4. Prinsip Tanggung Jawab dan Akuntabilitas

Prinsip tanggung jawab dan akuntabilitas adalah dua pilar penting dalam etika ilmu komputer. Tanggung jawab merujuk pada kewajiban profesional untuk memastikan bahwa tindakan dan keputusan yang diambil tidak merugikan individu atau masyarakat secara keseluruhan. Ini mencakup tanggung jawab untuk memastikan bahwa perangkat lunak dan sistem yang dikembangkan aman, efisien, dan efektif.

Akuntabilitas, di sisi lain, merujuk pada kewajiban untuk menjelaskan dan mempertanggungjawabkan tindakan dan keputusan yang diambil. Dalam konteks ilmu komputer, ini bisa berarti mempertanggungjawabkan keputusan desain, penggunaan data, atau cara penanganan masalah keamanan (Zhang dkk., 2023).

Prinsip tanggung jawab dan akuntabilitas sangat penting dalam ilmu komputer karena teknologi memiliki dampak yang signifikan pada masyarakat. Misalnya, keputusan desain dalam pengembangan algoritma dapat mempengaruhi privasi dan kebebasan individu, sementara keputusan tentang bagaimana data digunakan

dapat mempengaruhi hak asasi manusia dan demokrasi (Zuboff, 2019). Oleh karena itu, sangat penting bagi profesional ilmu komputer untuk memahami dan menerapkan prinsip tanggung jawab dan akuntabilitas dalam pekerjaan mereka.

2.2. Teori Etika yang Berlaku dalam Ilmu Komputer

Ilmu komputer, seperti bidang profesional lainnya, memerlukan kerangka etika yang kuat untuk membimbing praktisi dalam membuat keputusan yang bertanggung jawab dan etis. Beberapa teori etika utama yang berlaku dalam ilmu komputer meliputi utilitarianisme, deontologi, teori hak asasi manusia, dan teori keadilan.

2.2.1. Utilitarianisme dalam Ilmu Komputer

Utilitarianisme adalah teori etika yang berfokus pada hasil atau konsekuensi dari tindakan. Dalam konteks ilmu komputer, utilitarianisme dapat diterapkan untuk mengevaluasi dampak teknologi dan keputusan yang dibuat dalam pengembangan dan penerapan teknologi. Pendekatan ini menekankan pada pencapaian hasil yang paling menguntungkan bagi sebanyak mungkin orang (Cavalier, 2005).

Dalam prakteknya, utilitarianisme dalam ilmu komputer bisa berarti membuat keputusan desain atau implementasi yang berfokus pada manfaat maksimal bagi pengguna. Misalnya, dalam pengembangan algoritma kecerdasan buatan, pendekatan utilitarian mungkin akan mempertimbangkan bagaimana algoritma tersebut dapat digunakan untuk memberikan manfaat terbesar bagi sebanyak mungkin orang, seperti dengan memaksimalkan efisiensi atau efektivitas.

Namun, utilitarianisme juga memiliki tantangan. Salah satunya adalah bagaimana menentukan apa yang dianggap "baik" atau "menguntungkan". Dalam konteks ilmu komputer, ini bisa menjadi kompleks, karena teknologi seringkali memiliki dampak yang beragam dan tidak terduga. Selain itu, utilitarianisme juga bisa berpotensi mengabaikan hak dan kepentingan individu atau kelompok minoritas jika mereka tidak sejalan dengan "kebaikan" mayoritas.

Dalam konteks etika komputasi, utilitarianisme harus digunakan dengan hati-hati, dengan mempertimbangkan berbagai dampak potensial dari teknologi dan keputusan yang dibuat dalam pengembangannya. Selain itu, penting juga

untuk mempertimbangkan pendekatan etika lainnya, seperti deontologi dan teori hak asasi manusia, untuk memastikan bahwa keputusan yang dibuat tidak hanya menguntungkan, tetapi juga adil dan menghormati hak-hak individu (Zuber, 2022).

2.2.2. Deontologi dalam Ilmu Komputer

Deontologi adalah teori etika yang menekankan pada tindakan itu sendiri, bukan hasil dari tindakan tersebut. Dalam konteks ilmu komputer, deontologi dapat digunakan untuk mengevaluasi tindakan yang dilakukan oleh profesional IT, seperti pengembang perangkat lunak, administrator sistem, dan lainnya, berdasarkan prinsip-prinsip moral dan etika, bukan berdasarkan hasil atau konsekuensi dari tindakan tersebut (Prabhumoye dkk., 2020).

Misalnya, dalam pengembangan perangkat lunak, pendekatan deontologis akan menekankan pada pentingnya mengikuti standar dan pedoman pengembangan yang baik, seperti tidak menggunakan kode yang telah dipatenkan tanpa izin, atau tidak mencoba untuk menyembunyikan bug atau kesalahan dalam kode. Hal ini berlaku bahkan jika tindakan tersebut mungkin akan

menghasilkan perangkat lunak yang lebih baik atau lebih cepat (Hall, 2020).

Deontologi menekankan pada pentingnya tanggung jawab dan akuntabilitas. Dalam konteks ilmu komputer, ini berarti bahwa profesional IT harus bertanggung jawab atas tindakan mereka dan harus siap untuk menerima konsekuensi jika mereka melanggar prinsip-prinsip etika atau hukum yang berlaku. Pendekatan deontologis juga memiliki tantangan tersendiri. Misalnya, dalam situasi di mana ada konflik antara prinsip-prinsip etika, bisa jadi sulit untuk menentukan tindakan mana yang harus diambil. Selain itu, dalam dunia yang semakin digital dan terkoneksi, bisa jadi sulit untuk menentukan siapa yang harus bertanggung jawab atas tindakan tertentu (Burton dkk., 2023).

2.2.3. Teori Hak Asasi Manusia dalam Ilmu Komputer

Teori Hak Asasi Manusia dalam Ilmu Komputer merujuk pada prinsip-prinsip etika yang menekankan perlindungan dan penghormatan terhadap hak-hak dasar individu dalam konteks penggunaan dan pengembangan teknologi komputer. Dalam era digital saat ini, isu-isu seperti

privasi data, akses yang adil terhadap teknologi, dan kebebasan berekspresi online menjadi sangat penting.

Privasi data adalah salah satu aspek kunci dalam teori ini. Menurut *United Nations Human Rights Council* (2019), setiap individu memiliki hak untuk melindungi data pribadinya dan memiliki kontrol atas bagaimana data tersebut digunakan dan dibagikan. Dalam konteks ilmu komputer, ini berarti bahwa sistem dan aplikasi harus dirancang dengan mempertimbangkan privasi data pengguna.

Akses yang adil terhadap teknologi juga menjadi bagian penting dari teori hak asasi manusia dalam ilmu komputer. Dalam laporan oleh World Bank (2020), digital divide atau kesenjangan digital masih menjadi masalah global yang perlu ditangani. Oleh karena itu, dalam pengembangan dan implementasi teknologi, perlu dipastikan bahwa semua individu memiliki akses yang sama dan adil.

Kebebasan berekspresi online juga menjadi isu penting dalam teori ini. Menurut *Amnesty International* (2022), pembatasan kebebasan berekspresi dan penyalahgunaan teknologi untuk pengawasan merupakan pelanggaran hak asasi manusia. Oleh karena itu, dalam ilmu komputer,

penting untuk memastikan bahwa teknologi tidak digunakan untuk membatasi kebebasan individu untuk berkomunikasi dan berbagi informasi.

2.2.4. Teori Keadilan dalam Ilmu Komputer

Teori keadilan dalam ilmu komputer merujuk pada konsep bahwa semua individu harus memiliki akses yang sama dan adil terhadap teknologi dan manfaat yang ditawarkannya. Ini mencakup akses ke perangkat keras dan perangkat lunak, serta layanan dan sumber daya digital lainnya. Teori ini juga mencakup ide bahwa individu harus memiliki kesempatan yang sama untuk belajar dan mengembangkan keterampilan dalam ilmu komputer, serta kesempatan yang sama untuk berpartisipasi dalam pengembangan dan implementasi teknologi baru (Robbins, 2020).

Teori keadilan juga berfokus pada perlindungan terhadap individu dan kelompok yang rentan terhadap diskriminasi atau eksploitasi oleh teknologi. Misalnya, algoritma yang bias dapat menghasilkan hasil yang merugikan bagi kelompok tertentu, dan teori keadilan menekankan pentingnya mencegah dan mengatasi bias ini (O'Neil, 2016).

Selain itu, teori keadilan juga mencakup konsep distribusi yang adil dari risiko dan manfaat teknologi. Misalnya, dalam konteks kecerdasan buatan, ini bisa berarti memastikan bahwa manfaat dari AI, seperti peningkatan efisiensi dan produktivitas, dibagikan secara merata di seluruh masyarakat, sementara risiko, seperti hilangnya pekerjaan karena otomatisasi, tidak dipikul secara tidak proporsional oleh kelompok tertentu (Bryson, 2019).

2.3. Penerapan Etika dalam Praktek Ilmu Komputer

Etika dalam praktek ilmu komputer mencakup berbagai aspek, termasuk pengkodean dan pengembangan perangkat lunak, penggunaan dan pengelolaan data, serta komunikasi dan kolaborasi. Dalam setiap aspek ini, ada standar etika yang harus dipatuhi oleh para profesional di bidang ini.

2.3.1. Etika dalam Pengkodean dan Pengembangan Perangkat Lunak

Etika dalam pengkodean dan pengembangan perangkat lunak merujuk pada serangkaian prinsip dan standar yang membimbing perilaku profesional para pengembang perangkat lunak. Prinsip-prinsip

ini mencakup kejujuran, integritas, transparansi, dan tanggung jawab dalam semua aspek pengembangan perangkat lunak, mulai dari desain awal hingga pemeliharaan pasca-rilis.

Salah satu aspek penting dari etika pengkodean adalah kejujuran dan transparansi dalam proses pengembangan. Pengembang perangkat lunak harus selalu jujur tentang kemampuan dan batasan perangkat lunak yang mereka kembangkan, serta tentang bug dan masalah keamanan yang mungkin ada (Bélanger & Crossler, 2011). Mereka juga harus transparan tentang penggunaan data pengguna dan memastikan bahwa data tersebut digunakan dan disimpan dengan cara yang aman dan etis.

Etika pengkodean mencakup tanggung jawab untuk menciptakan perangkat lunak yang aman dan bebas dari bug sebanyak mungkin. Pengembang perangkat lunak harus berusaha keras untuk meminimalkan kesalahan dalam kode mereka dan harus segera memperbaiki bug atau masalah keamanan yang ditemukan.

Etika pengkodean juga mencakup pertimbangan tentang dampak sosial dan lingkungan dari perangkat lunak. Pengembang

perangkat lunak harus mempertimbangkan bagaimana perangkat lunak mereka dapat digunakan atau disalahgunakan, dan mereka harus berusaha untuk meminimalkan dampak negatif potensial dari perangkat lunak mereka (Friedman & Nissenbaum, 1996).

2.3.2. Etika dalam Penggunaan dan Pengelolaan Data

Etika dalam penggunaan dan pengelolaan data merujuk pada serangkaian prinsip dan pedoman yang mengatur bagaimana data dikumpulkan, disimpan, diproses, dan digunakan (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016). Dalam era digital saat ini, data telah menjadi aset yang sangat berharga dan penting. Namun, penggunaan dan pengelolaan data yang tidak etis dapat menimbulkan berbagai masalah, termasuk pelanggaran privasi, diskriminasi, dan penyalahgunaan data.

Pertama, dalam konteks pengumpulan data, etika menuntut transparansi dan persetujuan dari individu yang datanya dikumpulkan (Zwitter & Boisse-Despiaux, 2018). Ini berarti bahwa organisasi harus jelas tentang tujuan pengumpulan

data, jenis data yang dikumpulkan, dan bagaimana data tersebut akan digunakan dan disimpan.

Kedua, dalam penyimpanan data, etika menuntut perlindungan dan keamanan data yang memadai. Ini melibatkan penggunaan teknologi dan prosedur keamanan yang tepat untuk mencegah akses atau penggunaan data yang tidak sah (Bello-Orgaz, Jung, & Camacho, 2016).

Ketiga, dalam pengolahan dan penggunaan data, etika menuntut penggunaan data yang adil dan tidak diskriminatif. Ini berarti bahwa algoritma dan model yang digunakan untuk menganalisis data tidak boleh bias atau mendiskriminasi kelompok tertentu (Crawford & Schultz, 2014).

2.3.3. Etika dalam Komunikasi dan Kolaborasi

Komunikasi dan kolaborasi merupakan aspek penting dalam ilmu komputer, terutama dalam konteks pengembangan perangkat lunak dan manajemen proyek IT. Etika dalam komunikasi dan kolaborasi mencakup berbagai elemen seperti kejujuran, transparansi, rasa hormat, dan kerahasiaan (Al-Saqqa, 2022).

Kejujuran dan transparansi sangat penting dalam komunikasi dan kolaborasi. Dalam konteks

ilmu komputer, ini berarti bahwa semua anggota tim harus jujur tentang kemampuan mereka, batasan waktu, dan masalah yang mungkin muncul dalam proyek. Transparansi juga berarti berbagi informasi yang relevan dan penting dengan semua anggota tim (Schulz-Knappe, 2019).

Rasa hormat juga merupakan aspek penting dari etika dalam komunikasi dan kolaborasi. Ini mencakup menghargai ide dan pendapat orang lain, mendengarkan dengan penuh perhatian, dan menghindari perilaku yang merendahkan atau menghina. Rasa hormat juga mencakup pengakuan terhadap keragaman dan inklusivitas dalam tim (Levesque dkk., 2022).

Kerahasiaan juga penting dalam komunikasi dan kolaborasi dalam ilmu komputer. Informasi yang dibagikan dalam tim harus dijaga kerahasiaannya dan tidak boleh dibagikan tanpa izin. Ini juga berarti bahwa data dan informasi pribadi yang diperoleh selama proyek harus dijaga dan dilindungi (Zhao dkk., 2019).

2.4. Etika dalam Konteks Hukum dan Regulasi

Etika dalam ilmu komputer tidak hanya berfungsi sebagai pedoman moral bagi individu dan organisasi,

tetapi juga berinteraksi dengan hukum dan regulasi yang berlaku. Hukum dan regulasi seringkali mencerminkan standar etika masyarakat dan berfungsi untuk memastikan bahwa praktik dalam ilmu komputer mematuhi standar tersebut. Namun, hukum dan regulasi juga dapat berfungsi sebagai batas minimum, dengan etika memberikan pedoman lebih lanjut tentang bagaimana bertindak di atas dan di luar apa yang secara hukum diharuskan (Tavani, 2016).

2.4.1. Hukum dan Regulasi yang Berlaku

Hukum dan regulasi yang berlaku dalam ilmu komputer merupakan aspek penting dalam memastikan bahwa penggunaan teknologi informasi dan komputer dilakukan secara etis dan bertanggung jawab. Penerapan hukum dan regulasi yang tepat dapat membantu melindungi privasi, keamanan, dan hak-hak individu dalam era digital.

Hukum dan regulasi terkait ilmu komputer dapat mencakup berbagai aspek, seperti perlindungan data pribadi, hak kekayaan intelektual, keamanan siber, privasi online, dan aksesibilitas teknologi. Contohnya, dalam konteks perlindungan data pribadi, beberapa negara atau wilayah telah mengadopsi peraturan yang ketat

seperti *General Data Protection Regulation (GDPR)* di Uni Eropa atau *California Consumer Privacy Act (CCPA)* di Amerika Serikat. Ketentuan dalam peraturan ini mengatur bagaimana data pribadi harus diperlakukan, bagaimana pengguna harus memberikan persetujuan, dan apa yang harus dilakukan jika terjadi pelanggaran data.

Hukum dan regulasi dapat mengatur hak kekayaan intelektual terkait dengan perangkat lunak, algoritma, atau penemuan dalam ilmu komputer. Misalnya, Undang-Undang Hak Cipta di banyak negara melindungi perangkat lunak dan konten digital dari pelanggaran hak cipta. Hal ini penting untuk memastikan bahwa pencipta perangkat lunak mendapatkan pengakuan dan penghargaan yang layak atas karya mereka.

2.4.2. Implikasi Hukum dari Pelanggaran Etika Ilmu Komputer

Implikasi hukum dari pelanggaran etika dalam ilmu komputer adalah aspek penting yang perlu dipahami oleh para profesional dan praktisi di bidang ini. Ketika etika diabaikan atau dilanggar, konsekuensinya tidak hanya moral tetapi juga dapat melibatkan tindakan hukum dan sanksi.

Pelanggaran etika dalam ilmu komputer dapat menghasilkan kerugian finansial, kerugian reputasi, atau bahkan masalah hukum yang serius.

Salah satu contoh pelanggaran etika yang memiliki implikasi hukum adalah pencurian data atau pelanggaran privasi. Dalam era digital yang semakin maju, perlindungan data dan privasi menjadi perhatian utama. Jika seseorang atau suatu perusahaan mengakses, mencuri, atau menggunakan data pribadi tanpa izin, mereka dapat melanggar undang-undang privasi dan menjadi subjek tuntutan hukum. Sebagai contoh, kasus pelanggaran privasi yang melibatkan Facebook dan Cambridge Analytica pada tahun 2018 mengakibatkan investigasi dan tindakan hukum di berbagai negara, serta berdampak pada reputasi dan nilai saham Facebook.

Penyebaran malware, serangan siber, atau hacking juga merupakan pelanggaran etika dan melanggar hukum. Tindakan ini dapat merugikan individu atau organisasi dengan merusak sistem, mencuri informasi penting, atau mengganggu operasi yang sah. Pemerintah dan lembaga penegak hukum secara aktif menindak dan memperketat undang-undang terkait kejahatan komputer untuk

melindungi masyarakat dan infrastruktur yang rentan. Kasus terkenal seperti serangan ransomware WannaCry pada tahun 2017 dan serangan siber terhadap perusahaan besar seperti Equifax pada tahun 2017 juga menghasilkan tindakan hukum dan sanksi.

Gambar 2.1 Serangan Ransomware WannaCry (Healthcare IT News)

Implikasi hukum lainnya dari pelanggaran etika dalam ilmu komputer dapat mencakup pelanggaran hak kekayaan intelektual, penyebaran konten ilegal seperti pornografi anak, atau penggunaan teknologi untuk tujuan kriminal seperti perdagangan narkoba atau pencucian uang. Di setiap kasus ini, pelanggaran etika yang dilakukan di

dunia digital dapat memiliki konsekuensi hukum yang signifikan.

Penting untuk diingat bahwa implikasi hukum dapat bervariasi berdasarkan yurisdiksi dan undang-undang yang berlaku di negara tertentu. Oleh karena itu, sangat penting bagi para profesional dan praktisi dalam ilmu komputer untuk memahami dan mematuhi peraturan hukum yang relevan dalam lingkup kerja mereka.

2.5. Kasus Studi: Pelanggaran Etika dalam Ilmu Komputer

2.5.1. Analisis Kasus dan Dampaknya

Dalam studi kasus ini, kita akan menganalisis beberapa contoh pelanggaran etika dalam ilmu komputer yang telah terjadi dan mengidentifikasi dampaknya. Salah satu contoh yang relevan adalah pelanggaran privasi data yang melibatkan perusahaan teknologi besar seperti Facebook. Pada tahun 2018, terungkap bahwa data pribadi jutaan pengguna Facebook telah disalahgunakan oleh perusahaan konsultan politik Cambridge Analytica tanpa persetujuan yang jelas. Pelanggaran ini mengungkapkan kerentanan data pengguna dan memicu kekhawatiran tentang privasi online.

Gambar 2.2 Skandal Cambridge Analytica dan Facebook (Inc Magazine)

Dampak dari pelanggaran privasi data semacam ini sangat signifikan. Pengguna merasa kehilangan kepercayaan terhadap platform media sosial dan keraguan terhadap perlindungan privasi mereka. Selain itu, informasi yang dikumpulkan juga dapat digunakan untuk tujuan manipulatif seperti pengaruh politik dan iklan yang tidak etis. Pelanggaran ini juga dapat berdampak negatif pada reputasi perusahaan yang terlibat dan menyebabkan kerugian finansial yang serius.

Salah satu contoh pelanggaran etika dalam ilmu komputer di Indonesia adalah tindakan pembajakan atau penggunaan software bajakan. Hal ini sering terjadi karena harga software yang asli terkadang terlalu mahal bagi sebagian orang.

Namun, tindakan ini jelas melanggar hak cipta dan merugikan para pengembang software yang telah mengeluarkan biaya besar untuk mengembangkan produk mereka.

Sebuah studi tentang kejahatan siber dan serangan peretasan juga bisa menjadi kasus yang menarik untuk dianalisis. Contohnya adalah serangan peretasan terhadap sebuah perusahaan besar yang mengakibatkan pencurian data pribadi pelanggan dan kerugian finansial yang signifikan. Analisis kasus semacam ini akan menyoroti konsekuensi serius dari pelanggaran etika dalam ilmu komputer, termasuk kerugian keuangan, kerusakan reputasi, dan ketidakstabilan pasar.

2.5.2. Solusi dan Pencegahan untuk Kasus Pelanggaran Etika

Salah satu solusi adalah dengan meningkatkan kesadaran etika melalui pelatihan dan pendidikan. Ini dapat dilakukan dengan memasukkan isu etika dalam kurikulum pendidikan ilmu komputer dan menyediakan pelatihan khusus tentang etika dalam praktik industri. Studi menunjukkan bahwa pendidikan etika efektif dapat mempengaruhi sikap dan perilaku profesional

dalam menjaga integritas dan tanggung jawab dalam ilmu komputer.

Perlunya peran lembaga regulasi dan etika juga harus diperhatikan. Organisasi profesional seperti ACM (Association for Computing Machinery) dan IEEE (Institute of Electrical and Electronics Engineers) telah mengembangkan kode etik yang mengatur perilaku anggotanya dalam ilmu komputer. Penerapan dan penegakan kode etik ini merupakan langkah penting dalam mencegah pelanggaran etika dan mempromosikan tanggung jawab profesional.

Dalam mengatasi kasus pelanggaran etika, penting juga untuk mempertimbangkan aspek hukum dan regulasi yang berlaku. Pemerintah dan lembaga terkait harus memperkuat kerangka hukum yang mengatur penggunaan data pribadi, keamanan siber, privasi, dan pelanggaran etika lainnya dalam ilmu komputer.

Melalui solusi dan pencegahan yang tepat, diharapkan kita dapat meminimalkan kasus-kasus pelanggaran etika dalam ilmu komputer dan membangun lingkungan yang lebih etis, bertanggung jawab, dan aman dalam penggunaan teknologi.

BAB III
TANGGUNG JAWAB PROFESIONAL DALAM ILMU KOMPUTER

3.1. Pengenalan Tanggung Jawab Profesional dalam Ilmu Komputer

Dalam era digital yang semakin berkembang, ilmu komputer memiliki peran yang semakin krusial dalam kehidupan sehari-hari dan bisnis. Teknologi informasi telah membawa transformasi signifikan dalam berbagai bidang, termasuk komunikasi, kesehatan, pendidikan, dan industri. Seiring dengan kemajuan ini, muncul pula tanggung jawab yang lebih besar bagi para profesional di bidang ilmu komputer. Tanggung jawab ini mencakup tidak hanya aspek teknis, tetapi juga etika, keamanan, dan dampak sosial dari teknologi yang dihasilkan.

Tujuan dari tanggung jawab profesional dalam ilmu komputer adalah untuk memastikan bahwa perkembangan dan pemanfaatan teknologi informasi dan komputer dilakukan dengan cara yang etis, aman, dan bertanggung jawab. Tanggung jawab ini mencakup beberapa aspek penting, antara lain:

1. Etika Profesional

Para profesional ilmu komputer diharapkan mengikuti prinsip-prinsip etika dalam semua aspek pekerjaan mereka. Hal ini meliputi perlindungan hak cipta, kerahasiaan data, dan pengembangan teknologi yang menghormati nilai-nilai sosial.

2. Keamanan Informasi dan Privasi

   Profesional ilmu komputer harus bertanggung jawab dalam menjaga keamanan data dan privasi pengguna. Mereka harus mengidentifikasi potensi risiko dan melaksanakan langkah-langkah untuk melindungi sistem dan data dari serangan siber.

3. Kualitas Perangkat Lunak

   Profesional di bidang ini bertanggung jawab untuk mengembangkan perangkat lunak berkualitas tinggi yang memenuhi standar keandalan dan kinerja.

4. Pendidikan Profesional

   Tanggung jawab profesional juga mencakup upaya untuk terus mengembangkan pengetahuan mereka dengan mengikuti perkembangan teknologi terbaru dan berpartisipasi dalam pelatihan dan sertifikasi.

5. Dampak Sosial

Para profesional ilmu komputer juga memiliki tanggung jawab dalam memahami dampak sosial dari teknologi yang mereka hasilkan. Mereka harus berusaha untuk mengembangkan solusi yang bermanfaat bagi masyarakat dan menghindari dampak negatif.

3.2. Etika Profesional dalam Ilmu Komputer

Etika profesional dalam ilmu komputer mengacu pada seperangkat prinsip dan norma yang mengatur perilaku para profesional dalam industri teknologi informasi. Etika ini bertujuan untuk memastikan bahwa para profesional bertindak dengan integritas, transparansi, dan tanggung jawab dalam setiap aspek pekerjaan mereka. Prinsip Etika Profesional:

a. Integritas: Para profesional diharapkan untuk berperilaku jujur dan adil, menjaga kebenaran dan integritas dalam pekerjaan mereka. Mereka tidak boleh terlibat dalam manipulasi data atau informasi dengan cara yang merugikan.
b. Transparansi: Prinsip ini menekankan pentingnya memberikan informasi yang jelas dan akurat kepada semua pihak terkait. Profesional harus memastikan bahwa keputusan

teknis dan bisnis didasarkan pada data yang benar dan relevan.

c. Tanggung Jawab: Para profesional memiliki tanggung jawab terhadap pengguna akhir, masyarakat, dan lingkungan. Mereka harus memastikan bahwa teknologi yang dikembangkan tidak hanya bermanfaat, tetapi juga tidak membahayakan pengguna atau lingkungan.

Adapun tanggung Jawab terhadap pengguna akhir adalah para profesional harus mendengarkan dan memahami kebutuhan pengguna akhir. Mereka harus mengembangkan solusi yang mudah digunakan, aman, dan sesuai dengan tujuan pengguna. Profesional harus menjaga kerahasiaan informasi dan data yang diberikan oleh pengguna. Mereka tidak boleh mengungkapkan atau menyalahgunakan informasi pribadi atau rahasia. Profesional harus menghormati hak cipta dan kepemilikan intelektual. Mereka tidak boleh mencuri kode sumber, menyalin perangkat lunak tanpa izin, atau menggunakan materi yang dilindungi hak cipta tanpa izin. Para profesional harus mempertimbangkan dampak sosial dan lingkungan dari teknologi yang mereka kembangkan. Mereka harus menghindari

menciptakan teknologi yang dapat digunakan untuk tujuan merugikan atau melanggar hukum.

3.3. Keamanan Informasi dan Privasi

Keamanan informasi dan privasi merupakan aspek penting dalam tanggung jawab profesional dalam ilmu komputer. Ini melibatkan langkah-langkah untuk melindungi data dan informasi sensitif, baik milik pengguna akhir maupun organisasi, dari ancaman dan pelanggaran yang dapat merugikan. Para profesional harus mengambil langkah-langkah untuk melindungi data pribadi pengguna, seperti informasi identitas, alamat, nomor telepon, dan lainnya. Pengumpulan, penyimpanan, dan penggunaan data pribadi harus sesuai dengan peraturan dan hukum yang berlaku.

Profesional harus mengimplementasikan langkah-langkah keamanan yang kuat untuk melindungi jaringan dan sistem komputer dari serangan dan akses yang tidak sah. Ini melibatkan penggunaan firewall, enkripsi data, dan pembaruan rutin untuk melawan kerentanan keamanan

Ancaman siber seperti malware, serangan DDoS, pencurian data, dan phising adalah risiko nyata dalam lingkungan digital. Para profesional harus mengidentifikasi dan mengurangi risiko ini dengan

mengadopsi praktik-praktik keamanan yang tepat, seperti pemantauan jaringan, identifikasi ancaman, dan pelatihan keamanan bagi pengguna.

Keamanan harus dipertimbangkan sejak awal dalam pengembangan perangkat lunak. Para profesional harus mengintegrasikan langkah-langkah keamanan seperti pengujian penetrasi, pengkodean aman, dan penerapan prinsip Secure Development Lifecycle (SDL) untuk menghasilkan perangkat lunak yang tahan terhadap ancaman keamanan.

3.4. Kualitas dan Keandalan Perangkat Lunak

Kualitas dan keandalan perangkat lunak adalah faktor kunci dalam tanggung jawab profesional dalam ilmu komputer. Perangkat lunak yang berkualitas tinggi dan dapat diandalkan diperlukan untuk memastikan bahwa pengguna memiliki pengalaman yang baik dan untuk menghindari masalah yang dapat merugikan.

Profesional perlu mengikuti praktik-praktik pengembangan perangkat lunak yang baik, seperti penggunaan metodologi yang terstruktur, pemahaman kebutuhan pengguna yang jelas, serta dokumentasi yang akurat. Proses pengembangan yang terstruktur membantu meminimalkan kesalahan dan meningkatkan kualitas perangkat lunak.

Pengujian perangkat lunak adalah tahap penting dalam mengidentifikasi masalah dan cacat sebelum perangkat lunak diperkenalkan kepada pengguna akhir. Pengujian harus mencakup berbagai skenario, termasuk kasus uji ekstensif, fungsionalitas, dan kompatibilitas dengan lingkungan yang berbeda.

Setelah perangkat lunak diluncurkan, perawatan dan pemutakhiran rutin diperlukan untuk memastikan keandalan dan keamanannya. Profesional harus merespons umpan balik dari pengguna dan menerapkan pembaruan yang diperlukan untuk mengatasi masalah atau meningkatkan fitur.

3.5. Pengembangan Berkelanjutan dan Pendidikan Profesional

Pengembangan berkelanjutan dan pendidikan profesional merupakan bagian integral dari tanggung jawab profesional dalam ilmu komputer. Dalam dunia teknologi yang terus berkembang, para profesional harus terus memperbarui pengetahuan dan keterampilan mereka agar tetap relevan dan efektif dalam industri.

Profesional harus aktif mengikuti perkembangan teknologi terbaru. Mereka harus terus membaca artikel, buku, dan sumber daya online tentang tren terkini dalam

ilmu komputer, serta memahami bagaimana teknologi baru dapat diaplikasikan dalam pekerjaan mereka.

Menghadiri seminar, konferensi, dan workshop adalah cara yang baik untuk mendapatkan wawasan baru, berbagi pengalaman dengan profesional lain, dan memperluas jaringan. Ini juga merupakan peluang untuk mendengarkan para pakar dalam industri dan mendapatkan pemahaman mendalam tentang perkembangan terkini. Seminar, konferensi, dan workshop menyediakan platform untuk belajar dari para pakar dan berbagi pengalaman dengan profesional lainnya. Melalui acara-acara ini, para profesional dapat memperluas wawasan mereka, memahami tren terbaru, dan mendapatkan wawasan dalam praktik terbaik.

Sertifikasi dan akreditasi profesional adalah cara untuk mengukur dan mengakui kemampuan dan pengetahuan seorang profesional. Ini dapat mencakup sertifikasi dalam bahasa pemrograman, manajemen proyek, keamanan siber, dan banyak lagi. Sertifikasi ini membantu memvalidasi keahlian dan kompetensi seorang profesional di bidang tertentu. Sertifikasi dan akreditasi profesional adalah bukti bahwa seorang profesional memiliki pengetahuan dan keterampilan yang sesuai dengan standar industri. Ini membantu memvalidasi kemampuan seorang profesional dalam

bidang tertentu dan dapat meningkatkan kredibilitas dalam industri. Sertifikasi juga dapat membuka peluang karier yang lebih baik.

Pendidikan berperan penting dalam mempertahankan dan meningkatkan kualitas profesional. Dengan terus mengembangkan pengetahuan dan keterampilan, seorang profesional dapat mengikuti perkembangan industri dan dapat mengatasi tantangan baru dengan lebih baik. Pendidikan juga membantu profesional untuk beradaptasi dengan perubahan teknologi dan persyaratan industri.

3.6. Komitmen terhadap Pengguna dan Masyarakata

Komitmen terhadap pengguna dan masyarakat adalah salah satu aspek krusial dalam tanggung jawab profesional dalam ilmu komputer. Para profesional memiliki peran penting dalam memastikan bahwa teknologi yang dikembangkan tidak hanya memberikan manfaat bagi individu, tetapi juga untuk masyarakat secara keseluruhan.

Para profesional harus mengenali dan memahami dampak teknologi terhadap masyarakat secara luas. Mereka harus mempertimbangkan konsekuensi sosial, ekonomi, dan budaya dari teknologi yang mereka kembangkan. Ini melibatkan mengantisipasi potensi

dampak negatif dan mencari cara untuk meminimalkannya.

Teknologi dapat digunakan untuk mengatasi tantangan sosial dan lingkungan yang ada di masyarakat. Para profesional harus memiliki kesadaran tentang isu-isu seperti kemiskinan, pendidikan, kesehatan, dan lingkungan, serta berkontribusi dalam mengembangkan solusi teknologi yang dapat memberikan dampak positif. Para profesional harus mendukung pengguna dalam memahami dan menggunakan teknologi dengan bijak. Ini melibatkan menyediakan panduan yang jelas, dukungan teknis yang memadai, serta memastikan antarmuka pengguna yang intuitif dan mudah digunakan.

3.7. Kode Etik dan Standar Profesional dalam Ilmu Komputer

Kode etik dan standar profesional dalam ilmu komputer adalah panduan yang mengatur perilaku dan tanggung jawab para profesional dalam industri teknologi informasi. Kode etik ini membantu menjaga integritas, keamanan, dan kualitas dalam praktik-praktik profesional.

1. Kode Etik ACM (Association for Computing Machinery):

Kode Etik ACM memberikan pedoman bagi para profesional ilmu komputer dalam hal integritas, tanggung jawab, dan perlakuan adil terhadap semua pihak terkait. Kode ini menekankan kepentingan etika dalam pekerjaan dan menghormati nilai-nilai masyarakat.

2. Kode Etik IEEE (Institute of Electrical and Electronics Engineers):

   Kode Etik IEEE menggarisbawahi pentingnya tanggung jawab sosial dan profesional dalam pekerjaan teknik dan ilmu komputer. Kode ini menekankan pada kewajiban menghindari konflik kepentingan, menghormati privasi, dan mempertahankan kualitas teknik yang tinggi.

3. Standar ISO terkait Ilmu Komputer:

   ISO (International Organization for Standardization) memiliki serangkaian standar terkait ilmu komputer yang mencakup berbagai aspek seperti manajemen keamanan informasi (ISO/IEC 27001), manajemen kualitas perangkat lunak (ISO/IEC 9001), serta standar untuk bahasa pemrograman, sistem jaringan, dan lainnya.

BAB IV
PRIVASI DAN KEAMANAN INFORMASI

4.1. Mengapa Keamanan Penting?

Organisasi perusahaan atau pemerintah memiliki banyak informasi di yang sangat penting. Mereka banyak berinvestasi dalam melakukan penelitian di bidang-bidang yang memiliki kepentingan strategis, militer, atau kompetitif. Hilangnya informasi ini kepada pihak ketiga yang memiliki kepentingan yang sama dapat menyebabkan strategi menjadi sia-sia, sehingga menyia-nyiakan seluruh investasi dan upaya bertahun-tahun.

Perlindungan informasi bisnis yang bernilai adalah alasan utama keamanan informasi. Ilmu pengetahuan dan teknologi menyediakan banyak alat dan orang-orang yang dapat digunakan untuk baik untuk tujuan yang baik maupun tujuan yang buruk.

Dengan konseptual dan berprinsip pada keamanan informasi, bisa menganalisis kebutuhan keamanan dalam kerangka yang tepat referensi atau konteks yang tepat sehingga bisa menyeimbangkan kebutuhan untuk mengizinkan akses dengan risiko akses tersebut.

4.2. Privasi dan Keamanan Informasi Saat ini

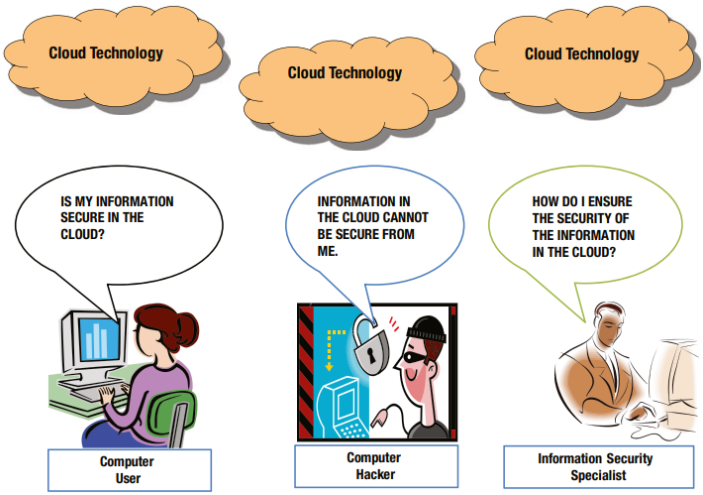
Mari kita jelajahi keamanan informasi dalam konteks saat ini. Keamanan informasi adalah masalah yang menjadi perhatian bagi organisasi dan individu. Peretas modern dilengkapi dengan pengetahuan dan alat teknologi untuk menyusup ke akun individu dan kartu kredit dan debit mereka.

Pencuri dan pihak berwenang selalu berselisih. Paling sering, pencuri memukuli pihak berwenang. Sering kali, polisi mempelajari teknik baru hanya setelah pencuri menggunakannya. Demikian pula, di bidang informasi, selalu ada perlombaan antara peretas dan cracker dan personel keamanan informasi. Dengan meluasnya penggunaan Informasi Teknologi Informasi dan alat-alat terkait, terutama dengan munculnya Internet, telah menjadi tantangan bagi organisasi dan karyawan mereka untuk mencegah penyalahgunaan informasi.

Informasi adalah segala sesuatu yang dikomunikasikan dalam bentuk apa pun, baik publik maupun pribadi. Penyingkapan informasi pribadi kepada orang lain dapat memberikan dampak yang signifikan bagi pihak-pihak yang terlibat, termasuk hilangnya reputasi, keuangan, atau konsekuensi lainnya tergantung pada sifat informasi tersebut. Semua bentuk

teknologi, termasuk Internet, kartu kredit atau kartu debit, ATM, portal web bank, dan sebagainya, semuanya dapat diserang; seringkali secara sengaja, terkadang secara tidak sengaja.

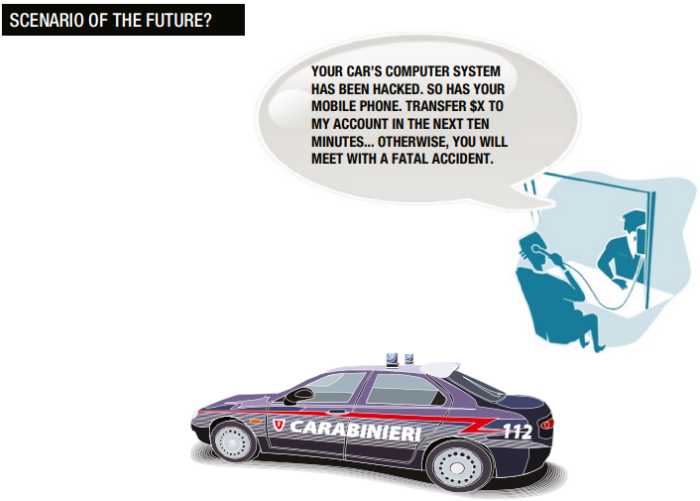
Komputasi awan *(Cloud computing)* adalah kata kunci yang populer saat ini dan memiliki banyak manfaat, tetapi juga menghadirkan banyak risiko baru. Ilustrasi kontekstual dari skenario ini diberikan pada Gambar 4.1.



Gambar 4.1. Ketidakpercayaan pada "Cloud" dan keamanannya

Meningkatnya penggunaan chip elektronik dalam segala hal, mulai dari dari mobil ke lemari es hingga TV adalah penyebab lain yang memprihatinkan. Teori-teori

tentang serangan semacam itu muncul setiap hari. Ini kemungkinan ini diilustrasikan pada Gambar 4.2.



Gambar 4.2. Apakah ini kondisi keamanan di masa depan?

Keamanan informasi merupakan perluasan dari keamanan komputer dan melampaui kontrol fisik hingga kontrol logis, kontrol atas media, dan kontrol atas media komunikasi. Keamanan informasi harus menjadi salah satu yang paling tujuan penting bagi semua orang, termasuk karyawan, kontraktor, pemasok/vendor, dan penyedia layanan lainnya.

Di dunia yang serba cepat ini, di mana informasi adalah aset dan pencapaian tujuan bisnis adalah tanggung jawab semua orang tanggung jawab semua orang, memastikan bahwa risiko keamanan informasi

diminimalkan dengan kontrol yang tepat, telah menjadi prioritas utama. Hal ini juga perlu dilakukan agar manajemen organisasi memahami risiko residual yang ditimbulkan oleh kontrol yang telah mereka terapkan. Metodologi penilaian dan manajemen risiko yang tepat yang tepat dan metodologi penilaian dan manajemen risiko yang tepat adalah salah satu kebutuhan utama kerangka kerja keamanan.

4.3. Ancaman Eksternal dan Internal

Ancaman eksternal berasal dari luar organisasi, terutama dari lingkungan tempat organisasi beroperasi. Ancaman ini dapat berupa ancaman fisik, ancaman sosio-ekonomi yang spesifik untuk suatu negara seperti situasi sosial dan ekonomi negara saat ini, ancaman keamanan jaringan, ancaman komunikasi, ancaman manusia seperti ancaman dari peretas, ancaman perangkat lunak, dan ancaman hukum. Ancaman rekayasa sosial seperti menggunakan situs sosial seperti menggunakan situs rekayasa sosial untuk mengumpulkan data dan menyamar sebagai orang lain dengan tujuan menipu mereka dan mendapatkan kredensial mereka untuk akses yang tidak sah semakin meningkat. Pencurian informasi pribadi yang dapat diidentifikasi, strategi rahasia, dan kekayaan intelektual

dan intelektual organisasi merupakan ancaman penting lainnya.

Beberapa ancaman eksternal yang penting diilustrasikan di bawah ini pada gambar 4.3.

Gambar 4.3 Ancaman eksternal

Ancaman internal berasal dari dalam organisasi. Kontributor utama ancaman internal adalah karyawan, kontraktor, atau pemasok yang pekerjaannya dialihdayakan. Ancaman utama adalah penipuan, penyalahgunaan informasi, dan/atau perusakan informasi.

Beberapa ancaman eksternal dan internal yang penting disusun dalam Tabel 4.1 untuk memudahkan referensi.

Tabel 4.1. Ancaman eksternal dan internal

External Threats	**Internal Threats**
Ancaman Fisik	**Ancaman Manusia**
1. Bencana alam seperti angin topan, 2. angin topan, banjir, gempa bumi, dll. 3. Kebakaran 4. Ancaman teroris seperti bom, situasi penyanderaan 5. Penghancuran perangkat keras 6. Gangguan fisik 7. Sabotase 8. Pencurian aset dan aset/informasi sensitif Kekayaan Intelektual	1. Penipuan, penyalahgunaan aset atau informasi. 2. Kesalahan atau kekeliruan oleh karyawan 3. Rekayasa Sosial oleh karyawan 4. Eksploitasi kurangnya pengetahuan atau ketidaktahuan sesama karyawan 5. Penggunaan kata sandi administrator yang lemah atau kata sandi orang lain dan mendapatkan akses yang tidak sah

Ancaman Jaringan	Masalah Aplikasi Internal
1. Menyadap (Sniffing) 2. Masalah TCP/IP seperti pengintaian, serangan autentikasi, pembajakan koneksi 3. Penipuan (Spoofing) 4. Serangan orang di tengah-tengah 5. Serangan penolakan layanan 6. Injeksi SQL 7. Eksploitasi kata sandi default pada peralatan jaringan yang tidak diubah 8. Eksploitasi enkripsi yang lemah	1. Input yang tidak valid 2. Aplikasi yang salah konfigurasi yang menyebabkan kesalahan atau pemrosesan yang salah 3. Penanganan kesalahan atau pengecualian yang tidak tepat yang menyebabkan masalah 4. Manipulasi parameter; Manipulasi Buffer 5. Akses yang tidak sah
Masalah Perangkat Lunak	**Masalah Lainnya**
1. Cacat yang menyebabkan kesalahan	10. Akses tidak terbatas ke USB yang menyebabkan pencurian informasi

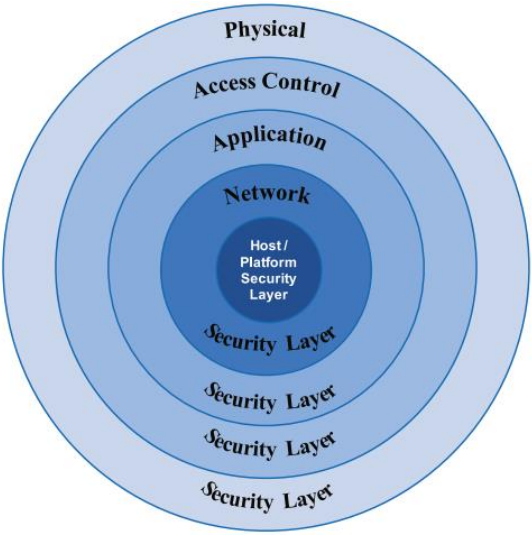
2. Cacat yang dieksploitasi
3. Malware seperti Virus, Worm, Trojan, Pintu belakang
4. Bot atau Botnet
5. Input yang tidak valid
6. Serangan otentikasi
7. Eksploitasi kesalahan konfigurasi
8. Masalah terkait Manajemen Sesi
9. Penanganan kesalahan atau pengecualian yang tidak tepat penanganan oleh aplikasi
11. Kerusakan sistem atau data dapat disebabkan oleh lonjakan daya, kegagalan kontrol suhu, atau karena alasan lain
12. Kegagalan perangkat keras karena tidak berfungsi
13. Infrastruktur seperti kegagalan UPS karena pemeliharaan yang tidak tepat

4.4. Kerangka Kerja Keamanan Informasi dan Arsitektur Keamanan Informasi

Kerangka kerja keamanan informasi memberikan panduan untuk implementasi keamanan informasi yang

efektif dalam organisasi dan pengembangan arsitektur keamanan informasi yang efektif, yang pada gilirannya, memberikan jaminan bahwa keamanan informasi telah diterapkan secara efektif dalam organisasi. Satu kata peringatan di sini: "Apapun apapun tingkat implementasinya, Anda tidak bisa 100% yakin akan keamanan informasi". Namun, jika Anda telah menerapkan keamanan informasi secara efektif, hal ini akan memungkinkan Anda untuk mengendalikan banyak ancaman keamanan dan mempersiapkan Anda untuk cepat cepat dalam memberikan tanggapan reaktif terhadap ancaman. Organisasi hanya bisa bersikap defensif dalam pendekatan mereka karena strategi ofensif strategi ofensif adalah ilegal. Kerangka kerja atau arsitektur seperti itu memungkinkan Anda untuk mencegah atau mendeteksi dan bereaksi terhadap serangan atau pulih dari serangan.

Untuk melindungi informasi dan data dari ancaman di atas, organisasi biasanya memiliki "lapisan perlindungan." Praktik pertahanan berlapis ini meningkatkan postur keamanan organisasi secara keseluruhan. Organisasi yang berhasil organisasi yang sukses memiliki lapisan keamanan, seperti yang ditunjukkan pada Gambar 4.3.



Gambar 4.3. Pendekatan berlapis untuk keamanan

Seperti yang terdapat pada gambar 4.3. kelima lapisan keamanan ini saling mendukung dan melengkapi satu sama lain. Sementara Lapisan Akses atau Lapisan Pengguna memastikan autentikasi dan otorisasi yang jelas, izin keamanan melalui kontrol yang sesuai, Lapisan keamanan Aplikasi memastikan kontrol yang efektif atas server web, database, dan aplikasi melalui berbagai kontrol seperti enkripsi dan manajemen identitas. Lapisan keamanan Jaringan memberikan perlindungan melalui kontrol seperti firewall, IDS/IPS, sedangkan lapisan keamanan Platform/Host memastikan kontrol seperti Host IDS/IPS, dan anti-virus perangkat lunak,

sedangkan lapisan keamanan Fisik memastikan kontrol seperti akses yang aman, kontrol aset, dan proteksi kebakaran.

Keamanan Platform/Host dipastikan terutama melalui pengerasan server. Root / administrator diubah dari kata sandi default menjadi kata sandi yang kuat dan dikontrol dengan ketat. Selain itu, solusi solusi anti-virus bereputasi baik saat dipasang di server memberikan perlindungan yang signifikan bagi mereka dari malware atau infeksi spyware. Patch keamanan dirilis oleh sebagian besar vendor sistem operasi secara berkala. Tepat waktu aplikasi ini ke server yang bersangkutan setelah menguji dampaknya pada aplikasi yang bekerja seperti itu platform/host memastikan bahwa server ini terlindungi dengan baik. Demikian pula, driver perlu dipelihara dan diperbarui sebagai dibutuhkan. Pemeliharaan preventif berkala dari host-host ini untuk membersihkan ruang, menghapus file yang tidak diinginkan, mengarsipkan data, mendefrag disk, memastikan pembaruan patch terbaru dan relevan, dan peningkatan perangkat lunak atau driver, akan memastikan kinerja yang berkelanjutan. Jika tidak, mungkin akan terjadi penurunan kinerja yang berdampak pada ketersediaan dan peningkatan ancaman keamanan. Demikian pula, pemeliharaan

fasilitas dan utilitas, seperti kontrol suhu di server server/pusat data, kontrol kelembaban di ruang server/pusat data, dan pemeliharaan preventif UPS, akan membantu memastikan sistem yang aman. Kata sandi administrator yang lemah juga bisa membuat server berisiko.

Keamanan jaringan adalah lapisan pelindung berikutnya yang menghubungkan host/platform dengan yang lainnya. Beberapa aspek yang perlu dipastikan di sini adalah bahwa peralatan jaringan dikeraskan, kata sandi default selalu diganti dengan kata sandi yang lebih kuat, semua peralatan jaringan seperti router dikonfigurasi dengan benar dan protokol digunakan dengan tepat tergantung pada infrastruktur dan kebutuhan organisasi. Firewall dan IDS/IPS perlu diatur dengan tepat dengan konfigurasi dan kebijakan yang relevan sehingga mereka dapat mendeteksi, memperingatkan, atau mencegah beberapa serangan. Kata sandi administrator yang lemah, enkripsi yang lemah atau tidak terlindungi kunci, atau kesalahan konfigurasi dapat dieksploitasi dan dapat menempatkan organisasi dan bisnisnya dalam risiko.

Keamanan aplikasi adalah masalah utama di seluruh dunia. Server web dan basis data perlu diamankan dengan cara yang tepat instalasi dan

konfigurasi yang tepat. Di dunia yang serba cepat ini, fokus pada penyelesaian pengembangan perangkat lunak dan pengirimannya menjadi lebih penting daripada keamanannya. Anehnya, sebagian besar aplikasi ini tidak diuji untuk keamanan. Aplikasi-aplikasi ini dapat rentan terhadap serangan seperti injeksi SQL, buffer overflow, dan input data yang tidak valid yang pada akhirnya dapat menyebabkan kompromi pada sistem host tempat aplikasi tersebut berjalan. Demikian pula, aplikasi yang tidak efektif aplikasi yang tidak diuji atau salah konfigurasi dapat menyebabkan kesalahan pemrosesan atau tidak memvalidasi kesalahan, yang mengarah ke hilangnya integritas data. Mekanisme otentikasi dan otorisasi yang lemah yang ada di dalam aplikasi ini atau kesalahan konfigurasi dari aplikasi ini dapat menyebabkan akses yang tidak sah atau masalah lain seperti korupsi data dan dan sejenisnya. Cacat pada aplikasi tidak hanya dapat menyebabkan kesalahan pada data tetapi cacat yang terkait dengan keamanan dapat menyebabkan pelanggaran keamanan. pelanggaran. Aplikasi yang tidak ditambal tepat waktu mungkin rentan terhadap virus atau eksploitasi kelemahan keamanan tersebut atau kesalahan. Mungkin juga antarmuka antara dua aplikasi lemah, yang menyebabkan transfer data yang tidak aman data antara

aplikasi-aplikasi ini, dan pemaparan data ini kepada orang lain.

Akses ke sistem diatur oleh lapisan **kontrol akses**. Lapisan kontrol akses harus diatur sesuai dengan kebijakan kontrol akses organisasi. Beberapa model kontrol akses yang menarik adalah kontrol akses wajib, kontrol akses diskresioner, dan model kontrol akses non-diskresioner. Beberapa administrasi kontrol akses model administrasi adalah model administrasi terpusat, model administrasi terdesentralisasi, dan administrasi hibrida model administrasi hibrida. Baik kontrol akses internal maupun eksternal dan eksternal perlu ditangani dengan tepat. Otentikasi dan otorisasi harus diatur dengan tepat. Ancaman utama karena lapisan akses yang tidak dikonfigurasi dengan benar adalah akses yang tidak sah atau memiliki akses yang salah atau penolakan akses yang sesuai. Seiring waktu, telah diamati bahwa satu mekanisme otentikasi tunggal relatif mudah dibobol, sehingga beberapa otentikasi lebih disukai untuk keamanan maksimum.

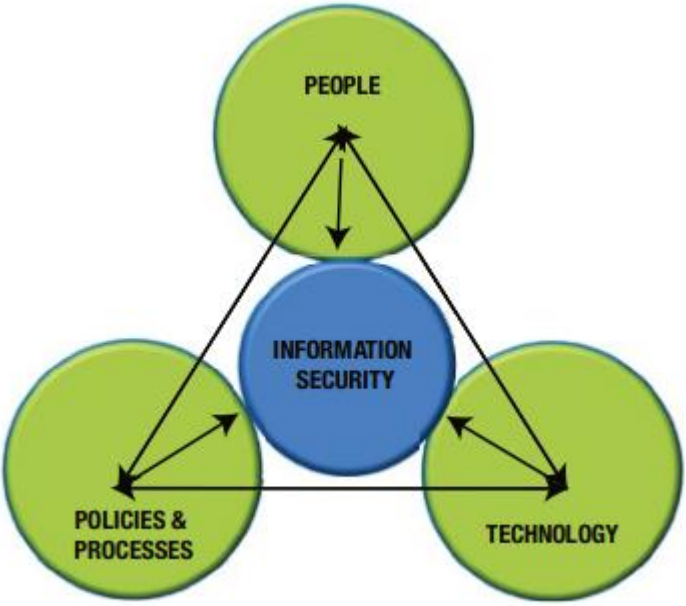
Lapisan penting lainnya adalah lapisan **keamanan fisik**. Secara tradisional, penjaga keamanan dan kunci adalah yang utama sarana keamanan fisik. Karena adanya unsur manusia yang terlibat di mana kelalaian atau ketidaktahuan dapat menyebabkan ancaman

keamanan ancaman, kontrol keamanan pelengkap seperti akses biometrik (sidik jari, pemindaian iris mata, dll.), akses melalui kartu pintar kartu pintar yang digabungkan dengan kode sandi, dan sejenisnya, diimplementasikan. Pemilihan lokasi yang sesuai untuk organisasi melindunginya dari potensi bahaya alam seperti banjir. Mengamankan kabel listrik dengan pengaman yang sesuai mekanisme seperti lubang arde yang terpelihara dengan baik, UPS untuk daya yang diatur, tripper, dan sekering memberikan keamanan dari kebakaran listrik. Praktik yang baik seperti tidak menyimpan bahan yang mudah terbakar seperti solar, bensin, bahan kimia lainnya di tempat, dan tidak menyimpan bahan yang mudah terbakar seperti karton kosong atau kertas bekas dalam jumlah besar mengurangi mengurangi ancaman kebakaran. Mekanisme kontrol pengunjung yang tepat dan kontrol atas titik masuk dan keluar dapat mengurangi kecenderungan untuk gangguan fisik atau akses fisik yang tidak sah atau sabotase, vandalisme, spionase, pencurian, dan perusakan sistem. Kebijakan yang tidak diikuti oleh karyawan dapat memungkinkan ancaman seperti itu karena tailgating yang merupakan masalah yang sangat umum di sebagian besar organisasi. yang sangat umum di sebagian besar organisasi.

Ketidaktahuan dan ketidakmampuan, serta kurangnya kesadaran dan pelatihan dapat menyebabkan kesalahan.

4.5. Pilar Keamanan

Keamanan adalah proses yang berkelanjutan. Proses ini melibatkan orang, kebijakan, prosedur, proses, dan teknologi. Ketiganya kategori ini dapat dianggap sebagai pilar keamanan informasi. Pilar-pilar keamanan ini dan interkoneksinya digambarkan dalam Gambar 4.5.



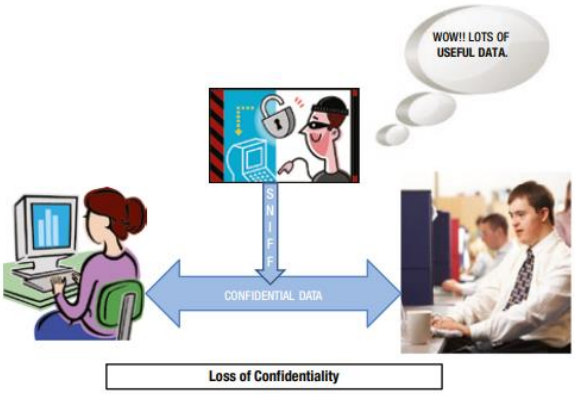
Gambar 4.5 Tiga serangkai Manusia, Proses, dan Teknologi untuk keamanan informasi

Seperti yang telah kita lihat di paragraf sebelumnya, orang adalah bagian penting dan tak terlupakan dari keamanan informasi. Keamanan informasi yang efektif melibatkan penugasan peran dan tanggung jawab yang jelas bagi orang-orang di setiap organisasi.

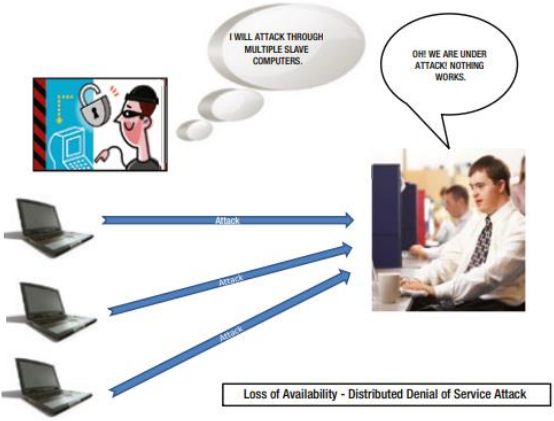
Manusia adalah pilar terkuat dari terkuat dari keamanan informasi di satu sisi. Namun, mereka terkadang cenderung menjadi pilar terlemah karena kurangnya kesadaran atau motif yang buruk. Mereka mudah rentan terhadap serangan rekayasa sosial atau serangan berbahaya lainnya. Oleh karena itu, untuk keamanan informasi yang kuat, kesadaran, kewaspadaan, dan keterlibatan positif mereka harus ditingkatkan dan dipastikan.

4.6. Konsep Keamanan Informasi

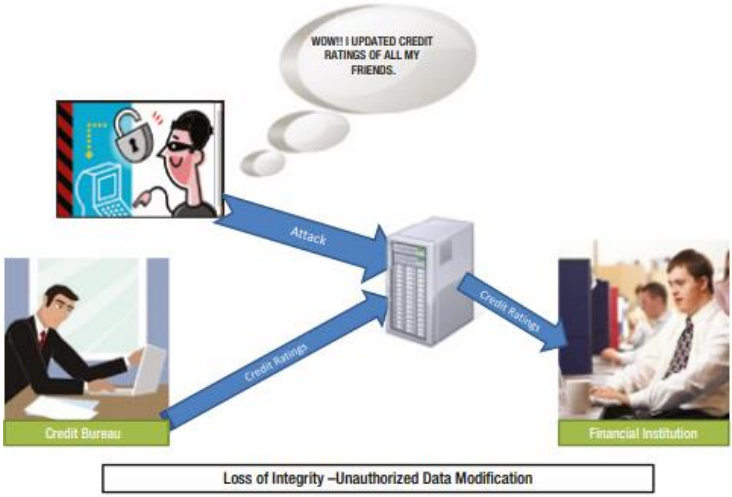
Kompromi keamanan informasi adalah salah satu masalah terbesar yang dihadapi oleh industri TI dan industri yang mendukung TI, yang hampir setiap industri saat ini. Beberapa skenario dari kemungkinan kompromi keamanan informasi digambarkan pada Gambar 4.6.



Loss of Confidentiality



Loss of Availability - Distributed Denial of Service Attack



Gambar 4.6. Kompromi keamanan informasi

4.7. Penerapan Keamanan Informasi

Tidaklah mudah untuk menerapkan keamanan informasi. Semua pilar keamanan informasi harus diberikan perhatian yang yang memadai. Pelingkupan yang tepat harus dilakukan untuk upaya tersebut dan perencanaan yang tepat harus dilakukan dengan melibatkan semua pemangku kepentingan. Perencanaan harus didukung oleh eksekusi yang kuat dari hal yang sama dan mengatasi hambatan saat eksekusi dilakukan. yang kuat dan mengatasi hambatan saat eksekusi dilakukan. Fokus untuk memastikan keberhasilan implementasi diperlukan dengan semua orang yang

relevan ditugaskan dan yang relevan ditugaskan dan dilibatkan secara tepat.

Gambar 4.9. menunjukkan siklus implementasi keamanan informasi yang umum. Tergantung pada konteks organisasi organisasi, mungkin ada beberapa model yang berbeda yang digunakan untuk implementasi.

Gambar 4.9 Siklus penerapan keamanan informasi

Pendekatan yang efektif untuk penerapan keamanan informasi adalah kunci keberhasilannya. Organisasi pada tahap yang berbeda dalam

keberadaannya mungkin melakukan pendekatan implementasi dengan cara yang berbeda. Sebuah organisasi yang sudah yang sudah ada biasanya mendorong perjalanannya menuju keamanan informasi terutama melalui inisiasi penilaian risiko penilaian risiko. Oleh karena itu, berbagai standar dan kerangka kerja menyoroti aspek penilaian risiko sebagai langkah penting penting dalam konteks keseluruhan penerapan keamanan informasi.

1. *Risk Assessment*

   Pemahaman tentang risiko dalam konteks konteks seluruh organisasi, dengan memperhatikan kerentanan dan ancaman terhadap aset informasi bahkan dari dunia luar, memahami kontrol saat ini yang ada dan kuantifikasi risiko untuk memahami eksposur risiko biasanya mendorong respons risiko termasuk mitigasi risiko yang akan dilakukan. Mitigasi risiko adalah ditentukan berdasarkan pengendalian efektif yang telah diterapkan oleh organisasi lain, yang disarankan oleh lembaga lain, dengan penerapan perangkat, melalui kebijakan dan proses, melalui kontrol tambahan lainnya yang diperlukan termasuk kesadaran dan pelatihan karyawan, kontraktor dan

pemasok, atau melalui pencegahan seperti perjanjian hukum. Karyawan biasanya juga termasuk pekerja sementara.

2. *Planning and Architecture*

   Dalam organisasi yang sudah ada, perencanaan dapat dimulai dengan dimulainya yang efektif yang melibatkan semua pemangku kepentingan yang relevan. Dalam organisasi baru, perencanaan dapat dilakukan untuk secara efektif mendekati pencapaian keamanan informasi dengan menggunakan langkah-langkah yang relevan seperti yang disarankan oleh kerangka kerja atau metodologi yang sesuai. Rencana juga mengidentifikasi pemilik untuk berbagai kegiatan, peran, dan tanggung jawab untuk pelaksanaan yang efektif dari rencana-rencana ini. Langkah-langkah yang direncanakan tergantung pada metodologi atau kerangka kerja yang digunakan. Perencanaan perlu harus dilakukan dengan pendekatan yang terintegrasi, metodis, dan terkoordinasi dengan baik, sehingga menghasilkan informasi yang efektif.

3. Gap Analysis

   Banyak hal berubah: bisnis dapat berubah, teknologi berubah, orang-orang berubah.

Perubahan adalah satu-satunya hal yang konstan di dunia saat ini. Selain itu, kerentanan yang sampai saat ini tidak diketahui akan terekspos ke dunia atau dilaporkan. Untuk memastikan hal ini, analisis kesenjangan secara berkala perlu dilakukan yang terkadang memunculkan kejutan yang signifikan. Hal ini untuk memastikan pemeriksaan pada implementasi kebijakan, prosedur, dan proses, serta efektivitas perlindungan yang ada atau kontrol yang ada termasuk efektivitas arsitektur keamanan informasi.

4. *Integration and Deployment*

   Setiap implementasi yang dilakukan secara terpisah-pisah dan bukan di seluruh organisasi tidak memberikan perlindungan yang memadai perlindungan yang memadai. Oleh karena itu, sebuah pandangan yang terintegrasi setiap saat dalam totalitas bisnis dan organisasi diperlukan. Selain itu, sebuah penyebaran semua kebijakan, prosedur, dan proses yang dimaksudkan, bersama dengan implementasi yang dimaksudkan arsitektur keamanan informasi dan berbagai lapisannya diperlukan.

5. *Operations*

Operasi harus dilakukan secara ketat sesuai dengan kebijakan, prosedur, dan proses yang telah ditetapkan. Setiap pelanggaran untuk mempercepat kegiatan atau ketidaktahuan dapat menyebabkan konsekuensi yang serius. Demikian pula, tidak melakukan kegiatan tertentu tertentu yang penting sesuai dengan kebijakan dan prosedur, dapat menggagalkan tujuan keamanan informasi.

6. *Monitoring*

   Pemantauan merupakan bagian integral dari aktivitas apa pun, baik yang berhubungan dengan bisnis maupun aktivitas yang berhubungan dengan keamanan informasi. Setiap organisasi perlu terus memantau ancaman terhadapnya sehingga dapat bereaksi terhadap ancaman secara efektif dan tepat waktu. Aktivitas ini memakan waktu. Sebagai contoh, untuk mengetahui semua aktivitas penyusup secara manual melalui log adalah aktivitas yang sangat besar.

7. *Legal Compliance and Audit*

   Salah satu ancaman terbesar bagi eksistensi organisasi adalah ketidakpatuhan terhadap persyaratan hukum. Organisasi dapat ditutup

secara permanen jika ketidakpatuhannya parah. Terkadang, organisasi dapat dikenakan denda yang sangat besar karena ketidakpatuhan atau kelalaian. Selain itu, ada banyak undang-undang yang diberlakukan untuk mencegah penyalahgunaan teknologi informasi dan harus dipatuhi. Hal ini mungkin memerlukan keahlian khusus untuk memahami kepatuhan dalam konteks teknologi informasi. Oleh karena itu, audit berkala oleh ahli independen atau internal yang berpengetahuan luas akan membantu organisasi untuk memahami masalah ketidakpatuhan dan menanggulanginya sebelum menjadi parah. menjadi parah.

8. *Crisis Management*

   Rencana Manajemen Krisis, Rencana Kesinambungan Bisnis, atau Rencana Pemulihan Bencana digunakan secara bergantian untuk menunjukkan satu entitas, meskipun ada perbedaan halus di antara mereka. Untuk tujuan diskusi di sini, mari kita pertimbangkan mereka sebagai satu kesatuan. Organisasi dapat menghadapi krisis karena bencana alam, kesalahan karyawan, manajemen senior, atau manajemen, atau karena serangan eksternal

seperti serangan dari peretas. Organisasi tidak bisa berdiam diri. Mereka harus merespons secara efektif dan juga mengembalikan bisnis mereka kembali ke keadaan normal setelah serangan tersebut.

BAB V
ETIKA DALAM PENGEMBANGAN PERANGKAT LUNAK

5.1. Pengertian Etika dalam Konteks Perangkat Lunak

Etika dalam konteks pengembangan perangkat lunak merujuk pada seperangkat prinsip, nilai, norma, dan panduan moral yang mengarahkan tindakan dan keputusan para pengembang perangkat lunak. Tujuannya adalah untuk memastikan bahwa perangkat lunak yang dikembangkan tidak hanya efektif dan efisien dalam fungsinya, tetapi juga menghormati nilai-nilai dan hak-hak individu, masyarakat, dan lingkungan.

Berikut adalah beberapa komponen utama pengertian etika dalam pengembangan perangkat lunak:

1. Transparansi dan Keterbukaan: Pengembang perangkat lunak harus memastikan bahwa pengguna memiliki pemahaman yang jelas tentang bagaimana perangkat lunak tersebut beroperasi, bagaimana data pengguna diolah, dan dampak apa yang mungkin timbul dari penggunaannya.

2. Privasi dan Perlindungan Data Pengguna: Etika dalam pengembangan perangkat lunak menuntut perlindungan data pribadi pengguna. Pengembang harus merancang sistem yang memastikan data sensitif diamankan dan hanya digunakan sesuai dengan persetujuan pengguna.
3. Keamanan Cyber dan Perlindungan Terhadap Ancaman: Perangkat lunak harus dirancang dengan mempertimbangkan faktor keamanan. Pengembang harus mengidentifikasi potensi risiko keamanan dan melindungi perangkat lunak dari ancaman siber, seperti peretasan atau serangan malware.
4. Keadilan dalam Algoritma dan Keputusan Otomatis: Dalam sistem yang menggunakan kecerdasan buatan (AI) atau algoritma untuk mengambil keputusan, etika memerlukan adanya keadilan dan penghindaran bias yang dapat mengakibatkan diskriminasi.
5. Tanggung Jawab Sosial dan Dampak Lingkungan: Pengembang perangkat lunak harus mempertimbangkan dampak sosial dan lingkungan dari produk yang mereka hasilkan. Ini mencakup aspek seperti penggunaan sumber

daya, dampak karbon, dan dampak sosial yang lebih luas.

6. Penghormatan Hak Kekayaan Intelektual: Etika memerlukan pengembang untuk menghormati hak kekayaan intelektual orang lain, termasuk penggunaan kode sumber terbuka (open source) dan hak cipta.
7. Keterlibatan Pengguna dan Partisipasi Masyarakat: Etika juga mendorong pengembang untuk melibatkan pengguna dan masyarakat dalam proses pengembangan, mendengarkan masukan, dan memperbaiki produk berdasarkan umpan balik.
8. Kepatuhan terhadap Regulasi dan Standar: Pengembang perangkat lunak harus mematuhi regulasi hukum dan standar industri yang berkaitan dengan etika dan keamanan perangkat lunak.
9. Pendekatan Jangka Panjang: Etika dalam pengembangan perangkat lunak juga mempertimbangkan dampak jangka panjang dari produk tersebut, bukan hanya keuntungan jangka pendek.

Secara keseluruhan, etika dalam pengembangan perangkat lunak melibatkan pertimbangan yang mendalam terhadap implikasi moral dan sosial dari produk yang dibuat, dengan tujuan menghasilkan perangkat lunak yang tidak hanya bermanfaat secara fungsional, tetapi juga sesuai dengan nilai-nilai kemanusiaan dan keadilan.

5.2. Proses Pengembangan Perangkat Lunak yang Mengedepankan Etika

Proses pengembangan perangkat lunak yang mengedepankan etika melibatkan langkah-langkah khusus yang dirancang untuk memastikan bahwa nilai-nilai etika diintegrasikan secara mendalam dalam seluruh tahapan pengembangan. Berikut adalah contoh proses yang dapat diikuti:

1. Analisis Kebutuhan dengan Perspektif Etika:
    - Identifikasi dampak potensial terhadap pengguna, masyarakat, dan lingkungan.
    - Pertimbangkan implikasi etika dari fitur-fitur yang diusulkan.
    - Libatkan pemangku kepentingan untuk mendapatkan pandangan tentang masalah etika yang relevan.
2. Perancangan Etika dan Fitur Keamanan:

- Rancang fitur-fitur keamanan, privasi, dan transparansi sebagai bagian integral dari desain produk.
- Gunakan desain privasi by design, di mana perlindungan data dan privasi sudah tertanam dalam desain produk.
- Pastikan transparansi dalam bagaimana data pengguna diolah dan dimanfaatkan.

3. Implementasi dengan Prinsip Etika:
    - Pilih alat dan teknologi yang memungkinkan pengembangan perangkat lunak dengan keamanan tinggi.
    - Ikuti praktik pengkodean yang aman dan hindari celah keamanan yang dapat dieksploitasi.
    - Pertimbangkan konsekuensi dari setiap keputusan teknis terhadap etika.
4. Uji Keamanan dan Pengujian Etika:
    - Lakukan pengujian keamanan dan penetesan untuk mengidentifikasi potensi masalah keamanan dan privasi.
    - Uji fitur-fitur yang berkaitan dengan etika, seperti penggunaan data pengguna atau pengambilan keputusan otomatis, untuk memastikan integritas dan akurasi.

5. Pemantauan Kehandalan dan Keamanan:
    - Tetap pantau dan evaluasi kinerja keamanan serta etika produk setelah diluncurkan.
    - Tangani masalah yang mungkin muncul seiring waktu dan pertahankan komitmen terhadap nilai-nilai etika.
6. Libatkan Pengguna dan Masyarakat:
    - Ajak pengguna dan masyarakat umum untuk memberikan masukan terkait etika dan dampak produk.
    - Gunakan umpan balik untuk perbaikan produk dan pengambilan keputusan.
7. Pemeliharaan Berkelanjutan:
    - Terus perbarui dan perbaiki produk dalam hal etika, keamanan, dan privasi.
    - Tetap mengikuti perkembangan regulasi dan standar etika terbaru.
8. Pelatihan Etika Bagi Tim Pengembang:
    - Memberikan pelatihan secara rutin kepada tim pengembang tentang prinsip-prinsip etika dalam pengembangan perangkat lunak.
    - Berbagi contoh kasus etika yang relevan untuk mempromosikan pemahaman yang lebih baik.
9. Pengawasan dan Penilaian Independen:

Melibatkan pihak ketiga independen untuk melakukan penilaian etika dan keamanan produk secara objektif.

10. Evaluasi Dampak Lingkungan dan Sosial:
    - Pertimbangkan dampak produk terhadap lingkungan dan masyarakat.
    - Cari cara untuk mengurangi dampak negatif dan meningkatkan dampak positif.

Mengintegrasikan etika dalam seluruh tahap pengembangan perangkat lunak bukan hanya tentang mematuhi aturan, tetapi juga tentang menghormati nilai-nilai moral yang mendasari tindakan kita sebagai pengembang. Proses ini berfokus pada menciptakan perangkat lunak yang bermanfaat, aman, dan sesuai dengan harapan masyarakat serta norma etika yang berlaku.

5.3. Keterlibatan Pengguna dan Partisipasi Masyarakat

Keterlibatan pengguna dan partisipasi masyarakat adalah konsep yang merujuk pada melibatkan individu atau kelompok dalam proses pengambilan keputusan, perencanaan, implementasi, dan evaluasi berbagai inisiatif atau program yang dapat mempengaruhi

mereka. Tujuan dari keterlibatan pengguna dan partisipasi masyarakat adalah untuk memastikan bahwa perspektif dan kebutuhan mereka diakomodasi, sehingga menghasilkan keputusan dan solusi yang lebih baik, lebih akurat, dan lebih relevan.

Ada beberapa alasan mengapa keterlibatan pengguna dan partisipasi masyarakat penting:

1. Meningkatkan Akurasi dan Efektivitas: Melibatkan pengguna akhir dan masyarakat dalam proses pengambilan keputusan memungkinkan pemahaman yang lebih baik tentang kebutuhan, masalah, dan tantangan yang dihadapi. Hal ini dapat mengarah pada solusi yang lebih akurat dan efektif.
2. Peningkatan Legitimitas dan Penerimaan: Partisipasi masyarakat dapat meningkatkan tingkat dukungan dan penerimaan terhadap kebijakan atau proyek tertentu. Ketika masyarakat merasa terlibat dalam pembuatan keputusan, mereka cenderung lebih menerima dan mendukung hasilnya.
3. Inovasi dan Kreativitas: Dengan mengundang pandangan dan ide dari berbagai kelompok masyarakat, peluang untuk inovasi dan solusi kreatif dapat meningkat. Keterlibatan pengguna

dapat membuka potensi ide-ide baru yang tidak terpikirkan sebelumnya.

4. Pemberdayaan Masyarakat: Keterlibatan aktif dalam proses pengambilan keputusan dapat meningkatkan rasa memiliki dan pemberdayaan masyarakat. Ini dapat meningkatkan kepercayaan diri dan kemampuan masyarakat untuk mengatasi masalah mereka sendiri.
5. Transparansi dan Akuntabilitas: Dengan melibatkan masyarakat, transparansi dalam proses pengambilan keputusan dapat ditingkatkan. Ini dapat membantu mengurangi potensi kecurangan atau ketidakadilan.
6. Pengurangan Konflik: Dengan memasukkan berbagai pandangan dan kepentingan, potensi konflik dapat berkurang karena berbagai kelompok telah diberi kesempatan untuk berbicara dan berkontribusi.
7. Peningkatan Hasil Jangka Panjang: Keterlibatan pengguna dan partisipasi masyarakat tidak hanya berkaitan dengan hasil jangka pendek, tetapi juga memungkinkan untuk merencanakan dan mengimplementasikan solusi yang lebih berkelanjutan dan berdampak jangka panjang.

Untuk mengimplementasikan keterlibatan pengguna dan partisipasi masyarakat, beberapa langkah yang dapat diambil meliputi:

- Pemahaman Konteks: Memahami konteks sosial, budaya, dan ekonomi dari masyarakat yang terlibat.
- Komunikasi Efektif: Mengkomunikasikan tujuan, manfaat, dan proses keterlibatan dengan jelas kepada masyarakat.
- Pemilihan Metode: Memilih metode yang sesuai untuk melibatkan masyarakat, seperti pertemuan umum, kelompok fokus, survei, atau platform daring.
- Diversifikasi Peserta: Mengundang peserta dari berbagai lapisan masyarakat untuk memastikan representasi yang luas.
- Keterbukaan dan Penghargaan: Mendorong keterbukaan dalam diskusi dan menghargai kontribusi setiap individu.
- Integrasi Masukan: Memastikan bahwa masukan dan pandangan masyarakat benar-benar diintegrasikan dalam proses pengambilan keputusan.
- Umpan Balik dan Evaluasi: Memberikan umpan balik tentang bagaimana masukan masyarakat

telah berdampak pada keputusan atau proyek, dan terus memperbaiki proses keterlibatan.

- Kontinuitas: Menjaga keterlibatan masyarakat dari tahap perencanaan hingga implementasi dan evaluasi.
- Edukasi: Memastikan bahwa masyarakat memiliki pemahaman yang cukup tentang isu-isu yang dibahas sehingga mereka dapat berpartisipasi dengan efektif.
- Sumber Daya: Memastikan ada sumber daya yang cukup untuk mendukung keterlibatan masyarakat, seperti waktu, dana, dan teknologi.

Keterlibatan pengguna dan partisipasi masyarakat adalah pendekatan yang berharga untuk menghasilkan solusi yang lebih holistik dan berkelanjutan dalam berbagai bidang, termasuk pembangunan sosial, proyek infrastruktur, kebijakan publik, dan inisiatif lingkungan.

5.4. Regulasi dan Standar Etika dalam Pengembangan Perangkat Lunak

Regulasi dan standar etika dalam pengembangan perangkat lunak sangat penting untuk memastikan bahwa produk perangkat lunak yang dihasilkan aman, andal, dan sesuai dengan nilai-nilai etika yang diakui

secara luas. Ini membantu melindungi pengguna, mengurangi risiko pelanggaran privasi, dan memastikan bahwa perangkat lunak berkontribusi pada masyarakat secara positif. Berikut adalah beberapa contoh regulasi dan standar etika dalam pengembangan perangkat lunak:

1. General Data Protection Regulation (GDPR): GDPR adalah regulasi Uni Eropa yang mengatur perlindungan data pribadi warga Uni Eropa. Perangkat lunak yang mengumpulkan dan mengelola data pribadi harus mematuhi persyaratan GDPR, termasuk persetujuan pengguna, hak untuk mengakses data, dan tanggung jawab pengolahan data.
2. Health Insurance Portability and Accountability Act (HIPAA): HIPAA adalah undang-undang di Amerika Serikat yang mengatur perlindungan informasi kesehatan pasien. Perangkat lunak yang digunakan dalam industri kesehatan harus mematuhi standar keamanan dan privasi yang ditetapkan oleh HIPAA.
3. Ethical Guidelines for AI: Beberapa organisasi dan lembaga telah menerbitkan pedoman etika untuk pengembangan kecerdasan buatan (AI) dan teknologi terkait. Misalnya, "The IEEE Global

Initiative on Ethics of Autonomous and Intelligent Systems" dan "The Asilomar AI Principles" adalah contoh pedoman etika untuk pengembangan AI yang bertanggung jawab.

4. Software Engineering Code of Ethics and Professional Practice: Institute of Electrical and Electronics Engineers (IEEE) telah mengembangkan Kode Etika dan Praktik Profesional Rekayasa Perangkat Lunak. Kode ini memberikan panduan etika bagi para insinyur perangkat lunak dalam mengembangkan produk mereka.
5. ISO 27001: ISO 27001 adalah standar internasional untuk manajemen keamanan informasi. Ini memberikan kerangka kerja untuk melindungi informasi sensitif, termasuk data yang dikelola oleh perangkat lunak.
6. UN Guiding Principles on Business and Human Rights: Prinsip-prinsip ini menekankan tanggung jawab perusahaan untuk menghormati hak asasi manusia dalam semua operasi mereka, termasuk dalam pengembangan perangkat lunak.
7. Open Source Initiative (OSI) Definition: Bagi perangkat lunak sumber terbuka, OSI

menyediakan definisi dan kriteria yang harus dipenuhi agar dapat dianggap sebagai perangkat lunak sumber terbuka. Ini termasuk akses terbuka ke kode sumber, hak untuk memodifikasi, dan larangan terhadap diskriminasi.

8. Net Neutrality: Meskipun bukan regulasi langsung terhadap perangkat lunak, prinsip netralitas jaringan penting untuk memastikan akses yang setara dan tidak diskriminatif terhadap aplikasi dan layanan perangkat lunak.
9. Accessibility Standards: Berbagai regulasi dan standar, seperti Web Content Accessibility Guidelines (WCAG), mengatur bahwa perangkat lunak harus dapat diakses dengan mudah oleh semua individu, termasuk mereka dengan keterbatasan fisik atau kognitif.
10. International Standards Organization (ISO) untuk Kualitas Perangkat Lunak: Serangkaian standar ISO terkait dengan kualitas perangkat lunak, termasuk ISO/IEC 25010 tentang kualitas produk perangkat lunak dan ISO/IEC 25000 tentang standar kualitas perangkat lunak.

Mengikuti regulasi dan standar etika dalam pengembangan perangkat lunak membantu menciptakan produk yang lebih aman, lebih andal, dan lebih sesuai dengan nilai-nilai sosial yang diinginkan oleh masyarakat. Selain itu, ini juga membantu menghindari potensi dampak negatif terhadap privasi, keamanan, dan hak asasi manusia.

5.5. Pelatihan Etika dalam Pengembangan Perangkat Lunak

Pelatihan etika dalam pengembangan perangkat lunak adalah suatu program pelatihan yang bertujuan untuk meningkatkan pemahaman dan kesadaran para pengembang perangkat lunak tentang masalah etika yang terkait dengan pekerjaan mereka. Dalam era digital dan teknologi informasi saat ini, pengembang perangkat lunak memiliki peran penting dalam membentuk produk dan layanan yang dapat memiliki dampak besar pada masyarakat dan lingkungan.

Berikut adalah beberapa poin penting yang dapat dicakup dalam pelatihan etika dalam pengembangan perangkat lunak:

1. Pemahaman tentang Etika Komputer dan Teknologi: Pengembang perangkat lunak perlu memahami dasar-dasar etika komputer dan

teknologi, termasuk prinsip-prinsip yang berkaitan dengan privasi, keamanan, integritas data, dan kebebasan berbicara.

2. Dampak Sosial dan Lingkungan: Pelatihan harus membahas tentang bagaimana perangkat lunak dan teknologi yang dikembangkan dapat memiliki dampak sosial, ekonomi, dan lingkungan. Ini melibatkan pertimbangan tentang bagaimana teknologi dapat mempengaruhi pekerjaan, masyarakat, dan planet kita.
3. Keanekaragaman dan Inklusi: Etika dalam pengembangan perangkat lunak juga mencakup keanekaragaman dan inklusi dalam produk dan layanan yang dibuat. Pelatihan dapat membahas mengenai pentingnya mempertimbangkan kebutuhan dan perspektif semua pengguna, termasuk mereka yang berasal dari latar belakang berbeda.
4. Keamanan Data dan Privasi: Pengembang perangkat lunak perlu memahami pentingnya melindungi data pengguna dan menjaga privasi. Pelatihan dapat mencakup praktik terbaik dalam mengelola, menyimpan, dan mengamankan data pengguna.

5. Pengembangan Berkelanjutan dan Ramah Lingkungan: Etika juga melibatkan pertimbangan terhadap dampak lingkungan dari teknologi yang dikembangkan. Pelatihan dapat mengajarkan tentang bagaimana membuat perangkat lunak yang lebih efisien secara energi dan berkelanjutan.
6. Transparansi dan Tanggung Jawab: Pengembang perangkat lunak perlu bertanggung jawab atas produk yang mereka buat. Pelatihan dapat membahas bagaimana memberikan informasi yang jelas kepada pengguna tentang cara perangkat lunak beroperasi dan bagaimana mengatasi masalah yang mungkin muncul.
7. Konflik Etika dan Pengambilan Keputusan: Pelatihan dapat membantu pengembang menghadapi situasi-situasi yang melibatkan konflik etika dalam pengembangan perangkat lunak. Ini melibatkan kemampuan untuk mempertimbangkan implikasi moral dari keputusan teknis.
8. Studi Kasus dan Diskusi: Pelatihan dapat mencakup studi kasus nyata tentang masalah etika dalam pengembangan perangkat lunak yang telah muncul sebelumnya. Diskusi tentang

bagaimana masalah-masalah ini dapat diatasi secara etis juga dapat meningkatkan pemahaman peserta.

9. Etika Kecerdasan Buatan: Jika pelatihan dilakukan di era di mana kecerdasan buatan (AI) semakin merambah ke berbagai bidang, penting untuk membahas etika yang terkait dengan pengembangan dan penerapan AI.

Pelatihan etika dalam pengembangan perangkat lunak tidak hanya membantu para pengembang dalam membuat produk yang lebih baik secara etis, tetapi juga membantu dalam membangun citra perusahaan yang positif dan menjaga kepercayaan pengguna.

BAB VI
ETIKA DALAM KECERDASAN BUATAN

6.1. Apa itu *Artificial* Intelligence?

Dengan berkembangnya teknologi, semakin praktis pula kehidupan sehari-hari manusia. Seluruh pekerjaan yang memakan waktu lama, kini dapat diringkas berkat teknologi. Salah satu titik revolusi perkembangan teknologi manusia adalah dikembangkannya teknologi uap yang dalam sejarahnya dikenal sebagai Revolusi Industri 1.0. Sebelum masuk ke era tersebut, manusia dihadapkan dengan segala jenis pekerjaan yang hanya mengandalkan tenaga manusia maupun hewan, baik itu dalam bidang pertanian, manufaktur, transportasi, dan lain sebagainya. Namun, pada saat masuk di era Revolusi Industri 1.0 perubahan pun terjadi secara masif. Revolusi Industri 1.0 ditandai ketika James Watt, menemukan sebuah alat penenun benang mekanik pada tahun 1784. Temuannya tersebut menggunakan mesin uap sehingga tidak memerlukan lagi tenaga hewan maupun manusia.

Sejak saat itu, teknologi pun berkembang sangat pesat hingga masuk ke abad 21 dimana Revolusi Industri 3.0 sudah diterapkan dan kini sudah masuk era Revolusi

4.0. Revolusi Industri 3.0 ditandai dengan ditemukannya mesin penggerak yang dapat berpikir sendiri, komputer. Pada Revolusi Industri inilah *Artificial Intelligence* (AI) ditemukan. Selanjutnya, memasuki era Industri 4.0 AI pun sudah sangat berkembang, kini dengan adanya internet, segala sesuatu yang bersifat elektronik dapat dihubungkan dengan internet yang menciptakan konsep baru bernama *Internet of Things* (IoT) serta beberapa dari teknologi tersebut sudah ditanamkan teknologi AI.

Artificial Intelligence (AI) muncul pertama kali pada tahun 1956 dalam konferensi Dartmouth. Nama Kecerdasan Buatan sendiri pertama kali disebutkan oleh John McCarthy pada tahun 1956 pada konferensi yang sama. Hadirnya AI di kehidupan manusia sangat membantu dalam segala bidang. Baik itu perekonomian, manufaktur, retail, kesehatan, keamanan dan lain-lain. Perkembangan AI yang begitu pesat membuat interaksi antara manusia dan AI pun semakin intens. Pada awalnya, AI dibuat untuk membantu manusia dalam pekerjaannya sehari-hari. Mulai dari sistem pemberi rekomendasi yang biasa ditemukan di beberapa website yang menyediakan jasa layanan yang ada di internet seperti Youtube, Netflix, Tokopedia dan Shopee, mesin pencari tingkat lanjut yang digunakan oleh Google, sistem rekognisi suara seperti Alexa atau Siri atau sistem

mengemudi otomatis yang dimiliki oleh Tesla. Semua fitur tersebut merupakan hasil dari perkembangan AI dan juga sangat membantu manusia dalam kesehariannya. Namun, akhir-akhir ini kita melihat mulai banyak pekerjaan yang justru diambil alih oleh AI. Industri media mulai menggunakan AI dalam menjalankan bisnisnya. Presenter yang di salah satu tv swasta nasional mulai menggunakan presenter AI dalam membawakan berita. Pada waktu yang berbeda, seorang CEO dari India memecat 90% pekerjanya untuk digantikan dengan AI, meskipun hasil dari pemecatan tersebut membawa keuntungan hingga 85% untuk perusahaan. Tapi dari sisi kemanusiaan, apa yang dilakukan oleh pemimpin perusahaan tersebut justru dapat menghancurkan hidup dari mantan pekerjanya.

Machine Learning (ML) merupakan istilah yang digunakan terhadap mesin yang dapat belajar sendiri tanpa mengikuti instruksi secara khusus. *Machine Learning* menggunakan algoritma dan model secara statistik untuk dapat mengenali pola, tren, kedekatan maupun anomali dalam data. Hal ini membuat *Machine Learning* dapat mempelajari berbagai model data seperti data penjualan yang memiliki rentang waktu, data daftar barang yang selanjutnya dikembangkan menjadi sistem rekomendasi dan lain sebagainya. Tetapi, karena hanya

menggunakan model statistik dalam penerapan pembelajaran komputer, bisa saja akan terjadi bias dalam pembelajarannya.

6.2. Bias Dalam Kecerdasan Buatan

Artificial Intelligence sangat bergantung data dalam pengambilan keputusannya, karena algoritma yang diguanakan merupakan model statistik maka semakin terjaga integritas dari sebuah data akan semakin baik pula pengambilan keputusan. Data yang tidak melalui proses pembersihan dan validasi akan membuat data tersebut menjadi data cacat dan tidak memiliki integritas. Pada penerapannya, komputer selalu menggunakan data dalam membuat keputusan, sehingga data yang cacat akan menghasilkan keputusan yang cacat juga.

> "JIKA DATA YANG CACAT DIMASUKKAN KE DALAM SISTEM, MAKA KOMPUTER AKAN MEMBUAT KEPUTUSAN YANG CACAT JUGA"
>
> -DR. BENJAMIN BADER

Sekarang bayangkan, jika pada saat memasukkan data ke dalam sistem yang tanpa melewati proses

pembersihan data dan validasi. Sistem tersebut merupakan sistem penunjang keputusan dalam merekrut karyawan baru di sebuah perusahaan. Karena data yang dimasukkan ke dalam sistem merupakan data yang cacat, maka komputer pun akan memproses data cacat tersebut dan akan menghasilkan keputusan yang juga cacat. Disisi lain, sistem yang selalu diberikan data yang cacat dapat mengakibatkan sistem tersebut mengalami bias dalam pengambilan keputusan. Contohnya seperti ini, ketika dalam perekrutan karyawan perusahaan selalu mengambil karyawannya dari suku tertentu, lalu data pribadi karyawan beserta dengan sukunya dimasukkan ke dalam sistem. Hal ini akan mengakibatkan kriteria dalam merekrut karyawan dari suku tertentu akan menjadi variabel dalam perhitungan pengambilan keputusan oleh AI. Tentu ini akan menjadi bias dalam AI dan sangat merugikan perusahaan yang menggunakan AI tersebut.

Inilah salah satu kelemahan dari AI yang harus diperhatikan oleh para penggunanya. Kecerdasan buatan selalu terikat dengan data dan tidak bisa berpikir diluar dari data. Dalam dunia ini, meskipun pengambilan keputusan berdasarkan data itu baik, tetapi tidak semua yang menggunakan data itu merupakan keputusan yang tepat. Sebagai manusia, sudah sepantasnya tidak bias

dalam pengambilan keputusan apalagi jika hal itu berkenaan dengan hal yang sensitif, seperti agama, suku, ras, etnis maupun jenis kelamin.

Bias dalam kecerdasan buatan sudah menjadi topik yang sangat populer pada tahun 2019. Bahkan menjadi salah satu masalah serius berkenaan dengan pengembangan kecerdasan buatan. Salah satu kasus populer bagaimana kecerdasan buatan dapat berperilaku bias adalah kasus diskriminasi oleh kecerdasan buatan yang dimiliki oleh departemen urusan dalam negeri New Zealand. Pada saat itu, foto dari seorang remaja keturunan asia dan berusia 16 tahun ditolak oleh sistem dikarenakan matanya terdeteksi tertutup. Pada akhirnya, sistem menyatakan foto remaja tersebut *invalid* dan tidak dapat digunakan untuk pembuatan pasport baru. Kasus lain yang serupa adalah ketika seorang wanita berkulit hitam ingin memperbarui pasportnya di UK dan fotonya terdeteksi dalam kualitas yang buruk serta mulutnya dinyatakan terbuka di foto tersebut yang mengakibatkan fotonya ditolak oleh sistem.

Kasus-kasus tersebut merupakan sebagian dari banyak kasus tentang biasnya kecerdasan buatan dalam pengambilan keputusan. Lemahnya pengawasan langsung oleh manusia dan algoritma yang digunakan

oleh vendor penyedia kecerdasan buatan yang selalu dirahasiakan membuat variabel yang digunakan dalam pengambilan keputusan oleh kecerdasan buatan tidak akurat.

6.3. Privasi Dalam Kecerdasan Buatan

Selain perilaku bias yang dapat terjadi pada kecerdasan buatan, keamanan data dan privasi pengguna pun menjadi salah satu kekhawatiran dalam penggunaan kecerdasan buatan.

6.3.1. Penggunaan Data Personal Oleh Pemerintah

Tiongkok merupakan salah satu negara yang memiliki teknologi kecerdasan buatan paling maju di dunia. Salah satu hasil dari teknologi kecerdasan buatan mereka adalah sebuah sistem yang bernama Sistem Kredit Sosial. Sistem ini memungkinkan pemerintah Tiongkok untuk bisa mendata dan memonitor seluruh warganya dan memberikan mereka kredit sosial tergantung dari kelakuan warganya masing-masing. Semakin baik warga negara Tiongkok dalam bernegara seperti membantu sesama, tidak terlibat tindakan kriminal maupun kejujuran akan membuat kredit sosialnya naik, begitupun sebaliknya. Kredit sosial yang tinggi

akan memberikan beberapa keuntungan seperti keringanan pajak, fasilitas gratis, transportasi publik yang murah dan lain sebagainya. Semua itu bisa dilakukan berkat kecerdasan buatan. Disisi lain, justru ini juga menjadi salah satu masalah privasi yang serius bagi warga Tiongkok.

Sistem Kredit Sosial akan memonitor seluruh warganya baik itu secara individu, organisasi maupun perusahaan. Perlakuan monitor ini tentu saja melanggar privasi bagi setiap orang dimana mereka kehilangan waktu privasi mereka. Salah satu dampak dari penggunaan kekuasaan atas monitoring yang dilakukan oleh pemerintah Tiongkok adalah ketika mereka menggunakan kecerdasan buatan untuk melacak perilaku dari tokoh-tokoh religius dari masyarakat Uighur.

Masyarakat Uighur yang tinggal di Xianjiang harus rela data mereka diambil secara paksa, dipantau selama 24/7 dan juga setiap kegiatan yang mereka lakukan seperti mereka tinggal dimana, pergi kemana saja, apakah mereka pernah melakukan pertukaran naskah kitab suci dan lain sebagainya.

6.3.2. Privasi Genetik

Data genetik adalah data yang biasa digunakan dalam dunia kedokteran. Dengan data tersebut, seorang dokter bisa tahu kondisi medis dari setiap orang. Dulu, pengurutan genom memiliki tarif yang sangat mahal yang mengakibatkan hanya beberapa orang saja yang mampu untuk melakukan ini. Tetapi, sekarang harga untuk melakukan pengurutan genom sudah sangat terjangkau dan bisa dilakukan oleh berbagai kelas masyarakat menengah ke bawah. Bahkan ada beberapa perusahaan yang kini telah berdiri dengan model bisnis pengurutan genom ini. Tentu ini membantu masyarakat secara umum untuk dapat mengenal genom mereka dan apakah mereka memiliki penyakit bawaan atau tidak. Tetapi disisi lain, kekhawatiran akan kepemiliki data genetik, keamanan perusahaan dalam melindungi data pasiennya menjadi pertanyaan besar jika suatu saat perusahaan itu bangkrut atau dibeli oleh perusahaan lain.

Kecerdasan buatan kini sudah bisa merekam data biometrik manusia dan mencocokkan secara otomatis melalui sistem. Data seperti sidik jari, wajah, kornea mata maupun genom, kini sudah

dapat dideteksi secara otomatis oleh kecerdasan buatan. Salah satu produk yang kini dikembangkan dan memiliki teknologi kecerdasan buatan adalah kamera pengawas biometrik. Kamera pengawas ini akan memantau dan mengikuti perilaku manusia yang berada dalam jangkauan tangkapan layarnya. Kamera ini akan mendeteksi dan secara otomatis mencocokkan wajah orang-orang yang berada di dalam rekaman dengan basis data biometrik yang sudah ada. Hal ini tentu saja dapat meningkatkan kontrol atas tindakan warga oleh pihak pemerintah akan tetapi ini juga menjadi isu privasi yang cukup berat.

Kasus yang cukup ramai diperbincangkan mengenai kamera biometrik ini adalah ketika kasus salah tangkap yang terjadi karena kesalahan kecerdasan buatan dalam mengenali wajah pelaku. Pria tersebut bernama Nijeer Park, dia menjadi korban salah tangkap karena kesalahan dalam pendeteksian wajah. Pada saat itu, dia sedang berada 30 mile dari lokasi kejadian akan tetapi tetap saja ditangkap karena polisi lebih mempercayai kecerdasan buatan ketimbang manusia. Kasus tersebut tentu saja menjadi perhatian khalayak

publik, apalagi kecerdasan buatan menjadi dalang dibalik mengapa ia bisa tertangkap.

6.3.3. Perlindungan Data dan Privasi

Dari beberapa kasus privasi dan keamanan data diatas membuktikan bahwa kecerdasan buatan bukan berarti bisa selalu benar dan ada beberapa hal yang harus diperhatikan ketika membuat atau membangun sistem dengan teknologi kecerdasan buatan.

Ada tujuh tipe privasi yang harus kita pahami terlebih dahulu sebelum membuat sistem dengan teknologi kecerdasan buatan :

a) Individu
b) Perilaku dan aksi
c) Komunikasi
d) Data dan foto
e) Pikiran dan perasaan
f) Lokasi dan ruang
g) Asosiasi

Dari ketujuh tipe privasi tersebut, hampir seluruhnya berhubungan dengan data. Nissenbaum (2019) menyarankan agar privasi dapat diartikan sebagai integritas kontekstual. Artinya adalah

perlindungan privasi spesifik terhadap konteks dan pengumpulan informasi perlu disesuaikan dengan konteks yang ada.

6.4. Manipulasi

Apakah kecerdasan buatan dapat memanipulasi manusia? Jawabannya adalah, ya. Salah satu hal yang dapat mengubah perilaku manusia ketika melakukan kegiatan sehari-hari adalah dengan menggunakan sistem rekomendasi berdasarkan perilaku.

Mungkin sistem ini tidak terdengar asing di telinga orang-orang pada umumnya. Sistem ini merupakan salah satu sistem yang paling sering dijumpai ketika sedang berselancar di dunia maya. Pada saat mencari barang atau informasi di mesin pencari seperti Google, maka pencarian tersebut akan direkam oleh Google untuk keperluan iklannya. Hasilnya adalah kalian akan sering menjumpai barang-barang yang kalian cari melalui iklan dari Google ketika sedang bermain sosial media.

Contoh, kalian pernah mencari ponsel dalam mesin pencari, maka selanjutnya kalian akan menemukan iklan-iklan tentang ponsel dari berbagai brand yang muncul di sosial media. Ini merupakan salah satu trik marketing serta manipulasi data personal yang

dilakukan oleh raksasa mesin pencari. Dengan begini, mereka bisa mendapatkan *revenue* yang lebih besar ketimbang memakai trik marketing konvensional lainnya.

6.5. Etika Kecerdasan Buatan

Dari beberapa kasus yang dijelaskan sebelumnya, kita dapat menyimpulkan bahwa banyak pelanggaran yang terjadi karena keterlibatan kecerdasan buatan, baik itu karena kesalahan dari kecerdasan buatan itu sendiri maupun karena kesalahan dari sisi praktis manusia dalam memanfaatkan teknologi kecerdasan buatan. Rendahnya pengetahuan tentang pentingnya data dan cara menentukan variabel yang tepat dalam pengembangan model *machine learning* dapat mengakibatkan bias secara desain model dan berdampak buruk kepada yang menggunakan teknologi tersebut.

Selain itu, publik juga harus memiliki pemahaman bahwa hasil keputusan dari kecerdasan buatan bukan nilai yang absolut, tetapi kita tetap harus kritis terhadap hasilnya. Pada akhirnya, kecerdasan buatan terbatas dengan kemampuan si pembuatnya dan algoritma yang diterapkan, sangat berbeda dengan manusia yang tidak terbatas akan algoritma statistika. Meskipun tidak memiliki kemampuan berpikir milidetik seperti

kecerdasan buatan, manusia memiliki kemampuan untuk menimbang dan memilih hasil terbaik bukan hanya berdasarkan fakta tetapi insting dan pengalaman manusia itu sendiri. Kecerdasan buatan sepatutnya hanya digunakan untuk membantu manusia dalam melakukan pekerjaannya sehari-hari bukan malah sebaliknya.

Maka dari itu, pembuatan kecerdasan buatan harus didasarkan etika dan moral yang dimiliki oleh manusia. Desain modelnya pun harus sangat teliti dan akurat, tanpa memperlihatkan celah bias yang dapat berakibatkan masalah rasis seperti kasus foto pembaruan pasport dan juga harus tetap tau batasan dalam menghargai privasi setiap warga dunia.

BAB VII
KOMPUTASI AWAN DAN *BIG DATA*

7.1. Konsep Dasar Komputasi Awan dan *Big data*

Komputasi awan merupakan suatu paradigma transformasional dalam teknologi yang memungkinkan organisasi dan individu untuk mengakses, menyimpan, dan mengelola sumber daya komputasi melalui jaringan internet (Liu et al., 2012). Model layanan utama dalam komputasi awan mencakup Software as a Service (SaaS), dimana perangkat lunak dapat diakses langsung melalui web tanpa perlu instalasi lokal; Platform as a Service (PaaS), yang menyediakan lingkungan untuk pengembangan dan implementasi aplikasi; serta Infrastructure as a Service (IaaS), yang memungkinkan akses ke sumber daya infrastruktur seperti server dan penyimpanan. Implementasi komputasi awan dapat bersifat publik, di mana penyedia layanan menawarkan akses terbuka ke sumber daya, atau pribadi, di mana organisasi membangun dan mengelola lingkungan komputasi internal. Fleksibilitas, skalabilitas, dan kemampuan beradaptasi dengan kebutuhan yang berubah membuat konsep komputasi awan menjadi

solusi yang kuat dalam menghadapi tuntutan teknologi saat ini.

Big data merujuk pada volume data yang sangat besar dan beragam yang dihasilkan oleh berbagai sumber seperti sensor, perangkat mobile, dan platform online. Konsep dasar *Big data* terdiri dari beberapa karakteristik utama, termasuk Volume, yang mengacu pada kuantitas data yang besar dan berkembang secara cepat; Variety, yang mencakup berbagai jenis data dari teks hingga multimedia; Velocity, yang menunjukkan kecepatan data yang dihasilkan dan harus diolah; serta Veracity, yang menekankan keandalan dan kualitas data (Zikopoulos & Eaton, 2011). Nilai dari *Big data* terletak pada kemampuannya untuk memberikan wawasan mendalam melalui analisis data yang cermat, membantu organisasi mengambil keputusan yang lebih baik dan mendapatkan pemahaman yang lebih baik tentang tren dan pola yang mendasarinya.

Komputasi awan dan *Big data* seringkali saling terkait dan saling memperkuat. Komputasi awan memberikan skala dan sumber daya yang diperlukan untuk mengelola dan menganalisis *Big data* dengan efisien. Dengan menggunakan infrastruktur cloud, organisasi dapat dengan mudah mengakses dan menyimpan data besar, mengimplementasikan alat

analisis canggih, dan mengelola tuntutan komputasi yang tinggi yang terlibat dalam pengolahan data besar. Kombinasi antara komputasi awan dan *Big data* juga mendorong inovasi dan pengembangan layanan baru, menghasilkan wawasan yang lebih mendalam, dan memfasilitasi perkembangan teknologi yang lebih lanjut dalam berbagai industri.

7.2. Peran Penting Komputasi Awan dan *Big data*

Komputasi awan memainkan peran krusial dalam transformasi digital saat ini. Dengan menyediakan akses terhadap sumber daya komputasi seperti server, penyimpanan, dan perangkat lunak melalui internet, komputasi awan memberikan fleksibilitas dan skalabilitas yang tak terbatas (Erl, Puttini, & Mahmood, 2013). Organisasi dapat dengan mudah mengelola dan mengalokasikan sumber daya sesuai permintaan, mengurangi biaya investasi awal dalam infrastruktur fisik, dan meningkatkan efisiensi operasional. Selain itu, komputasi awan memungkinkan kolaborasi global dan akses universal ke data dan aplikasi, mempercepat inovasi produk, dan memberikan layanan yang lebih baik kepada pelanggan. Dengan layanan keamanan dan pemulihan bencana yang disediakan, komputasi awan

juga melindungi data dan memastikan kelangsungan bisnis.

Big data telah mengubah cara kita memahami dan memanfaatkan informasi. Dengan analisis data dalam skala besar dan kompleksitas tinggi, *Big data* memungkinkan kita mengidentifikasi pola, tren, dan wawasan bisnis yang mendalam (Mayer-Schönberger & Cukier, 2013). Organisasi dapat menggunakan wawasan ini untuk membuat keputusan yang lebih baik dan meramalkan tren masa depan. Analisis *Big data* juga membantu dalam personalisasi layanan, meningkatkan pengalaman pelanggan, dan mengoptimalkan operasional. Keamanan data dan deteksi ancaman juga ditingkatkan melalui analisis *Big data*, sementara kemampuan pemrosesan real-time memungkinkan tindakan segera dalam menghadapi perubahan situasi.

Kombinasi komputasi awan dan *Big data* menciptakan sinergi yang kuat. Komputasi awan memberikan infrastruktur yang diperlukan untuk menyimpan dan mengelola volume besar data, sedangkan *Big data* memberikan alat analisis yang diperlukan untuk menggali wawasan dari data tersebut. Pengolahan *Big data* dapat dijalankan di lingkungan cloud, memungkinkan organisasi untuk dengan cepat mengukur dan menyesuaikan sumber daya sesuai

kebutuhan analisis. Kolaborasi global juga ditingkatkan melalui komputasi awan, memungkinkan tim di seluruh dunia untuk bekerja bersama dalam menganalisis data dan mengambil keputusan berdasarkan wawasan yang ditemukan.

Keduanya, komputasi awan dan *Big data*, memainkan peran penting dalam evolusi teknologi. Dengan terus berkembangnya kapabilitas komputasi awan dan alat analisis *Big data*, organisasi akan semakin mampu memanfaatkan potensi data untuk inovasi, pengambilan keputusan yang lebih baik, dan pengembangan layanan yang lebih unggul. Namun, seiring dengan manfaatnya, perhatian terhadap keamanan data, privasi, dan etika dalam penggunaan *Big data* juga akan semakin penting untuk diperhatikan dalam menghadapi tantangan masa depan.

7.2.1. Arsitektur Komputasi Awan

Arsitektur Komputasi Awan adalah suatu model pengelolaan sumber daya komputasi yang melibatkan infrastruktur jaringan yang luas, yang biasanya diakses melalui internet. Arsitektur ini memungkinkan pengguna untuk menyewa atau menggunakan sumber daya komputasi seperti pemrosesan data, penyimpanan, jaringan, dan

layanan lainnya dari penyedia layanan komputasi awan (Thomas, Zaigham, & Ricardo, 2013). Tujuan utama dari Arsitektur Komputasi Awan adalah untuk memberikan skalabilitas, elastisitas, dan ketersediaan yang tinggi bagi pengguna tanpa harus mengelola secara langsung perangkat keras atau infrastruktur fisik. Beberapa karakteristik utama dari Arsitektur Komputasi Awan meliputi:

1. Pembagian Sumber Daya:

   Sumber daya komputasi pemrosesan, penyimpanan, dan jaringan dibagi dan dialokasikan sesuai kebutuhan pengguna.

2. Elastisitas:

   Awan melakukan penyesuaian otomatis terhadap permintaan beban kerja yang bervariasi, sehingga pengguna dapat memperbesar atau memperkecil sumber daya dengan mudah.

3. Pembayaran Penggunaan:

   Pengguna membayar hanya untuk sumber daya yang mereka gunakan, mirip dengan model pembayaran utilitas.

4. Akses Jarak Jauh:

Pengguna dapat mengakses sumber daya komputasi awan dari mana saja dengan koneksi internet.

5. Ketersediaan Tinggi:
   Layanan komputasi awan dirancang untuk memberikan tingkat ketersediaan yang tinggi dengan menggunakan pemantauan dan replikasi yang cermat.
6. Layanan Mandiri:
   Pengguna dapat menyewa layanan tanpa perlu mengelola secara detail infrastruktur yang mendasarinya.

Beberapa contoh penyedia layanan komputasi awan terkenal adalah Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), dan IBM Cloud.

7.3. Tanggung Jawab Etis Penggunaan *Big data*

Tanggung jawab etis dalam penggunaan *big data* merupakan komitmen moral yang menuntun praktik pengumpulan, pengolahan, dan pemanfaatan data dalam skala besar untuk memastikan penggunaannya sejalan dengan prinsip-prinsip moral, hak asasi manusia, dan nilai-nilai sosial. Dalam era dimana data menjadi

komoditas yang semakin penting, tanggung jawab etis ini memerlukan perlindungan terhadap privasi individu dan penggunaan data yang adil serta berkeadilan. Pemahaman implikasi etis penggunaan *big data* haruslah meliputi pengakuan akan risiko pelanggaran privasi, kepentingan komersial yang bisa mengarah pada manipulasi data, dan potensi penguatan bias yang ada dalam data tersebut (Boyd & Crawford, 2012).

Penerapan transparansi adalah aspek kunci dalam tanggung jawab etis. Organisasi yang mengumpulkan dan menganalisis *big data* perlu memberikan informasi yang jelas tentang tujuan pengumpulan data, jenis data yang dikumpulkan, serta cara data tersebut akan digunakan (Mayer-Schönberger & Cukier, 2013). Keterbukaan ini memungkinkan individu untuk mengambil keputusan informasional tentang partisipasi mereka dalam proses tersebut. Selain itu, tanggung jawab etis juga mencakup upaya menghindari bias dan diskriminasi dalam analisis data. Di sinilah peran pemahaman mendalam tentang konteks sosial dan historis menjadi penting. Penggunaan *big data* harus dilakukan dengan memahami potensi munculnya bias dalam algoritma dan model, dengan memastikan bahwa data yang digunakan mencerminkan keberagaman masyarakat secara akurat (Diakopoulos, 2016).

Dapat disimpulkan, bahwa tanggung jawab etis dalam penggunaan *big data* mendorong perlindungan privasi, transparansi, dan keadilan dalam semua tahapan proses pengumpulan dan analisis data. Dengan mengikuti prinsip-prinsip ini, kita dapat memanfaatkan potensi *big data* untuk mendorong kemajuan sosial dan teknologi, dengan tetap menjaga integritas nilai-nilai etis dan kemanusiaan.

7.3.1. Etika Pengelolaan *Big data*

Etika pengelolaan *big data* merupakan serangkaian prinsip dan pedoman yang mengatur bagaimana *big data* diperlakukan, dikumpulkan, diproses, dan digunakan dengan cara yang adil, transparan, dan bertanggung jawab (Zwitter, 2014). Tujuan dari etika ini adalah untuk menjaga privasi individu, mencegah penyalahgunaan data, dan memastikan manfaat yang adil dari penggunaan *big data*. Berikut adalah beberapa prinsip etika dalam pengelolaan *big data*:

1. Pentingnya Privasi: Data pribadi individu harus dijaga dan dilindungi dengan sangat serius. Informasi sensitif dihapus atau diidentifikasi secara anonim agar tidak

dapat ditelusuri kembali ke individu tertentu.

2. Transparansi: Penggunaan dan tujuan pengumpulan data harus dinyatakan dengan jelas kepada individu yang bersangkutan. Penggunaan data harus sesuai dengan apa yang telah dijelaskan kepada mereka.
3. Kewajaran dan Keadilan: Penggunaan data harus adil dan tidak diskriminatif. Tidak boleh ada pengambilan keputusan atau pemberian layanan yang merugikan atau menguntungkan kelompok tertentu secara tidak adil.
4. Pertanggung jawaban: Yang mengumpulkan, memproses, dan menggunakan *big data* harus bertanggung jawab atas tindakan mereka. Mereka siap untuk menghadapi konsekuensi yang mungkin timbul dari penggunaan data tersebut.
5. Kepatuhan Hukum: Pengelolaan *big data* harus mematuhi hukum dan regulasi yang berlaku, termasuk undang-undang privasi dan perlindungan data.

Contoh Kasus: Penggunaan *big data* dalam analisis kesehatan masyarakat Sebuah kelompok riset mengumpulkan data kesehatan dari berbagai sumber, termasuk catatan medis elektronik, data genetik, dan data gaya hidup individu. Mereka menganalisis data untuk mengidentifikasi pola-pola kesehatan dan risiko penyakit tertentu. Namun, tanpa izin yang jelas dan transparan, serta tindakan yang memadai untuk melindungi privasi, risiko penyalahgunaan data atau pelanggaran privasi dapat timbul.

7.4. Etika Keamanan Data dalam Komputasi Awan

Etika keamanan data merujuk pada prinsip-prinsip dan praktik mengatur perlindungan dan pengelolaan data yang disimpan dan diproses dalam lingkungan komputasi awan. Etika keamanan data dalam komputasi awan sangat penting karena melibatkan penyimpanan dan pemrosesan data sensitif dari berbagai organisasi dan individu.

Beberapa prinsip etika keamanan data dalam komputasi awan meliputi (Regulation, 2018):

1. Kerahasiaan Data: Penyedia layanan awan harus menjaga kerahasiaan data pelanggan. Mereka mengimplementasikan langkah-langkah enkripsi

yang tepat untuk melindungi data saat istirahat dan saat diproses.

2. Integritas Data: Data yang disimpan dan diproses dalam komputasi awan harus tetap utuh dan tidak diubah tanpa otorisasi. Perlindungan terhadap perubahan data yang tidak sah harus diimplementasikan.
3. Ketersediaan Layanan: Penyedia layanan awan harus memastikan ketersediaan data dan layanan secara konsisten. Mereka perlu mengadopsi praktik redundansi dan pemulihan bencana untuk mengatasi gangguan layanan.
4. Transparansi: Penyedia layanan awan harus memberikan informasi yang jelas kepada pelanggan tentang bagaimana data dikelola dan dilindungi. Keterbukaan ini membantu pelanggan membuat keputusan informasi yang lebih baik.
5. Pematuhan Regulasi: Penyedia layanan awan harus mematuhi semua peraturan dan perundangan yang berlaku terkait dengan perlindungan data, seperti General Data Protection Regulation (GDPR) di Uni Eropa.
6. Penghapusan Data yang Aman: Pelanggan harus memiliki kontrol atas data, termasuk

kemampuan untuk menghapusnya dari layanan awan dengan aman dan permanen.

7. Keamanan Jaringan dan Aplikasi: Selain melindungi data, komputasi awan juga harus melindungi infrastruktur jaringan dan aplikasi dari ancaman keamanan.
8. Kualitas Layanan: Penyedia layanan awan harus memberikan tingkat layanan yang dijanjikan kepada pelanggan dalam hal keamanan dan ketersediaan.

7.4.1. Perlindungan Data dalam Penyimpanan Awan

Perlindungan data dalam penyimpanan awan adalah upaya untuk menjaga keamanan, kerahasiaan, integritas, dan ketersediaan data yang disimpan di layanan penyimpanan awan. Penyimpanan awan mengacu pada praktik menyimpan data pada infrastruktur komputasi yang dikelola oleh penyedia layanan, seperti Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Dropbox, dan layanan serupa.

Perlindungan data dalam penyimpanan awan menjadi krusial karena data yang disimpan di

lingkungan awan dapat diakses melalui internet dan melibatkan banyak pihak yang terlibat, termasuk pengguna, penyedia layanan, dan mungkin juga pihak jahat. Beberapa aspek kunci dalam perlindungan data dalam penyimpanan awan meliputi:

1. Enkripsi Data: Enkripsi adalah metode untuk melindungi data dengan mengubahnya menjadi bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang tepat. Ada dua jenis enkripsi yang relevan dalam penyimpanan awan:
    - Enkripsi Data Istirahat: Data yang disimpan dalam penyimpanan awan harus dienkripsi saat berada dalam istirahat. Ini mencegah akses tidak sah ke data bahkan jika perangkat keras fisiknya dicuri atau diakses oleh pihak yang tidak berwenang.
    - Enkripsi Data Pergerakan: Data yang dikirim antara perangkat pengguna dan penyimpanan awan harus dienkripsi saat bergerak melalui jaringan internet. Hal ini melindungi data dari serangan sniffing atau penyadapan.

2. Manajemen Akses: Penyedia layanan awan harus memberikan alat untuk mengelola akses pengguna dan hak istimewa, termasuk otentikasi (verifikasi identitas) dan otorisasi (pengaturan izin akses). Memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses dan mengelola data.
3. Audit dan Pemantauan: Penyedia layanan awan harus menyediakan alat untuk melacak aktivitas pengguna dan akses ke data. Audit dan pemantauan ini membantu mendeteksi potensi ancaman dan melacak jejak audit jika terjadi pelanggaran keamanan.
4. Pemulihan Bencana dan Cadangan: Layanan penyimpanan awan harus memiliki rencana pemulihan bencana yang memungkinkan pemulihan data setelah insiden keamanan atau gangguan layanan. Pemulihan data yang efektif dan rutin menjaga integritas data.

Contoh Kasus:

Bayangkan perusahaan e-commerce yang menyimpan semua informasi pelanggan, transaksi,

dan inventaris di penyimpanan awan. Mereka harus memastikan bahwa data pelanggan tidak dapat diakses oleh pihak yang tidak berwenang dan bahwa transaksi online aman dari peretasan. Dalam hal ini, mereka dapat mengadopsi praktik seperti enkripsi data istirahat untuk melindungi data pelanggan saat disimpan di penyimpanan awan. Mereka juga harus memastikan bahwa data transaksi dikirimkan dengan aman melalui enkripsi data pergerakan.

7.5. Transparansi dan Akuntabilitas Penggunaan Komputasi Awan dan *Big data*

Transparansi serta akuntabilitas penggunaan komputasi awan dan *big data* merupakan prinsip-prinsip kunci yang membentuk dasar tata kelola yang aman dan etis dalam pengolahan data modern. Transparansi melibatkan penyediaan informasi yang jelas dan mudah dipahami kepada pengguna dan pemangku kepentingan lainnya tentang bagaimana data dikumpulkan, diproses, dan digunakan dalam lingkungan komputasi awan dan *big data*. Dalam hal ini, organisasi harus memberikan gambaran yang akurat tentang praktik-praktik mereka, tujuan penggunaan

data, serta langkah-langkah yang diambil untuk melindungi privasi dan keamanan data.

Sebagai contoh kasus, pertimbangkan situasi dimana sebuah perusahaan e-commerce menggunakan layanan komputasi awan untuk menyimpan data pelanggan dan menganalisis perilaku belanja mereka. Perusahaan ini harus secara transparan mengkomunikasikan kepada pelanggan tentang jenis data yang dikumpulkan, alasan dibalik pengumpulan data, serta bagaimana data tersebut membantu dalam meningkatkan pengalaman belanja. Selain itu, perusahaan tersebut bertanggung jawab dalam melindungi data pelanggan dengan menerapkan langkah-langkah keamanan yang kuat dan mengikuti regulasi perlindungan data yang berlaku, seperti GDPR di Uni Eropa.

Disisi akuntabilitas, organisasi harus memiliki tanggung jawab yang jelas terkait dengan pengelolaan data dan harus siap memberikan pertanggungjawaban jika terjadi pelanggaran privasi atau kebocoran data. Misalnya, sebuah rumah sakit yang menggunakan teknologi *big data* untuk menganalisis data medis pasien harus mengambil langkah-langkah akuntabilitas dengan memastikan bahwa data pasien dijaga kerahasiaannya, hanya diakses oleh pihak yang berwenang, dan bahwa

analisis data dilakukan sesuai dengan etika medis dan regulasi kesehatan.

Contoh Kasus:

- Pelanggaran Privasi di Layanan Komputasi Awan: Sebuah perusahaan menyimpan data sensitif pelanggan di platform komputasi awan. Namun, mereka tidak mengimplementasikan langkah-langkah keamanan yang memadai, dan akibatnya data pelanggan terekspos secara tidak sah. Dalam konteks ini, transparansi berarti perusahaan memberikan informasi pada pelanggan tentang bagaimana data mereka akan dikelola dan dijamin untuk keamanannya. Akuntabilitas akan mewajibkan perusahaan untuk bertanggung jawab atas kebocoran data dan mengambil langkah-langkah perbaikan yang sesuai.
- Analisis *Big data* di Bidang Kesehatan: Sebuah lembaga medis menggunakan analisis *big data* untuk mengidentifikasi tren dan pola dalam data pasien guna meningkatkan pengobatan. Transparansi dalam kasus ini akan melibatkan komunikasi yang jelas kepada pasien tentang bagaimana data medis mereka akan digunakan dan diolah dalam proses analisis. Akuntabilitas

akan berarti lembaga medis harus memastikan bahwa data pasien dijaga kerahasiaannya dan bahwa hasil analisis digunakan dengan tanggung jawab untuk memperbaiki perawatan pasien.

7.6. Manajemen Risiko dalam Komputasi Awan dan *Big data*

Manajemen Risiko dalam Komputasi Awan dan *Big data* adalah pendekatan yang komprehensif untuk mengidentifikasi, mengukur, mengelola, dan memitigasi risiko-risiko yang terkait dengan penerapan dan penggunaan teknologi komputasi awan dan pengelolaan data besar. Komputasi Awan melibatkan penyediaan layanan IT melalui jaringan internet, sedangkan *Big data* melibatkan analisis dan pemrosesan data dalam skala besar untuk mendapatkan wawasan berharga.

Dalam konteks Komputasi Awan, risiko utama melibatkan keamanan data, dimana informasi sensitif dapat terancam oleh serangan peretasan atau ancaman siber lainnya. Manajemen risiko harus memperhatikan langkah-langkah seperti enkripsi data saat bergerak dan saat istirahat, serta pemantauan aktif terhadap aktivitas mencurigakan. Selain itu, aspek ketersediaan layanan juga penting; oleh karena itu, strategi manajemen risiko

harus melibatkan perencanaan ketidaktersediaan sementara dan cadangan yang efektif.

Dalam *Big data*, risiko utama adalah privasi data dan ketidakakuratan. Pemrosesan data besar dapat mengungkapkan informasi pribadi, mengancam privasi individu, dan melanggar peraturan privasi seperti GDPR. Manajemen risiko dalam hal ini dapat melibatkan teknik anonimisasi data atau penghapusan identitas individu sebelum analisis. Selain itu, risiko ketidakakuratan data dapat mempengaruhi keputusan bisnis yang diambil. Maka dari itu, organisasi perlu memastikan integritas data dan melakukan validasi secara berkelanjutan.

7.6.1. Tantangan Etis Manajemen Risiko Bisnis

Pembahasan permasalahan etika yang timbul dalam mengelola risiko bisnis yang melibatkan penggunaan teknologi komputasi awan dan analisis *big data*. Teknologi ini memungkinkan perusahaan untuk menyimpan, mengolah, dan menganalisis jumlah data yang besar untuk mengambil keputusan yang lebih informasional dan strategis. Namun, pemanfaatan teknologi ini juga menyajikan sejumlah tantangan etis yang perlu diperhatikan oleh organisasi.

Tantangan-tantangan etis dalam manajemen risiko bisnis terkait dengan komputasi awan dan *big data* meliputi:

1. Privasi dan Keamanan Data: Penyimpanan data di awan dan analisis *big data* dapat mengancam privasi individu jika tidak diatur dengan baik. Perusahaan harus menjaga data pelanggan dan karyawan aman dan menghindari penyalahgunaan informasi. Tantangan etis muncul ketika data sensitif yang tidak sah diakses oleh pihak yang tidak berwenang atau ketika data digunakan tanpa persetujuan.

   Contoh Kasus: Sebuah perusahaan teknologi menyimpan data pengguna di awan. Namun, celah keamanan yang tidak terdeteksi memungkinkan peretas mengakses data pribadi pelanggan, termasuk informasi keuangan dan kontak. Penyalahgunaan data ini dapat merugikan privasi dan keuangan pelanggan.
2. Transparansi dan Pengawasan:Penggunaan teknologi ini dapat membuat sulit bagi pelanggan atau pihak terkait untuk memahami bagaimana data digunakan.

Ketidaktransparan ini dapat menyebabkan kehilangan kepercayaan dan merugikan citra perusahaan.

Contoh Kasus: Sebuah perusahaan media sosial mengumpulkan data pengguna untuk menyediakan rekomendasi konten yang disesuaikan. Namun, algoritma yang digunakan untuk rekomendasi ini tidak diungkapkan secara transparan kepada pengguna. Sebagai hasilnya, pengguna tidak tahu bagaimana rekomendasi tersebut dibuat atau bagaimana data mereka digunakan.

3. Diskriminasi Algoritma:

   Penggunaan analisis *big data* dapat menghasilkan keputusan yang tidak adil atau diskriminatif jika algoritma tidak dikalibrasi dengan baik atau memiliki bias tersembunyi. Hal ini dapat mengarah pada perlakuan yang tidak setara terhadap kelompok tertentu.

   Contoh Kasus: Sebuah perusahaan asuransi menggunakan analisis *big data* untuk menilai risiko pelamar asuransi. Namun, algoritma ini secara tidak sengaja

memberikan penilaian yang lebih rendah kepada pemohon dari latar belakang etnis tertentu, menghasilkan diskriminasi tak disengaja.

4. Ketidakpastian Hukum dan Regulasi: Teknologi komputasi awan dan *big data* berkembang lebih cepat daripada regulasi yang mengaturnya. Perusahaan harus memastikan bahwa mereka mematuhi hukum dan regulasi terkait perlindungan data.

   Contoh Kasus:

   Sebuah perusahaan perbankan menggunakan layanan cloud untuk menyimpan data nasabah. Namun, undang-undang perlindungan data baru-baru ini diberlakukan yang mengharuskan data nasabah tetap berada di yurisdiksi tertentu. Perusahaan ini menghadapi tantangan untuk mematuhi regulasi baru tanpa mengganggu operasional mereka.

5. Pemanfaatan Data Etis:

   Meskipun data besar dapat memberikan wawasan berharga, perusahaan harus memastikan bahwa penggunaan data

tersebut adalah etis dan sesuai dengan nilai-nilai sosial. Penggunaan data yang tidak etis dapat merugikan pelanggan, karyawan, atau masyarakat secara umum.

Contoh Kasus:

Sebuah perusahaan retail menggunakan analisis *big data* untuk menentukan harga produk berdasarkan perilaku pembelian pelanggan. Namun, perusahaan memanfaatkan data pelanggan untuk memanipulasi harga dan meningkatkan keuntungan tanpa memberikan manfaat yang adil kepada konsumen.

Dalam setiap contoh kasus di atas, perusahaan dihadapkan pada tantangan etis dalam pengelolaan risiko bisnis terkait dengan komputasi awan dan *big data*. Solusi untuk tantangan-tantangan ini melibatkan pengembangan kebijakan yang jelas terkait privasi dan penggunaan data, transparansi kepada pihak yang terpengaruh, pengawasan dan audit yang ketat terhadap algoritma, pematuhan hukum dan regulasi, serta penggunaan data yang etis dan bertanggung jawab.

7.6.2. Etika Bisnis untuk Keuntungan Ekonomi

Etika bisnis dalam pemanfaatan teknologi Komputasi Awan dan *Big data* untuk mencapai keuntungan ekonomi memerlukan keseimbangan antara tujuan bisnis dan tanggung jawab sosial. Salah satu contoh kasus yang menggambarkan hal ini adalah penggunaan data konsumen dalam industri periklanan. Sebuah perusahaan periklanan menggunakan teknologi *Big data* untuk mengumpulkan dan menganalisis data dari perilaku online konsumen, seperti riwayat pencarian, preferensi produk, dan aktivitas media sosial. Tujuannya adalah untuk membuat iklan yang lebih efektif dan personal.

Namun, dalam kasus ini, etika bisnis menjadi relevan dalam beberapa aspek. Pertama, perlindungan privasi konsumen harus dijaga dengan cermat. Penggunaan data pribadi tanpa izin atau tanpa transparansi dapat melanggar privasi konsumen dan merusak kepercayaan mereka terhadap perusahaan. Kedua, ada risiko potensial untuk diskriminasi atau stereotipe yang tidak disengaja dalam penyegmentasian target iklan. Misalnya, penggunaan data demografis yang keliru

dapat mengarah pada iklan yang eksklusif atau menyingkirkan sebagian kelompok masyarakat.

Dalam menghadapi tantangan ini, perusahaan periklanan harus mengambil pendekatan etis dengan memprioritaskan privasi konsumen, memberikan transparansi tentang penggunaan data, dan menerapkan analisis data yang bebas dari bias. Dengan melakukan hal ini, perusahaan dapat mencapai tujuan ekonomi mereka dengan menghormati prinsip-prinsip etika bisnis dan memastikan dampak positif pada masyarakat secara keseluruhan.

BAB VIII
ETIKA DALAM SISTEM OTOMASI DAN *INTERNET OF THINGS* (IoT)

8.1. Pengertian IoT

IoT (*Internet of Things*) adalah sebuah konsep di dunia teknologi yang merujuk pada jaringan perangkat fisik (seperti perangkat elektronik, sensor, aktuator, dan objek lainnya) yang terhubung ke internet dan dapat saling berkomunikasi serta berbagi data dengan perangkat lainnya melalui jaringan, tanpa melibatkan interaksi manusia. Istilah "*Internet of Things*" secara harfiah mengacu pada ide bahwa objek atau perangkat yang berada dalam keseharian kita dapat "berbicara" satu sama lain melalui internet.

Beberapa karakteristik penting dari IoT adalah:

1. Koneksi: Perangkat IoT harus memiliki kemampuan untuk terhubung ke internet atau jaringan lainnya. Ini biasanya melibatkan penggunaan teknologi seperti Wi-Fi, Bluetooth, 4G/5G, atau protokol jaringan khusus.
2. Sensor dan Aktuator: Perangkat IoT sering dilengkapi dengan sensor untuk mendeteksi

informasi dari lingkungan sekitarnya, seperti suhu, kelembaban, cahaya, dan sebagainya. Mereka juga dapat memiliki aktuator yang memungkinkan mereka untuk melakukan tindakan fisik, seperti mengendalikan lampu, mesin, atau perangkat lainnya berdasarkan informasi yang diterima dari sensor.

3. Komunikasi: IoT memungkinkan perangkat untuk saling berkomunikasi dan berbagi data dengan perangkat lainnya. Ini memungkinkan pengumpulan data yang real-time dan kerjasama antara perangkat.
4. Data: Data yang dikumpulkan oleh perangkat IoT dapat diolah dan dianalisis untuk mengambil keputusan atau memberikan informasi berharga.
5. Automasi: Salah satu tujuan utama IoT adalah meningkatkan efisiensi dan kenyamanan dengan mengotomatiskan tindakan berdasarkan data yang diterima dari perangkat.

Contoh penggunaan IoT meliputi rumah pintar (*smart home*) yang dapat mengontrol pencahayaan, pendingin udara, dan sistem keamanan melalui smartphone, kendaraan otonom yang menggunakan sensor dan data untuk mengemudi secara mandiri,

sistem kesehatan yang memantau kondisi pasien secara real-time, dan banyak aplikasi lainnya di berbagai sektor seperti industri, pertanian, dan kota pintar.

IoT telah mengubah cara kita berinteraksi dengan dunia fisik dan memiliki potensi besar untuk meningkatkan efisiensi, produktivitas, dan kualitas hidup kita. Namun, juga menghadirkan tantangan baru terkait dengan privasi, keamanan, dan etika yang harus diperhatikan dalam pengembangan dan implementasinya.

8.2. Konsep Otomasi

Otomasi adalah konsep yang merujuk pada penggunaan teknologi dan sistem untuk menggantikan atau mengotomatiskan tugas-tugas yang sebelumnya dilakukan oleh manusia. Tujuan utama dari otomasi adalah meningkatkan efisiensi, konsistensi, akurasi, dan produktivitas dalam berbagai bidang.

Berikut adalah beberapa konsep kunci dalam otomasi:

1. Proses Otomasi: Proses otomasi melibatkan penggunaan perangkat keras dan perangkat lunak untuk mengotomatiskan tugas-tugas tertentu. Proses ini dapat berkisar dari tugas sederhana seperti mengirimkan email otomatis

hingga tugas yang lebih kompleks seperti pengendalian produksi di pabrik.

2. Perangkat Keras Otomasi: Ini mencakup penggunaan mesin, robot, sensor, aktuator, dan perangkat fisik lainnya untuk mengotomatiskan tugas-tugas fisik. Contohnya adalah robot industri yang dapat melakukan pengelasan atau pemindahan barang secara otomatis.
3. Perangkat Lunak Otomasi: Perangkat lunak otomasi digunakan untuk mengotomatiskan tugas-tugas berbasis komputer. Ini termasuk dalam pengembangan perangkat lunak, pemrosesan data, pengambilan keputusan, dan tugas-tugas administratif lainnya. Contoh termasuk algoritma kecerdasan buatan (AI) yang dapat mengotomatiskan pengenalan wajah, analisis data, atau chatbot yang dapat menjawab pertanyaan pelanggan secara otomatis.
4. Kendali Otomatis: Konsep ini melibatkan penggunaan sensor untuk mengukur kondisi dan input dari lingkungan, dan kemudian menggunakan algoritma untuk mengambil tindakan secara otomatis berdasarkan data yang diterima. Contoh adalah termostat pintar yang

mengatur suhu dalam ruangan berdasarkan suhu luar dan preferensi pengguna.

5. Otomasi Proses Bisnis: Ini mencakup penggunaan otomasi untuk mengotomatiskan tugas-tugas dalam proses bisnis, seperti manajemen inventaris, penjadwalan, pengiriman pesanan, dan pembayaran. Otomasi proses bisnis dapat meningkatkan efisiensi operasional dan mengurangi biaya.
6. Otomasi Kendaraan: Kendaraan otonom adalah contoh dari otomasi transportasi, di mana kendaraan dapat beroperasi tanpa pengemudi manusia. Ini melibatkan sensor, perangkat lunak, dan kecerdasan buatan untuk mengemudi dan mengambil keputusan secara mandiri.
7. Keamanan Otomasi: Dalam konteks otomasi, keamanan sangat penting. Perlindungan terhadap ancaman siber, keselamatan fisik, dan privasi data harus dipertimbangkan dengan serius dalam pengembangan dan implementasi sistem otomasi.
8. Etika Otomasi: Seperti yang dibahas sebelumnya, etika juga merupakan aspek penting dalam otomasi. Pertanyaan etis seperti dampak sosial,

pengangguran akibat otomasi, dan privasi data harus dijawab secara hati-hati.

Otomasi memiliki potensi besar untuk meningkatkan produktivitas dan kualitas hidup, tetapi juga membawa sejumlah tantangan yang perlu dikelola dengan baik. Dalam mengimplementasikan otomasi, perlu mempertimbangkan aspek-aspek seperti biaya, keamanan, kesiapan teknis, dan dampak sosial dan etis yang mungkin terjadi.

8.3. Manfaat dan Tantangan IoT dan Otomasi

IoT (*Internet of Things*) dan otomasi memberikan berbagai manfaat yang signifikan, tetapi juga menghadapi sejumlah tantangan yang perlu diatasi. Berikut adalah beberapa manfaat dan tantangan utama dari kedua konsep ini:

Manfaat IoT:

1. Efisiensi Operasional: IoT memungkinkan perusahaan dan organisasi untuk mengoptimalkan operasi mereka dengan mengumpulkan data real-time dari perangkat dan sensor. Ini dapat mengarah pada penghematan biaya yang signifikan.

2. Peningkatan Produktivitas: Dengan otomatisasi tugas-tugas rutin, pekerjaan manusia dapat diarahkan ke tugas yang lebih kreatif dan berorientasi pada nilai tambah, yang pada gilirannya dapat meningkatkan produktivitas.
3. Pemantauan Jarak Jauh: IoT memungkinkan pemantauan jarak jauh dari perangkat dan sistem. Ini berarti Anda dapat mengontrol perangkat di rumah Anda, memantau produksi di pabrik, atau mengawasi kondisi pasien di rumah sakit dari jarak jauh.
4. Analisis Data yang Lebih Baik: Data yang dikumpulkan oleh perangkat IoT dapat dianalisis untuk mengambil keputusan yang lebih baik. Ini berlaku untuk bisnis, ilmu pengetahuan, dan banyak aspek lain dari kehidupan sehari-hari.
5. Kenyamanan Pengguna: IoT telah menciptakan berbagai perangkat pintar yang meningkatkan kenyamanan pengguna, seperti rumah pintar (smart home) yang dapat mengontrol pencahayaan, suhu, keamanan, dan perangkat lainnya dengan mudah.

Tantangan IoT:

1. Privasi dan Keamanan: Data yang dikumpulkan oleh perangkat IoT dapat menjadi target serangan siber. Privasi pengguna juga dapat terancam jika data yang dikumpulkan digunakan dengan tidak etis.
2. Ketergantungan pada Teknologi: Dalam beberapa kasus, kita dapat menjadi sangat tergantung pada teknologi IoT, yang dapat mengakibatkan masalah jika ada kegagalan sistem atau serangan siber.
3. Interoperabilitas: Perangkat IoT dari berbagai produsen seringkali tidak kompatibel satu sama lain, yang dapat menghambat adopsi yang lebih luas dan integrasi yang mudah.

Manfaat Otomasi:

1. Efisiensi Operasional: Otomasi tugas-tugas manusia dapat mengurangi kesalahan manusia dan meningkatkan efisiensi dalam berbagai sektor, termasuk manufaktur dan bisnis.
2. Ketepatan dan Konsistensi: Sistem otomatis dapat melakukan tugas-tugas dengan ketepatan yang tinggi dan konsistensi, tanpa kelelahan atau kesalahan.

3. Peningkatan Keamanan: Dalam beberapa kasus, otomasi dapat meningkatkan keamanan, misalnya dalam sistem keamanan pintu dan alarm.

Tantangan Otomasi:

1. Pengangguran dan Perubahan Pekerjaan: Otomasi dapat menggantikan pekerjaan manusia, yang dapat menyebabkan pengangguran dalam beberapa kasus. Hal ini juga memerlukan perubahan dalam kualifikasi dan keterampilan yang diperlukan oleh tenaga kerja.
2. Biaya Implementasi: Implementasi otomasi dapat memerlukan investasi yang signifikan dalam perangkat keras dan perangkat lunak, yang mungkin tidak dapat diakses oleh semua bisnis atau organisasi.
3. Keamanan Sistem: Seperti halnya IoT, otomasi juga dapat menjadi target serangan siber jika tidak dielola dengan baik.
4. Etika: Penerapan otomasi dalam beberapa kasus memunculkan pertanyaan etika, seperti dalam penggunaan kecerdasan buatan dalam

pengambilan keputusan yang memengaruhi hidup manusia.

Penting untuk mengenali manfaat dan tantangan ini dan mengambil langkah-langkah yang diperlukan untuk meminimalkan risiko serta memaksimalkan potensi manfaat dari IoT dan otomasi. Ini mencakup investasi dalam keamanan siber, regulasi yang bijak, dan perencanaan yang matang dalam menghadapi perubahan sosial dan ekonomi yang mungkin terjadi.

8.4. Aspek Etika dalam IoT dan Otomasi

Aspek etika sangat penting dalam perkembangan dan penggunaan *Internet of Things* (IoT) dan otomasi. Dalam kedua domain ini, terdapat berbagai pertimbangan etis yang perlu diperhatikan untuk memastikan bahwa teknologi ini digunakan dengan cara yang bermanfaat, aman, dan adil. Berikut adalah beberapa aspek etika utama yang perlu diperhatikan dalam IoT dan otomasi:

Aspek Etika dalam IoT:

1. Privasi Data: Pengumpulan dan penggunaan data pribadi oleh perangkat IoT adalah masalah utama. Penting untuk memastikan bahwa data yang dikumpulkan dijaga kerahasiaannya dan

bahwa pengguna memiliki kendali atas data mereka. Perusahaan harus mengikuti praktik privasi yang ketat dan mendukung hak pengguna untuk menghapus atau membatasi akses ke data mereka.

2. Kemungkinan Penyalahgunaan Data: Data yang dikumpulkan oleh perangkat IoT dapat digunakan untuk tujuan yang tidak etis, seperti penargetan iklan yang agresif atau penyalahgunaan informasi pribadi. Perusahaan harus menghindari penggunaan data yang merugikan pengguna atau masyarakat.
3. Keamanan: Keamanan perangkat IoT harus diutamakan. Perangkat yang rentan terhadap serangan siber dapat digunakan untuk tujuan jahat, termasuk mengganggu privasi pengguna atau bahkan mengendalikan perangkat secara tidak sah.
4. Pertimbangan Sosial: Perkembangan IoT harus memperhitungkan dampak sosialnya. Ini mencakup pertimbangan seperti pengangguran akibat otomasi, perubahan dalam cara kita berinteraksi dengan teknologi, dan dampak pada kehidupan sehari-hari.

5. Ketergantungan Teknologi: Ketika kita semakin bergantung pada IoT, kita juga semakin rentan terhadap gangguan atau kegagalan sistem. Ini memunculkan pertanyaan etis tentang kesiapan kita dalam menghadapi situasi darurat atau keadaan yang tidak terduga.

Aspek Etika dalam Otomasi:

1. Pengangguran dan Perubahan Pekerjaan: Otomasi dapat menggantikan pekerjaan manusia, yang dapat mengarah pada pengangguran. Penting untuk mempertimbangkan dampak sosial dari otomasi dan menyediakan solusi seperti pelatihan dan transisi pekerjaan.
2. Diskriminasi Algoritma: Jika algoritma otomasi dibuat dengan bias atau data yang tidak representatif, ini dapat menyebabkan diskriminasi terhadap kelompok tertentu. Harus ada upaya untuk memastikan bahwa algoritma dan model machine learning adil dan tidak mendiskriminasi.
3. Keamanan dan Keselamatan: Otomasi dalam kendaraan, pabrik, atau perangkat lain harus memprioritaskan keamanan dan keselamatan.

Kesalahan atau kegagalan otomasi dapat berdampak serius pada nyawa manusia.

4. Etika Pengambilan Keputusan: Otomasi seringkali melibatkan pengambilan keputusan berdasarkan data dan algoritma. Pertanyaan etis muncul tentang siapa yang bertanggung jawab jika keputusan tersebut salah atau merugikan.
5. Kesadaran Etika: Penting untuk meningkatkan kesadaran etika dalam pengembangan dan penggunaan otomasi. Ini termasuk pelatihan bagi mereka yang mengelola dan bekerja dengan teknologi otomasi.
6. Transparansi: Pengguna harus dapat memahami bagaimana otomasi mengambil keputusan. Transparansi dalam algoritma dan proses otomasi adalah penting untuk memastikan akuntabilitas.

Dalam kedua kasus, etika harus menjadi bagian integral dari pengembangan, desain, dan implementasi teknologi. Ini memerlukan kerja sama antara perusahaan teknologi, pemerintah, akademisi, dan masyarakat sipil untuk mengembangkan kerangka kerja etika yang memandu perkembangan dan penggunaan

IoT dan otomasi dengan cara yang bermanfaat bagi semua pihak.

8.5. Standar Etika dan Regulasi

Standar etika dan regulasi adalah penting dalam mengarahkan pengembangan, penggunaan, dan manajemen *Internet of Things* (IoT) dan otomasi. Mereka membantu memastikan bahwa teknologi ini digunakan dengan cara yang aman, adil, dan bermanfaat, dan melindungi hak dan privasi individu. Berikut adalah beberapa standar etika dan regulasi yang relevan untuk IoT dan otomasi:

1. Standar Etika:
    a) IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: IEEE mengembangkan standar etika yang memandu pengembangan sistem otonom dan cerdas yang berfokus pada isu-isu seperti transparansi, akuntabilitas, dan keputusan berbasis AI yang adil.
    b) The European Union's Ethics Guidelines for Trustworthy AI: Panduan ini menyediakan kerangka kerja etika untuk pengembangan kecerdasan buatan yang dapat dipercaya dan adil. Panduan ini menggarisbawahi prinsip-

prinsip seperti keadilan, transparansi, dan akuntabilitas.

2. Regulasi Umum:
    a) General Data Protection Regulation (GDPR) (UE): GDPR adalah peraturan yang berlaku di Uni Eropa yang mengatur perlindungan data pribadi. Ini memiliki dampak besar pada pengumpulan, penyimpanan, dan penggunaan data dalam konteks IoT.
    b) Children's Online Privacy Protection Act (COPPA) (AS): COPPA adalah undang-undang Amerika Serikat yang melindungi privasi anak-anak di bawah usia 13 tahun dalam konteks layanan online, termasuk perangkat IoT.
3. Regulasi Khusus:
    a. Regulasi Keamanan IoT: Beberapa negara dan badan regulasi mengembangkan regulasi yang mengatur keamanan perangkat IoT. Misalnya, California memiliki regulasi yang mengharuskan perangkat IoT yang terhubung ke internet mematuhi standar keamanan tertentu.
    b. Standar Keselamatan Kendaraan Otonom: Regulasi dan standar keselamatan diperlukan

untuk kendaraan otonom. Berbagai negara dan badan regulasi telah mengeluarkan regulasi dan standar untuk menguji dan mengoperasikan kendaraan otonom dengan aman.

4. Standar Industri:
    a. ISO/IEC 27001 (Keamanan Informasi): Standar ini mengatur praktik manajemen keamanan informasi, yang relevan dalam melindungi data yang dikumpulkan oleh perangkat IoT.
    b. ISO/IEC 20243 (Keamanan dalam Sistem IoT): Standar ini berfokus pada keamanan dalam konteks *Internet of Things* dan memberikan panduan tentang bagaimana melindungi perangkat dan data dalam lingkungan IoT.
5. Standar Keselamatan Produk:
    a. CE Marking (Konformitas Eropa): Ini adalah tanda konformitas yang diperlukan untuk produk yang dijual di Uni Eropa, termasuk perangkat IoT. Ini memastikan bahwa produk memenuhi standar keselamatan yang diperlukan.

b. FCC (Federal Communications Commission) (AS): FCC mengatur perangkat yang beroperasi di Amerika Serikat, termasuk perangkat IoT yang menggunakan komunikasi nirkabel.

Penting untuk memahami dan mematuhi standar etika dan regulasi yang berlaku di wilayah Anda ketika terlibat dalam pengembangan atau penggunaan IoT dan otomasi. Dengan mematuhi standar ini, kita dapat memastikan bahwa teknologi ini digunakan dengan cara yang bertanggung jawab dan memenuhi norma etika yang diperlukan.

BAB IX
ETIKA DALAM REALITAS VIRTUAL DAN AUGMENTASI

9.1. Relevansi Etika dalam Konteks Realitas Virtual dan Augmentasi

Dalam konteks ini, etika memegang peranan yang sangat relevan karena teknologi ini dapat mempengaruhi berbagai aspek kehidupan.

1. Privasi dan Keamanan

   Dalam dunia realitas virtual dan augmentasi, data pribadi kita sering terlibat. Pertanyaan etis muncul tentang bagaimana data ini dikumpulkan, disimpan, dan digunakan. Dalam lingkungan virtual yang semakin terhubung, perlindungan data pribadi menjadi sangat penting.

2. Psikologis dan Emosional

   Teknologi ini dapat memiliki dampak psikologis dan emosional pada penggunanya. Misalnya, realitas virtual yang begitu imersif dapat mengubah persepsi tentang realitas yang

sebenarnya, yang dapat memiliki implikasi etis terkait kesehatan mental dan kesejahteraan.

3. Ketercampuran Dunia Nyata dan Virtual
   Dalam realitas virtual dan augmentasi, batas antara dunia nyata dan dunia virtual menjadi kabur. Pertanyaan etis muncul tentang bagaimana kita memahami realitas ini, bagaimana kita memperlakukan perbedaan antara keduanya, dan apa dampaknya pada persepsi dunia dan interaksi sosial kita.
4. Dampak Sosial dan Budaya
   Penggunaan teknologi ini juga dapat memiliki dampak besar pada tatanan sosial dan budaya. Perubahan dalam cara kita berinteraksi, bekerja, dan berkomunikasi dapat membawa tantangan etis baru, seperti potensi isolasi sosial atau peningkatan kesenjangan teknologi.

9.2. Tantangan Etika dalam Realitas Virtual dan Augmentasi

Prinsip-prinsip privasi mengalami tantangan serius dalam dunia virtual dan augmentasi. Penggunaan teknologi ini seringkali melibatkan berbagi data pribadi atau informasi sensitif, dan pertanyaan etis muncul tentang bagaimana data ini dikumpulkan, digunakan,

dan melibatkan privasi pengguna. Perangkat teknologi dapat mengumpulkan informasi tentang perilaku, preferensi, atau lokasi pengguna tanpa mereka sadari, sehingga menggarisbawahi perlunya prinsip-prinsip privasi yang kuat.

a. Ketidakjelasan Antara Dunia Virtual dan Dunia Nyata(Implikasi Etika)

   Salah satu tantangan etika terbesar dalam realitas virtual adalah ketidakjelasan antara dunia virtual dan dunia nyata. Penggunaan teknologi ini bisa membuat pengguna kesulitan membedakan antara pengalaman dalam dunia virtual dan realitas sehari-hari. Ini dapat memiliki implikasi etis terkait dengan tanggung jawab dan konsekuensi atas tindakan di dunia virtual, serta dampak psikologis atas perbedaan ini.

b. Dampak Psikologis dan Emosional dalam Pengalaman Realitas Virtual

   Realitas virtual dapat memiliki dampak psikologis dan emosional yang signifikan pada pengguna. Meskipun realitas virtual dapat memberikan pengalaman yang mendalam dan menyenangkan, penggunaan yang berlebihan atau pengalaman yang menakutkan dapat mengganggu keseimbangan emosi dan kesejahteraan mental. Pertanyaan etis

muncul tentang tanggung jawab pengembang untuk merancang pengalaman yang aman dan positif bagi pengguna.

9.3. Etika Penggunaan Realitas Virtual dan Augmentasi

Beberapa aspek etis yang perlu dipertimbangkan dalam mengintegrasikan teknologi ini dalam berbagai konteks.

1. Etika dalam Penggunaan Realitas Virtual untuk Pelatihan dan Pendidikan

   Penggunaan realitas virtual untuk tujuan pelatihan dan pendidikan telah menjadi semakin umum. Namun, pertanyaan etis muncul tentang bagaimana teknologi ini digunakan dalam hal memberikan pengalaman realistis tetapi aman bagi pelatihan situasi yang berpotensi berbahaya atau merugikan. Dampak pada moral dan etika pengguna juga menjadi perhatian, karena pengalaman dalam dunia virtual dapat mempengaruhi pandangan dan perilaku di dunia nyata.
2. Pengaruh Etika dalam Penggunaan Realitas Virtual dalam Bidang Kesehatan

Teknologi realitas virtual memiliki potensi besar dalam bidang kesehatan, mulai dari terapi hingga pelatihan dokter dan perawat. Namun, etika memainkan peran penting dalam memastikan bahwa penggunaan teknologi ini adalah aman, efektif, dan sesuai dengan standar medis. Pertimbangan etis juga mencakup privasi data pasien, persetujuan informasi, serta kualitas dan validitas informasi yang diberikan dalam pengalaman kesehatan virtual.

3. Implikasi Etika dari Augmentasi Manusia dan Identitas Digital

   Augmentasi manusia merujuk pada peningkatan kemampuan manusia melalui teknologi, seperti implantasi mikrochip atau perangkat bionik. Implikasi etis muncul tentang bagaimana penggunaan teknologi ini dapat mempengaruhi konsep identitas manusia, hak individu, dan kesetaraan. Selain itu, pertanyaan tentang bagaimana teknologi ini memengaruhi kehidupan pribadi dan profesional pengguna juga menjadi perhatian.

9.4. Etika dalam Konteks Bisnis dan Hiburan

Penggunaan teknologi realitas virtual dan augmentasi dalam pemasaran dan promosi telah membuka pintu untuk pengalaman yang lebih interaktif dan mendalam bagi konsumen. Namun, pertanyaan etis muncul tentang batas antara konten promosi yang informatif dan menguntungkan dengan konten yang menyesatkan atau memanipulasi. Pertimbangan etika juga mencakup penggunaan data pribadi untuk menyusun kampanye yang lebih personal dan efektif.

Industri hiburan telah mengadopsi teknologi realitas virtual untuk memberikan pengalaman yang lebih mendalam kepada penonton. Namun, pertanyaan etis muncul tentang dampak perubahan dalam cara kita mengkonsumsi hiburan. Dalam hal ini, pertimbangan termasuk keseimbangan antara realitas dan imajinasi, serta pengaruh teknologi pada etika kreativitas dan narasi.

Perusahaan yang mengadopsi teknologi realitas virtual dan augmentasi juga harus mempertimbangkan tanggung jawab sosialnya. Ini mencakup bagaimana penggunaan teknologi ini dapat mempengaruhi pelanggan, karyawan, dan masyarakat secara umum. Pertanyaan etis muncul tentang dampak pada

kesejahteraan, inklusi, dan dampak lingkungan dari produksi perangkat fisik.

9.5. Tantangan Regulasi dan Hukum

Tantangan hukum dan regulasi yang terkait dengan penggunaan teknologi realitas virtual dan augmentasi. Ini mencakup kesulitan dalam mengatur teknologi ini dan perlindungan hukum terhadap privasi serta keamanan pengguna.

a. Kesulitan dalam Mengatur Teknologi Realitas Virtual dan Augmentasi

   Pengembangan teknologi realitas virtual dan augmentasi telah melampaui batas-batas tradisional dalam banyak kasus. Regulasi yang tepat menjadi tantangan karena teknologi ini masih dalam tahap perkembangan dan evolusi yang cepat. Regulator harus memahami teknologi ini secara mendalam untuk mengembangkan kerangka kerja yang sesuai. Pertanyaan etis muncul tentang bagaimana mengatur konten yang mungkin melibatkan realitas virtual dan dunia nyata, serta sejauh mana teknologi ini dapat diakses oleh masyarakat umum.

b. Perlindungan Hukum untuk Privasi dan Keamanan Pengguna dalam Realitas Virtual

Teknologi realitas virtual sering melibatkan penggunaan data pribadi dan interaksi langsung dengan pengguna. Pertanyaan etis dan hukum muncul tentang bagaimana data ini harus dikelola dan dilindungi. Kebutuhan untuk privasi dan perlindungan data memerlukan kerangka kerja hukum yang memastikan bahwa data pengguna tidak disalahgunakan atau terekspos. Selain itu, pertimbangan juga mencakup perlindungan pengguna dari potensi ancaman keamanan dalam lingkungan virtual.

9.6. Masa Depan Etika dalam Realitas Virtual dan Augmentasi

Bagaimana pertimbangan etis dapat mengarah pada evolusi teknologi ini dan dampaknya pada masyarakat dan norma.

1. Antisipasi Etika Terkait Perkembangan Teknologi Realitas Virtual dan Augmentasi

   Masa depan teknologi realitas virtual dan augmentasi akan membawa perkembangan yang lebih lanjut. Pertimbangan etis menjadi sangat penting dalam mengantisipasi implikasi dari

perkembangan ini. Pertanyaan etis muncul tentang bagaimana menghadapi tantangan baru yang mungkin timbul, seperti kemungkinan peningkatan dalam manipulasi visual atau perubahan dalam cara kita berinteraksi dengan dunia digital dan fisik.

2. Masyarakat Virtual yang Beretika (Membangun Norma dan Nilai dalam Dunia Virtual)

   Dengan semakin intensifnya interaksi dalam dunia virtual, muncul kebutuhan untuk membangun norma dan nilai yang berlaku di ruang tersebut. Etika dalam dunia virtual melibatkan bagaimana kita berinteraksi satu sama lain, bagaimana kita memperlakukan data pribadi, dan bagaimana kita menjaga etika dalam lingkungan yang seringkali lebih tidak terkendali. Pertimbangan juga mencakup bagaimana kita mendorong inklusi, menghindari diskriminasi, dan menjaga integritas dalam dunia virtual.

9.7. Refleksi Etika dalam Realitas Virtual dan Augmentasi

Mempertimbangkan bagaimana etika telah berkembang seiring dengan evolusi teknologi ini dan

menggali cara-cara untuk menjaga keseimbangan antara inovasi dan tanggung jawab etis.

a. Menilai Perkembangan Etika dalam Teknologi Ini

   Tinjauan mengenai perkembangan etika dalam teknologi realitas virtual dan augmentasi akan melibatkan penilaian terhadap bagaimana isu-isu etis telah diakui, diatasi, atau bahkan muncul sebagai dampak langsung dari penggunaan teknologi ini. Hal ini melibatkan analisis tentang bagaimana perubahan dalam teknologi telah mengarah pada pertimbangan etika yang baru, serta upaya yang telah dilakukan oleh komunitas pengembang dan pemangku kepentingan untuk mengatasi tantangan etis.

b. Menjalin Keseimbangan antara Inovasi dan Tanggung Jawab Etis

   Salah satu tantangan utama dalam penggunaan teknologi realitas virtual dan augmentasi adalah menjaga keseimbangan antara inovasi yang mendukung kemajuan teknologi dan tanggung jawab etis terhadap pengguna, masyarakat, dan lingkungan. Refleksi ini akan mencakup pemaparan tentang upaya yang dapat dilakukan

untuk memastikan bahwa inovasi tidak melanggar prinsip-prinsip etis yang mendasar.

9.8. Etika dalam Pelatihan dan Simulasi untuk Profesional

Penggunaan teknologi realitas virtual untuk pelatihan profesional membuka peluang untuk menciptakan skenario yang mendekati situasi nyata. Namun, etika dalam pengembangan skenario pelatihan sangat penting. Ini mencakup:

1. Konteks Etis

   Pastikan bahwa skenario pelatihan yang dibuat mencerminkan nilai-nilai etis yang berkaitan dengan industri atau profesi tertentu.

2. Kesesuaian

   Skenario pelatihan harus sesuai dan relevan dengan tujuan pelatihan serta tidak mengekspos peserta pelatihan pada situasi yang merugikan atau menyesatkan.

3. Persetujuan

   Pastikan bahwa peserta pelatihan memberikan persetujuan yang jelas dan sadar untuk mengambil bagian dalam simulasi.

Penggunaan data pelatihan dalam realitas virtual juga melibatkan pertimbangan etis yang serius:

a. Privasi Data

   Pastikan bahwa data yang dikumpulkan selama pelatihan atau simulasi tidak disalahgunakan atau dibagikan tanpa izin peserta.

b. Anonimitas

   Jika data pelatihan digunakan untuk analisis atau penelitian lebih lanjut, pastikan bahwa peserta tetap anonim dan data tidak dapat ditelusuri kembali kepada individu.

c. Keamanan Data

   Lindungi data pelatihan dari akses yang tidak sah dan pastikan bahwa tindakan keamanan yang tepat diambil untuk mencegah pelanggaran data.

9.9. Antisipasi Etika dalam Perkembangan Teknologi Realitas Virtual dan Augmentasi

Pengembangan teknologi realitas virtual dan augmentasi terus berlanjut dengan cepat. Namun, banyak tantangan etika yang perlu dihadapi dalam proses ini:

1. Keamanan dan Privasi

Bagaimana mengembangkan teknologi yang memprioritaskan keamanan data dan privasi pengguna?

2. Pembiasan Algoritma

   Bagaimana mencegah algoritma yang digunakan dalam teknologi ini menghasilkan diskriminasi atau bias yang tidak disengaja?

3. Tanggung Jawab Pengembang

   Bagaimana mengembangkan kerangka kerja etika untuk memastikan tanggung jawab pengembang dalam menghadapi konsekuensi teknologi yang dibuat?

Pengembangan teknologi realitas virtual dan augmentasi dapat memiliki dampak sosial dan psikologis yang signifikan. Oleh karena itu, perlu mengantisipasi dampak-dampak tersebut:

a. Pengaruh Psikologis

   Bagaimana teknologi ini dapat memengaruhi kesejahteraan psikologis pengguna dan apakah ada risiko adiksi atau dampak negatif lainnya?

b. Perubahan Sosial

   Bagaimana teknologi ini dapat mengubah cara kita berinteraksi, bekerja, dan bermain, serta

bagaimana kita menghadapinya sebagai masyarakat?

c. Kesenjangan Digital

   Bagaimana mencegah terbentuknya kesenjangan digital yang lebih dalam akibat penggunaan teknologi ini?

BAB X
ETIKA DALAM PENGGUNAAN MEDIA SOSIAL & KOMUNIKASI ONLINE

10.1. Fenomena Abad 21

Era digital dimulai pada akhir abad ke-20 dan terus berlanjut hingga saat ini. Perkembangan teknologi digital, terutama dengan munculnya internet dan komputer pribadi, telah mengubah dramatis cara kita berinteraksi, bekerja, dan mengakses informasi.

Era digital juga ditandai dengan pertumbuhan media sosial, komunikasi daring, e-commerce, dan transformasi digital di berbagai industri. Era ini terus berkembang dengan inovasi dan kemajuan teknologi yang terus muncul, seperti kecerdasan buatan, *Internet of Things* (IoT), *big data*, dan kecerdasan komputasional.

Tentu saja, Era digital yang terus berkembang membawa banyak perubahan dan dampak signifikan dalam berbagai aspek kehidupan. Penggunaan Media sosial, aplikasi pesan instan, dan platform komunikasi lainnya memungkinkan kita untuk terhubung dengan orang lain secara global dalam waktu nyata.

Komunikasi menjadi lebih cepat, mudah, dan terjangkau. Belum lagi akses informasi yang menjadi lebih mudah diakses. Internet memberikan akses tak terbatas ke berbagai sumber informasi dan pengetahuan.

Sampai pada bidang bisnis dimana era digital telah mengubah lanskap bisnis dan ekonomi dengan membuka peluang baru dalam hal perdagangan, pemasaran, dan inovasi. Perusahaan-perusahaan juga harus beradaptasi dengan perubahan teknologi untuk tetap relevan dan bersaing di era digital.

Tak lupa juga di bidang pendidikan, teknologi digital telah membawa perubahan dalam pendidikan. Pembelajaran online, e-learning, dan sumber daya digital telah memperluas akses ke pendidikan dan memberikan fleksibilitas dalam cara kita belajar dan mengajar.

Era digital merasuk ke dalam kehidupan sehari-hari kita melalui perangkat pintar, aplikasi, dan teknologi terintegrasi lainnya. Dari rumah pintar hingga kesehatan digital, teknologi telah mempengaruhi cara kita mengelola dan menjalani kehidupan kita.

Akan tetapi, tidak sampai disitu, perlu diakui bahwa era ini pun memiliki sisi negatif yang terkait dengan perkembangan teknologinya. Dimulai dari kesenjangan digital yag bisa memperdalam kesenjangan

sosial dan ekonomi, sebagai akibat dari kesulitan akses, keterbatasan infrastruktur dan biaya.

Belum lagi dalam hal keamanan dan privasi data yang menjadi masalah yang signifikan. Pelanggaran data, serangan siber, dan pencurian identitas semakin marak terjadi.

Tak lupa juga, penyebaran Berita Palsu (Hoaks) dengan tujuan memanipulasi opini publik atau menciptakan kebingungan. Penyebaran hoaks dapat memiliki dampak negatif yang serius, termasuk mengganggu stabilitas sosial dan merusak reputasi individu atau kelompok. Dapat dilihat contoh gambar yang dimanipulasi yang dapat dikategorikan hoax (gambar 1).

"Foto dihasilkan oleh AI"

Gambar 1

Dalam aspek psikologi, manusia berusaha menampilkan kehidupan yang sempurna, ditambah lagi dengan cyberbullying, dan perbandingan sosial. Ketergantungan dan kecanduan digital pun berkontribusi terhadap kesehatan mental, produktivitas, dan hubungan sosial.

Menyadari kebaikan dan tantangan perkembangan digital ini dapat membantu kita mengembangkan pendekatan yang lebih bijaksana dan bertanggung jawab terhadap penggunaan teknologi digital, tentu saja dengan pertimbangan etika sehingga dapat mengevaluasi kebenaran dan kesalahan informasi online yang ditemui.

10.2. Kasus Pelanggaran etika di media sosial & komunikasi online

Realitas etika komunikasi terus berkembang seiring dengan perkembangan teknologi dan perubahan sosial. Hal ini membutuhkan pemahaman yang mendalam dan refleksi kritis terhadap praktik komunikasi yang kita lakukan, dengan mempertimbangkan nilai-nilai etis dan dampak sosial yang dihasilkan.

Beberapa contoh kasus pelanggaran etika komunikasi yang pernah terjadi baik Indonesia maupun

Luar Negeri. Berikut ini beberapa contoh kasus yang cukup umum:

1. Pencemaran Nama Baik dan Pelecehan Online: Ini melibatkan penyebaran informasi atau komentar yang merusak reputasi seseorang secara online, termasuk ancaman, pelecehan, dan intimidasi. Pencemaran nama baik dan pelecehan online dapat menyebabkan kerugian emosional dan psikologis pada individu yang menjadi sasaran.
2. Pelanggaran Privasi: Kasus ini melibatkan pengungkapan atau penggunaan informasi pribadi seseorang tanpa izin. Pelanggaran privasi dapat terjadi dalam bentuk penyadapan komunikasi pribadi, pemantauan ilegal, atau penyebaran informasi pribadi tanpa persetujuan.
3. Cyberbullying: Ini adalah kasus di mana individu atau kelompok secara sistematis melecehkan, mengintimidasi, atau menghina orang lain melalui media digital. Cyberbullying dapat berdampak serius pada kesehatan mental dan emosional korban.
4. Plagiarisme: Kasus ini melibatkan penggunaan atau pengambilan karya orang lain tanpa

memberikan pengakuan atau persetujuan yang sesuai. Plagiarisme adalah pelanggaran etika dalam komunikasi dan merusak kepercayaan serta integritas penulis asli.

5. Manipulasi atau Penyensoran Informasi: Ini terjadi ketika informasi sengaja dimanipulasi atau disensor untuk mengarahkan opini publik atau menyembunyikan kebenaran. Manipulasi atau penyensoran informasi yang tidak etis dapat merusak integritas jurnalisme dan menghalangi akses publik terhadap informasi yang benar dan akurat.
6. Konflik Kepentingan: Ini terjadi ketika jurnalis atau media memiliki konflik kepentingan yang memengaruhi objektivitas dan integritas penyajian berita. Konflik kepentingan dapat mengarah pada penyampaian berita yang bias atau tidak adil.
7. Penggunaan Tidak Etis Data Pribadi: Ini melibatkan pengumpulan, penggunaan, atau penjualan data pribadi orang lain tanpa izin atau melanggar peraturan privasi yang berlaku. Penyalahgunaan data pribadi dapat melibatkan pelanggaran privasi dan penyalahgunaan kepercayaan.

Kasus-kasus di atas menunjukkan bahwa etika komunikasi sangat penting dalam masyarakat Indonesia. Masyarakat, media massa, dan individu perlu menjunjung tinggi nilai-nilai etika, seperti kejujuran, integritas, keberagaman, dan menghormati martabat manusia. Etika komunikasi yang baik dapat mempromosikan pemahaman, harmoni, dan keadilan dalam interaksi komunikatif di masyarakat.

Penting untuk mencatat bahwa kasus-kasus ini merupakan contoh pelanggaran etika komunikasi dan bukan praktik yang diharapkan atau dianjurkan. Etika komunikasi yang baik melibatkan penghormatan, kejujuran, integritas, dan tanggung jawab dalam berkomunikasi dengan orang lain.

10.3. Etika Media Baru

Sebelum menelaah terkait etika dan elemen yang terkait, kita sebaiknya memahami media baru terlebih dahulu. Media baru merupakan babakan terbaru media massa sebagai kelanjutan era elektronik. Munculnya jaringan internet menjadikan media meanstream sperti koran, radio, televisi dikonvergensi menjadi media baru. Koran yang awalnya cetak dikonvergensi menjadi surat kabar online, radio yang hanya didengar dari studio radio dengan alokasi frekuensinya ataupun TV untuk

jenis audio visualnya, sekarang juga sudah terkonvergensi dengan jaringan internet jadilah radio dan TV yang memanfaatkan sarana online. Belum lagi sosial media dengan platform yang dipilih setiap individu.

Sementara itu, etika adalah studi tentang apa yang dianggap baik dan benar, serta prinsip-prinsip moral yang mengatur perilaku manusia. Secara umum, etika mencakup penilaian tentang apa yang seharusnya dilakukan atau dihindari oleh individu atau kelompok dalam berbagai situasi. Etika juga mencakup pertimbangan tentang konsekuensi moral dari tindakan-tindakan tersebut.

Etika berfungsi sebagai panduan atau kerangka kerja bagi manusia dalam mengambil keputusan dan bertindak dengan mempertimbangkan nilai-nilai moral dan prinsip-prinsip yang dianggap benar. Tujuan etika adalah untuk mempromosikan kehidupan yang adil, bermartabat, dan bertanggung jawab bagi individu dan masyarakat.

Etika juga melibatkan pemikiran kritis, refleksi, dan dialog moral. Dalam konteks profesional, etika sering dihubungkan dengan kode etik yang ditetapkan oleh organisasi atau profesi tertentu untuk memberikan

panduan bagi para anggotanya dalam menjalankan tugas mereka dengan integritas dan tanggung jawab.

Etika media baru, yang juga dikenal sebagai etika media digital atau etika media sosial, cabang etika yang berkaitan dengan prinsip-prinsip moral yang terkait dengan penggunaan media baru, teknologi digital, dan platform media sosial, membawa perubahan dalam cara kita berinteraksi dengan media dan mengakses informasi, dan etika media baru mencoba untuk mengatasi tantangan dan pertanyaan moral yang muncul dalam konteks ini.

Etika media baru berupaya untuk mengembangkan kerangka kerja etis yang relevan dan mempertimbangkan konsekuensi moral yang muncul dalam era digital. Hal ini melibatkan penerapan nilai-nilai seperti transparansi, keadilan, kebebasan berbicara, privasi, dan pertimbangan terhadap kepentingan dan kesejahteraan pengguna.

Penting untuk dicatat bahwa etika dapat bervariasi antara budaya, agama, dan konteks sosial. Namun, terdapat pula nilai-nilai universal seperti prinsip-prinsip dasar seperti menghormati martabat manusia, keadilan, kebenaran, dan kebaikan yang sering diakui di berbagai tradisi etika.

10.4. Pakar Etika Komunikasi Digital

Berikut ini adalah beberapa pakar yang dikenal dalam bidang etika komunikasi digital:

1. Charles Ess: Charles Ess adalah seorang profesor yang memiliki minat khusus dalam etika komunikasi digital dan media sosial. Ia telah menulis banyak artikel dan buku tentang topik ini, termasuk buku berjudul "Digital Media Ethics" yang menjadi referensi utama dalam studi etika komunikasi digital.
2. Luciano Floridi: Luciano Floridi adalah seorang filsuf dan ahli dalam bidang etika komputer dan informasi. Ia telah berkontribusi dalam pengembangan teori etika komunikasi digital, dengan penekanan pada isu-isu seperti privasi, identitas digital, dan etika kecerdasan buatan.
3. Rafael Capurro: Rafael Capurro adalah seorang filsuf dan pakar dalam bidang etika informasi dan komunikasi. Ia telah memperkenalkan konsep "etika informatika" yang melibatkan pemikiran etis dalam konteks teknologi informasi dan komunikasi.

Pakar-pakar ini memiliki pengetahuan dan pemahaman mendalam tentang isu-isu etika dalam

konteks komunikasi digital. Karya-karya mereka memberikan pandangan dan analisis yang berharga untuk memahami dan mempraktikkan etika komunikasi dalam era digital.

Perlu dicatat bahwa daftar ini tidak lengkap, dan masih ada banyak pakar lainnya bahkan dari Indonesia yang juga memiliki keahlian dan kontribusi dalam bidang etika komunikasi digital.

10.5. Manfaat Etika Komunikasi Digital

Etika komunikasi digital yang semakin mendesak di era digital saat ini menuntut etika komunikasi digital. Bukan tanpa alasan, Etika komunikasi digital melibatkan penggunaan teknologi dan platform digital. Dalam konteks ini, penting untuk menjaga **keamanan data pribadi dan menghormati privasi orang lain**. Etika komunikasi digital memerlukan penggunaan yang bertanggung jawab terhadap informasi pribadi dan menghindari pelanggaran privasi yang merugikan orang lain.

Selanjutnya, di era digital yang penuh dengan informasi, penting untuk berkomunikasi secara etis dengan **memerangi penyebaran informasi palsu atau hoaks**. Etika komunikasi digital melibatkan verifikasi informasi sebelum menyebarkannya, berbagi konten

yang akurat, dan berkontribusi pada penyebaran informasi yang dapat dipercaya.

Tak lupa juga, Etika komunikasi digital mengajarkan pentingnya menghindari kekerasan, pelecehan, atau perilaku yang merugikan orang lain dalam lingkungan online. Ini mencakup **menghindari penghinaan, pelecehan verbal, atau serangan pribadi yang dapat merusak kesejahteraan mental dan emosional orang lain.**

Etika komunikasi digital menjadi alternatif utama dalam mendorong penggunaan teknologi dan platform digital untuk tujuan yang positif, seperti berbagi ide, berkolaborasi, dan memupuk kreativitas. Dengan menghormati hak kekayaan intelektual, mengakui kontribusi orang lain, dan menghindari plagiarisme atau pencurian konten, etika komunikasi digital membangun lingkungan yang mendukung **kreativitas dan inovasi.**

Begitu banyak aspek-aspek yang muncul dalam etika dalam penggunaan media sosial & komunikasi online. Yang jelas, penerapan prinsip-prinsip etika komunikasi dalam era digital membantu membangun lingkungan online yang lebih positif, saling menghormati, dan berkontribusi pada kebaikan bersama. Dengan kesadaran dan penggunaan yang bertanggung jawab, kita dapat memanfaatkan teknologi

digital untuk berkomunikasi secara efektif, membangun hubungan yang sehat, dan menyebarkan informasi yang bermanfaat. Dengan mempraktikkan etika komunikasi digital, kita dapat menjaga integritas kita sendiri, menghormati privasi orang lain, dan membangun komunitas online yang positif dan inklusif.

BAB XI
ETIKA DALAM PENGGUNAAN TEKNOLOGI DI LINGKUNGAN KERJA

11.1. Latar Belakang

"Penerapan etika di lingkungan kerja" mengacu pada penerapan praktis dan integrasi prinsip dan nilai etika dalam operasi, praktik, dan proses pengambilan keputusan organisasi. Ini melibatkan penciptaan budaya yang mempromosikan perilaku etis, menetapkan pedoman dan kebijakan etis, dan memastikan bahwa karyawan memahami dan mematuhinya.

Organisasi mengembangkan dan mengkomunikasikan seperangkat standar dan kebijakan etis yang menentukan perilaku yang dapat diterima dan memandu karyawan dalam tindakan mereka. Standar-standar ini biasanya mencakup bidang-bidang seperti kejujuran, integritas, rasa hormat, keadilan, kerahasiaan, dan penggunaan sumber daya yang bertanggung jawab. Implementasi etis dimulai dari atas dengan para pemimpin yang menunjukkan dan mempromosikan perilaku etis. Pemimpin berfungsi sebagai panutan dan mengatur nada untuk perilaku etis dalam organisasi.

Mereka membuat keputusan etis, mengomunikasikan harapan, dan menganggap diri mereka sendiri dan orang lain bertanggung jawab atas perilaku etis.

Karyawan harus dilengkapi dengan pengetahuan dan keterampilan untuk membuat keputusan yang etis. Organisasi dapat menyediakan program pelatihan atau sumber daya yang membantu karyawan memahami pertimbangan etika, menganalisis dilema etika, dan membuat pilihan yang selaras dengan prinsip etika. Saluran komunikasi yang terbuka dan transparan sangat penting untuk implementasi etika. Karyawan harus merasa nyaman melaporkan masalah etika atau mencari panduan saat menghadapi tantangan etika. Organisasi harus menetapkan mekanisme seperti hotline, prosedur pelaporan, atau pejabat pengawas etika yang ditunjuk untuk memfasilitasi komunikasi tersebut.

Implementasi etika melibatkan pemantauan dan penegakan standar etika. Ini termasuk menetapkan mekanisme untuk mengidentifikasi dan mengatasi pelanggaran etika, melakukan penyelidikan bila perlu, dan menerapkan tindakan disipliner yang sesuai untuk pelanggaran. Membangun budaya etis sangat penting untuk implementasi etika yang berkelanjutan. Organisasi harus menumbuhkan lingkungan di mana perilaku etis dihargai, diakui, dan dihargai. Hal ini dapat

dicapai melalui evaluasi kinerja, mempromosikan pengambilan keputusan etis dalam operasi sehari-hari, dan menghargai penerapan etika.

Penerapan etika adalah proses yang berkelanjutan. Organisasi harus secara teratur menilai praktik etika mereka, mencari umpan balik dari karyawan, dan melakukan penyesuaian yang diperlukan untuk memperkuat perilaku etis dan mengatasi tantangan etika yang muncul. Dengan mengutamakan etika di lingkungan kerja, organisasi dapat meningkatkan kepercayaan, integritas, dan perilaku yang bertanggung jawab di antara karyawan, sehingga menumbuhkan lingkungan kerja yang positif dan meningkatkan reputasi mereka di mata para pemangku kepentingan.

11.2. Etika

Etika mengacu pada cabang filsafat yang berhubungan dengan prinsip moral, nilai, dan konsep benar dan salah. Ini mengeksplorasi pertanyaan tentang apa yang dianggap baik atau buruk secara moral, adil atau tidak adil, dan bagaimana individu dan masyarakat harus berperilaku. Etika memberikan kerangka kerja bagi individu dan kelompok untuk mengevaluasi dan memandu tindakan, keputusan, dan perilaku mereka

dengan cara yang bertanggung jawab secara moral. Ini melibatkan refleksi pada prinsip-prinsip seperti kejujuran, integritas, keadilan, rasa hormat, akuntabilitas, dan kasih sayang.

Etika berkaitan dengan mengidentifikasi dan memahami prinsip-prinsip moral dasar yang memandu perilaku manusia. Prinsip-prinsip ini dapat bervariasi lintas budaya dan sistem kepercayaan tetapi sering kali mencakup konsep seperti kejujuran, keadilan, kemurahan hati (berbuat baik), menghindari bahaya, otonomi (menghormati kebebasan dan martabat individu), dan kejujuran. Dilema etika muncul ketika ada pertimbangan moral yang bertentangan atau ketika individu menghadapi pilihan sulit antara prinsip etika yang bersaing. Menyelesaikan dilema etika seringkali membutuhkan analisis yang cermat, pertimbangan konsekuensi, dan menyeimbangkan kepentingan pemangku kepentingan yang berbeda.

Berbagai teori etika memberikan kerangka kerja untuk memahami dan menganalisis masalah etika. Teori-teori ini (Brandenburg, 2021) termasuk konsekuensialisme (berfokus pada hasil atau konsekuensi dari tindakan), deontologi (menekankan kepatuhan pada tugas dan prinsip moral), etika kebajikan (menekankan pengembangan karakter

moral), dan etika perawatan (menekankan pentingnya hubungan dan empati). Etika terapan melibatkan penerapan prinsip dan teori etika ke bidang, profesi, atau konteks tertentu. Contohnya termasuk etika bisnis, etika medis, etika lingkungan, dan bioetika. Etika terapan memeriksa masalah dan dilema etika yang muncul di bidang ini dan berusaha memberikan panduan untuk pengambilan keputusan dan perilaku yang bertanggung jawab.

Etika menekankan gagasan tentang tanggung jawab pribadi dan kolektif. Ini mengakui bahwa individu dan organisasi memiliki kewajiban moral untuk mempertimbangkan konsekuensi dari tindakan mereka, menegakkan standar etika, dan bertanggung jawab atas perilaku mereka. Tanggung jawab etis meluas ke interaksi dengan orang lain, lingkungan, dan masyarakat secara keseluruhan. Etika melibatkan pemikiran kritis dan penalaran untuk mengevaluasi pertanyaan moral dan membuat keputusan yang masuk akal secara etis. Itu membutuhkan pertimbangan berbagai perspektif, prinsip etika, konsekuensi, dan konteks di mana keputusan dibuat. Kepemimpinan etis melibatkan menunjukkan integritas, memberikan contoh, dan mempromosikan perilaku etis dalam organisasi dan komunitas. Pemimpin etis mengutamakan nilai-nilai

moral, menumbuhkan budaya etis, dan menginspirasi orang lain untuk bertindak etis.

Etika adalah bidang yang kompleks dan berkembang, dan diskusi tentang apa yang etis dapat bernuansa dan subyektif. Ini memainkan peran penting dalam membentuk perilaku individu dan kolektif, membimbing norma-norma sosial, dan berkontribusi pada kesejahteraan dan fungsi masyarakat yang harmonis.

11.3. Teknologi Informasi

Teknologi Informasi (TI) mengacu pada penggunaan, pengembangan, dan pengelolaan teknologi, sistem, dan proses untuk menyimpan, mengambil, mengirimkan, dan memanipulasi data dan informasi. Ini mencakup berbagai teknologi, termasuk perangkat keras komputer, perangkat lunak, jaringan, database, dan telekomunikasi.

TI mencakup perangkat keras komputer, yang terdiri dari perangkat fisik seperti komputer, server, laptop, perangkat seluler, perangkat penyimpanan, dan perangkat periferal seperti printer dan pemindai. Komponen-komponen ini membentuk fondasi untuk infrastruktur TI. TI melibatkan aplikasi perangkat lunak yang memungkinkan berbagai fungsi dan operasi. Ini

termasuk sistem operasi, perangkat lunak produktivitas (misalnya, pengolah kata, spreadsheet, dan alat presentasi), sistem manajemen basis data, sistem perencanaan sumber daya perusahaan (ERP), perangkat lunak manajemen hubungan pelanggan (CRM), dan aplikasi khusus untuk industri atau tujuan tertentu.

TI mencakup jaringan dan sistem telekomunikasi yang memfasilitasi komunikasi dan transfer data. Ini termasuk jaringan area lokal (LAN), jaringan area luas (WAN), konektivitas internet, router, sakelar, modem, dan protokol untuk mengirim dan menerima data. TI melibatkan penyimpanan, organisasi, dan pengelolaan data. Ini termasuk sistem basis data, proses pencadangan dan pemulihan data, keamanan data, tata kelola data, dan analitik data untuk mengekstrak wawasan dan membuat keputusan yang tepat.

TI mencakup tindakan dan praktik untuk melindungi informasi dan sistem dari akses, pelanggaran, dan ancaman yang tidak sah. Ini melibatkan penerapan protokol keamanan, teknik enkripsi, firewall, perangkat lunak antivirus, kontrol akses, dan kebijakan keamanan untuk memastikan kerahasiaan, integritas, dan ketersediaan data. TI mencakup fungsi dukungan untuk membantu pengguna dengan masalah teknis, pemecahan masalah,

pemasangan perangkat lunak, pemeliharaan perangkat keras, dan pemutakhiran sistem. Dukungan TI dapat disediakan oleh departemen TI internal atau dialihdayakan ke penyedia layanan eksternal.

TI melibatkan metodologi dan praktik manajemen proyek untuk merencanakan, melaksanakan, dan mengendalikan proyek TI secara efektif. Ini termasuk menentukan tujuan proyek, mengalokasikan sumber daya, mengatur jadwal, dan memastikan keberhasilan implementasi inisiatif TI. TI terus berkembang dengan munculnya teknologi baru. Ini termasuk kemajuan di berbagai bidang seperti komputasi awan, kecerdasan buatan (AI), pembelajaran mesin, *Internet of Things* (IoT), blockchain, virtual reality (VR), dan keamanan siber.

Penerapan Teknologi Informasi tersebar luas dan berdampak pada berbagai sektor dan industri, antara lain bisnis, pendidikan, kesehatan, keuangan, hiburan, komunikasi, dan pemerintahan serta termasuk pendidikan tinggi (Tsarova et al., 2023). TI memainkan peran penting dalam memungkinkan proses yang efisien, memfasilitasi komunikasi, meningkatkan produktivitas, mendukung pengambilan keputusan, dan mendorong inovasi di dunia digital saat ini.

11.4. Lingkungan Kerja

Lingkungan kerja mengacu pada kondisi, lingkungan, dan suasana di mana pekerjaan dilakukan. Ini mencakup berbagai faktor yang dapat memengaruhi kesejahteraan karyawan, kepuasan kerja, produktivitas, dan pengalaman kerja secara keseluruhan. Lingkungan kerja yang positif adalah lingkungan yang mendorong kolaborasi, keterlibatan, dan kepuasan karyawan secara keseluruhan.

Ruang kerja fisik mencakup faktor-faktor seperti tata letak kantor, pencahayaan, suhu, tingkat kebisingan, dan ergonomi. Lingkungan kerja yang ideal menyediakan tempat kerja yang nyaman dan dirancang dengan baik, pencahayaan yang memadai, kontrol suhu yang sesuai, dan langkah-langkah untuk meminimalkan kebisingan atau gangguan yang berlebihan. Budaya organisasi mengacu pada nilai, norma, dan keyakinan bersama yang membentuk cara karyawan berinteraksi dan berperilaku di tempat kerja. Lingkungan kerja yang positif memupuk budaya yang mendukung dan inklusif yang menghargai keragaman, mendorong komunikasi terbuka, mengakui pencapaian, dan mendorong kerja sama tim.

Lingkungan kerja yang sehat mendukung keseimbangan kehidupan-kerja, mengakui pentingnya

kesejahteraan pribadi dan komitmen di luar pekerjaan. Contoh mempromosikan keseimbangan kehidupan kerja termasuk jadwal kerja yang fleksibel, opsi kerja jarak jauh, kebijakan cuti melahirkan, dan inisiatif yang mempromosikan kesehatan karyawan dan manajemen stres.

Komunikasi yang efektif sangat penting dalam lingkungan kerja yang positif. Ini termasuk saluran komunikasi yang terbuka dan transparan, umpan balik reguler dan evaluasi kinerja, ekspektasi yang jelas, dan peluang bagi karyawan untuk menyuarakan pendapat dan kekhawatiran mereka tanpa takut akan pembalasan. Lingkungan kerja yang mendukung memberikan peluang bagi pertumbuhan dan perkembangan profesional karyawan. Ini mungkin termasuk akses ke program pelatihan, pendampingan, peluang peningkatan karir, dan inisiatif pembelajaran berkelanjutan yang membantu karyawan meningkatkan keterampilan dan pengetahuan mereka.

Mendorong kolaborasi dan kerja tim dapat berkontribusi pada lingkungan kerja yang positif. Ini melibatkan pembinaan budaya di mana karyawan didorong untuk bekerja sama, berbagi ide, dan berkontribusi pada tujuan bersama. Ruang kolaboratif, pekerjaan berbasis proyek, dan aktivitas membangun

tim adalah contoh dari pengembangan kerja sama tim. Mengakui dan menghargai kontribusi dan pencapaian karyawan dapat meningkatkan lingkungan kerja. Ini dapat berupa pujian verbal, pengakuan publik, imbalan uang, bonus berbasis kinerja, atau insentif lain yang mengakui dan menghargai upaya dan pencapaian karyawan.

Lingkungan kerja yang aman sangat penting untuk kesejahteraan karyawan. Ini melibatkan penyediaan ruang kerja yang aman dan sehat secara fisik, menerapkan protokol keselamatan, menawarkan pelatihan dan peralatan yang tepat, dan mempromosikan budaya kesadaran keselamatan dan kepatuhan terhadap peraturan kesehatan dan keselamatan kerja. Lingkungan kerja yang positif merangkul keberagaman dan inklusi. Ini menghargai perbedaan individu, mempromosikan kesempatan yang sama, dan memastikan suasana hormat dan inklusif di mana karyawan merasa diterima, dihargai, dan mampu menyumbangkan perspektif unik mereka.

Lingkungan kerja yang positif menjunjung standar etika yang tinggi. Ini termasuk mempromosikan perilaku etis, integritas, dan transparansi dalam semua aspek pekerjaan, serta menerapkan kebijakan etika dan kode etik yang memandu perilaku karyawan. Ini hanyalah

beberapa contoh faktor yang berkontribusi pada lingkungan kerja yang positif. Setiap organisasi mungkin memiliki karakteristik dan praktik uniknya sendiri, tetapi tujuan utamanya adalah untuk menciptakan lingkungan di mana karyawan merasa termotivasi, terlibat, dan didukung dalam pekerjaan mereka.

11.5. Etika Penggunaan Teknologi Yang Berlaku di Lingkungan Kerja

Etika implementasi teknologi di lingkungan kerja mengacu pada pertimbangan dan prinsip etis yang terlibat dalam adopsi, penggunaan, dan pengelolaan teknologi dalam suatu organisasi. Ini berfokus pada memastikan bahwa teknologi diterapkan dan digunakan dengan cara yang bertanggung jawab, adil, dan bermoral. Ini melibatkan penanganan masalah seperti privasi, keamanan data, ekuitas, aksesibilitas, akuntabilitas, dan dampak teknologi pada individu dan masyarakat.

Organisasi perlu mempertimbangkan implikasi etis dari pengumpulan, penyimpanan, dan penggunaan data pribadi dan sensitif. Ini melibatkan penerapan langkah-langkah untuk melindungi hak privasi individu, mendapatkan persetujuan, memberikan transparansi tentang praktik data, dan mematuhi peraturan perlindungan data yang relevan. Implementasi teknologi

etis memerlukan perlindungan data dan sistem terhadap akses tidak sah, pelanggaran, dan ancaman dunia maya. Ini melibatkan penerapan langkah-langkah keamanan yang kuat, protokol enkripsi, kontrol akses, dan memperbarui sistem secara teratur untuk mengurangi risiko dan melindungi informasi sensitif.

Organisasi harus mengupayakan keadilan dan akses yang setara ke sumber daya dan peluang teknologi. Implementasi teknologi yang etis melibatkan pertimbangan kebutuhan pengguna yang beragam, memastikan aksesibilitas bagi penyandang disabilitas, dan meminimalkan kesenjangan digital untuk menghindari memperburuk ketidaksetaraan. Saat menerapkan teknologi AI, pertimbangan etis mencakup transparansi dalam proses pengambilan keputusan AI, mengatasi bias dalam koding, memastikan keadilan dalam sistem otomatis, dan menghindari kerugian atau diskriminasi terhadap individu atau kelompok yang terpinggirkan.

Organisasi harus mempertimbangkan implikasi etis dari pengumpulan dan analisis data dalam jumlah besar. Ini termasuk memastikan bahwa pengumpulan data dibenarkan, bahwa wawasan yang diperoleh dari data digunakan secara bertanggung jawab, dan bahwa privasi dan hak individu dihormati. Penerapan teknologi

pemantauan tempat kerja, seperti perangkat lunak pemantauan karyawan atau sistem pengawasan, menimbulkan masalah etika. Organisasi harus menyeimbangkan kebutuhan pemantauan dengan hak privasi karyawan, menetapkan kebijakan yang jelas, dan mengomunikasikan tujuan dan jangkauan pemantauan kepada karyawan.

Implementasi teknologi etis membutuhkan transparansi dalam bagaimana teknologi digunakan dan dikelola dalam organisasi. Ini melibatkan transparansi tentang praktik data, proses pengambilan keputusan, dan dampak potensial pada karyawan, pelanggan, dan pemangku kepentingan lainnya. Organisasi juga harus menetapkan mekanisme akuntabilitas dan ganti rugi jika terjadi pelanggaran etika. Penerapan teknologi etis melibatkan pertimbangan dampak sosial dan lingkungan yang lebih luas dari penggunaan teknologi. Ini termasuk meminimalkan efek lingkungan yang negatif, memastikan praktik rantai pasokan yang bertanggung jawab, dan menyadari potensi konsekuensi sosial seperti perpindahan pekerjaan atau ketidaksetaraan sosial yang timbul dari adopsi teknologi.

Organisasi harus mempromosikan pengambilan keputusan etis di antara karyawan yang terlibat dalam implementasi teknologi. Ini termasuk memberikan

pedoman, pelatihan, dan dukungan untuk membantu karyawan menavigasi tantangan etika, membuat pilihan berdasarkan informasi, dan menyelaraskan praktik teknologi dengan prinsip etika. Implementasi teknologi etis adalah proses yang berkelanjutan. Organisasi harus secara teratur menilai implikasi etis dari penggunaan teknologi, meminta umpan balik dari pemangku kepentingan, dan membuat penyesuaian yang diperlukan untuk memastikan bahwa teknologi selaras dengan standar dan nilai etika.

Dengan mempertimbangkan etika penerapan teknologi, organisasi dapat memitigasi risiko, melindungi hak individu, menumbuhkan kepercayaan di antara pemangku kepentingan, dan berkontribusi pada penggunaan teknologi yang lebih bertanggung jawab dan berkelanjutan di lingkungan kerja.

11.6. Pelanggaran Etika Penggunaan Teknologi

Pelanggaran etika dalam implementasi teknologi mengacu pada kasus di mana prinsip dan standar etika diabaikan atau dilanggar selama adopsi, penggunaan, atau pengelolaan teknologi dalam suatu organisasi. Pelanggaran ini dapat memiliki konsekuensi negatif bagi individu, organisasi, dan masyarakat secara keseluruhan.

Pelanggaran privasi terjadi ketika organisasi gagal melindungi informasi pribadi individu atau menyalahgunakannya tanpa persetujuan. Ini dapat melibatkan akses tidak sah ke data sensitif, pelanggaran data yang mengakibatkan terungkapnya informasi pribadi, atau praktik berbagi data yang tidak etis yang membahayakan privasi.

Pelanggaran etika dapat terjadi ketika organisasi memanipulasi atau menyalahgunakan data dengan cara yang tidak etis. Ini dapat mencakup dengan sengaja mendistorsi atau salah mengartikan data untuk keuntungan pribadi, menggunakan data dengan cara yang diskriminatif atau bias, atau terlibat dalam praktik penambangan data yang tidak etis tanpa persetujuan atau transparansi yang tepat.

Teknologi pemantauan, jika diterapkan tanpa pertimbangan etis yang tepat, dapat melanggar hak privasi karyawan. Pelanggaran dapat terjadi ketika pemberi kerja melakukan pemantauan atau pengawasan berlebihan tanpa kebijakan yang transparan, tanpa memberi tahu karyawan, atau tanpa alasan yang sah. Organisasi dapat melanggar prinsip etika saat mereka mengumpulkan dan menggunakan data pengguna tanpa pengungkapan yang transparan atau tanpa memberikan kontrol atau persetujuan yang tepat kepada pengguna.

Ini dapat melibatkan pelacakan perilaku pengguna, membuat profil individu tanpa sepengetahuan mereka, atau menggunakan data untuk iklan atau manipulasi yang ditargetkan.

Pelanggaran etika dapat terjadi ketika organisasi gagal bersikap transparan tentang praktik data, proses pengambilan keputusan, atau penggunaan teknologi mereka. Kurangnya transparansi ini dapat mengikis kepercayaan dan mempersulit individu untuk memahami bagaimana data mereka digunakan atau untuk meminta pertanggungjawaban organisasi atas tindakan mereka. Jika organisasi gagal mempertimbangkan dampak sosial dan lingkungan yang lebih luas dari penerapan teknologi, hal itu dapat menyebabkan pelanggaran etika. Ini dapat termasuk berkontribusi terhadap kerusakan lingkungan melalui konsumsi energi yang berlebihan, mengabaikan dampak teknologi pada komunitas yang terpinggirkan, atau gagal mengatasi potensi konsekuensi negatif otomatisasi pada pekerjaan dan kesejahteraan masyarakat.

Organisasi yang lalai menerapkan tindakan dan protokol keamanan yang sesuai dapat membahayakan data sensitif, yang menyebabkan pelanggaran, kehilangan data, atau akses tidak sah. Gagal berinvestasi dalam tindakan keamanan siber yang memadai atau

mengabaikan praktik terbaik keamanan dapat mengakibatkan pelanggaran etika yang signifikan. Pelanggaran etika dapat terjadi ketika organisasi mengabaikan atau mengabaikan untuk mengatasi tantangan etika yang terkait dengan implementasi teknologi. Ini termasuk gagal memberikan pedoman, pelatihan, atau sumber daya yang tepat kepada karyawan untuk menavigasi dilema etika, atau gagal menetapkan mekanisme untuk melaporkan dan menangani masalah etika.

Pelanggaran etika dapat terjadi ketika organisasi mengumpulkan dan menggunakan data pribadi tanpa mendapatkan persetujuan dari individu. Ini dapat melibatkan berbagi data dengan pihak ketiga tanpa izin eksplisit atau menggunakan informasi pribadi untuk tujuan di luar yang disetujui individu. Mengatasi dan mencegah pelanggaran etika dalam implementasi teknologi mengharuskan organisasi untuk memprioritaskan pertimbangan etis, menetapkan pedoman dan kebijakan yang jelas, menyediakan program pelatihan dan kesadaran etis, dan menumbuhkan budaya tanggung jawab etis. Sangat penting untuk menjunjung tinggi prinsip dan nilai etis di seluruh siklus hidup implementasi teknologi untuk

memastikan penggunaan teknologi yang bertanggung jawab dan bermanfaat.

11.7. Dampak Pelanggaran Etika Penggunaan Teknologi di Lingkungan Kerja

Pelanggaran etika di lingkungan kerja dapat menimbulkan dampak negatif yang signifikan terhadap individu, organisasi, dan lingkungan kerja secara keseluruhan. Ketika etika dilanggar, kepercayaan di antara karyawan, manajemen, dan pemangku kepentingan dapat terkikis parah. Ketika individu menyaksikan atau mengalami perilaku tidak etis, hal itu merusak kepercayaan mereka terhadap organisasi dan kepemimpinannya. Hal ini dapat menyebabkan gangguan dalam kolaborasi, komunikasi, dan kerja sama tim.

Pelanggaran etika dapat menciptakan lingkungan kerja yang beracun, menyebabkan penurunan semangat kerja karyawan. Ketika karyawan mengamati perilaku yang tidak etis atau mengalami praktik yang tidak adil, hal itu dapat menyebabkan perasaan demotivasi, sinisme, dan pelepasan. Hal ini, pada gilirannya, dapat berdampak negatif terhadap produktivitas dan kepuasan kerja secara keseluruhan.

Pelanggaran etika dapat secara signifikan merusak reputasi dan kredibilitas organisasi. Berita pelanggaran etika menyebar dengan cepat, berdampak pada persepsi organisasi oleh pelanggan, mitra, investor, dan publik. Reputasi yang ternoda dapat menyebabkan penurunan loyalitas pelanggan, hilangnya peluang bisnis, dan kesulitan menarik dan mempertahankan karyawan berbakat. Pelanggaran etika dapat mengakibatkan konsekuensi hukum dan peraturan bagi organisasi. Pelanggaran undang-undang privasi, peraturan perlindungan data, undang-undang ketenagakerjaan, atau undang-undang antidiskriminasi dapat menyebabkan denda, tuntutan hukum, dan kerusakan pada kedudukan hukum organisasi. Konsekuensi ini dapat memiliki dampak finansial dan operasional yang signifikan.

Lingkungan kerja yang ditandai dengan pelanggaran etika cenderung mengalami perputaran karyawan yang lebih tinggi. Karyawan yang menyaksikan atau mengalami perilaku tidak etis dapat memilih untuk meninggalkan organisasi untuk mencari tempat kerja yang lebih etis dan terhormat. Tingkat perputaran yang tinggi dapat mengganggu kontinuitas, berdampak pada dinamika tim, dan meningkatkan biaya perekrutan dan pelatihan. Pelanggaran etika dapat

mengikis kepercayaan dan loyalitas pelanggan. Pelanggan lebih suka berbisnis dengan organisasi yang menunjukkan praktik etis, menghormati privasi pelanggan, dan bertindak dengan integritas. Ketika pelanggaran etika terungkap, pelanggan dapat kehilangan kepercayaan pada organisasi, yang menyebabkan penurunan loyalitas pelanggan, penurunan penjualan, dan berita negatif dari mulut ke mulut.

Pelanggaran etika dapat menciptakan dilema etika bagi karyawan yang mungkin merasa terpecah antara mengikuti arahan yang tidak etis atau bertindak sejalan dengan keyakinan etis pribadi mereka. Hal ini dapat menyebabkan tekanan moral, konflik batin, dan lingkungan kerja yang dikompromikan di mana karyawan merasa dikompromikan secara moral. Pelanggaran etika dapat merusak hubungan dengan pemangku kepentingan seperti pemasok, mitra, dan masyarakat setempat. Jika sebuah organisasi dianggap tidak etis, pemangku kepentingan dapat menjauhkan diri, memengaruhi kolaborasi, kemitraan, dan dukungan. Membangun kembali hubungan yang rusak dapat menjadi tantangan dan memakan waktu.

Lingkungan kerja yang tercemar oleh pelanggaran etika dapat menghambat inovasi dan kreativitas. Ketika

karyawan terlepas, kehilangan semangat, atau takut untuk berbicara, mereka cenderung tidak menyumbangkan ide-ide baru atau menantang status quo. Hal ini dapat menghambat pertumbuhan, membatasi kemampuan pemecahan masalah, dan menghambat daya saing organisasi. Pelanggaran etika yang berulang dapat menarik peningkatan pengawasan dan pengawasan regulasi. Regulator dapat membuat organisasi melakukan pemantauan, audit, atau penalti yang lebih ketat, yang selanjutnya dapat mengganggu operasi, menghabiskan sumber daya, dan merusak posisi organisasi.

Untuk mengurangi dampak pelanggaran etika, organisasi harus memprioritaskan dan mempromosikan budaya etika yang kuat, menetapkan pedoman dan kebijakan etika yang jelas, memberikan program pelatihan dan kesadaran etika, dan mengembangkan lingkungan di mana karyawan merasa aman untuk menyampaikan kekhawatiran dan melaporkan pelanggaran etika. Dengan menekankan perilaku etis, organisasi dapat mempromosikan lingkungan kerja yang positif, meningkatkan kepercayaan, dan melindungi reputasi mereka.

BAB XII
TANTANGAN ETIKA DI MASA DEPAN TEKNOLOGI

12.1. Pemahaman Tantangan Etika di Era Teknologi Lanjutan

Perkembangan teknologi yang pesat, seperti kecerdasan buatan, komputasi kuantum, dan realitas virtual, telah mengubah cara kita berinteraksi dengan dunia dan satu sama lain. Ini membawa berbagai tantangan etika, seperti:

1. Privasi dan Keamanan Data

   Teknologi baru sering mengumpulkan dan memproses data pribadi dengan cara yang belum pernah terjadi sebelumnya, memunculkan pertanyaan tentang bagaimana melindungi privasi dan mengamankan data.

2. Pengaruh Psikologis

   Teknologi seperti media sosial dapat memiliki dampak psikologis yang signifikan pada pengguna, memunculkan pertanyaan tentang tanggung jawab perusahaan teknologi dalam menjaga kesejahteraan mental pengguna.

3. Penggantian Pekerjaan oleh Otomasi

   Kemajuan dalam kecerdasan buatan dan otomasi dapat mengancam pekerjaan manusia, memunculkan pertanyaan tentang etika penggantian pekerjaan oleh mesin.

Penting untuk mengantisipasi dilema-dilema etika baru yang muncul akibat perkembangan teknologi. Hal ini melibatkan:

a. Pendekatan Etis Proaktif

   Menyadari bahwa teknologi baru dapat memunculkan pertanyaan etika yang belum pernah ada sebelumnya, penting untuk mengembangkan kerangka kerja etis yang siap menghadapi tantangan tersebut.

b. Kolaborasi Multidisiplin

   Mengajak ahli etika, ahli hukum, ilmu sosial, dan pemangku kepentingan lainnya dalam proses pengembangan teknologi dapat membantu mengidentifikasi dan mengatasi potensi dilema etika.

c. Pendidikan Etika Teknologi

   Mendidik para pengembang teknologi dan pengguna tentang implikasi etika dari teknologi

baru dapat membantu menciptakan kesadaran dan tanggung jawab yang lebih besar.

12.2. Etika dalam Era Teknologi Canggih: Landasan dan Pendekatan

Prinsip-prinsip etika universal, seperti keadilan, kemanusiaan, kebenaran, dan penghormatan, memiliki relevansi yang kuat dalam teknologi canggih. Beberapa poin penting adalah:

a. Keadilan dalam Algoritma

   Memastikan bahwa algoritma dan kecerdasan buatan tidak menghasilkan diskriminasi atau ketidaksetaraan yang tidak adil.

b. Kemanusiaan dalam Desain

   Mengintegrasikan nilai-nilai kemanusiaan dalam desain teknologi, termasuk penghormatan terhadap hak asasi manusia dan kebebasan individu.

c. Kebenaran dalam Informasi

   Memastikan integritas dan akurasi informasi yang disebarkan melalui teknologi.

Dalam menghadapi tantangan teknologi canggih, pendekatan etis yang holistik dapat diambil:

1. Antisipasi dan Pencegahan

Mengidentifikasi potensi dampak etis sejak dini dan mengambil langkah-langkah pencegahan yang sesuai.

2. Kolaborasi Multidisiplin

   Melibatkan berbagai disiplin ilmu, termasuk etika, hukum, ilmu sosial, dan teknologi, dalam proses pengembangan dan regulasi.

3. Kode Etik Profesional

   Membangun kode etik yang mengikat bagi para pengembang dan profesional teknologi untuk memastikan bahwa prinsip-prinsip etika diikuti dalam setiap tahap pengembangan.

12.3. Keamanan Data dan Privasi dalam Era Konvergensi Teknologi

Dengan konvergensi berbagai teknologi, data sering kali terhubung dan berpindah antarplatform, menciptakan tantangan keamanan yang serius:

a. Pengintaian dan Pencurian Data

   Integrasi teknologi meningkatkan risiko peretasan dan pencurian data, karena adanya banyak titik masuk potensial.

b. Keamanan Jaringan

Jika data dipertukarkan melalui jaringan yang rentan, risiko penyalahgunaan data menjadi lebih besar.

c. Ketidakcocokan Sistem Keamanan

Berbagai teknologi mungkin memiliki tingkat keamanan yang berbeda, menciptakan potensi celah keamanan saat diintegrasikan.

Privasi Pengguna di Tengah Konvergensi Data

Konvergensi teknologi juga memengaruhi privasi pengguna secara signifikan:

1. Penyatuan Data

   Data dari berbagai sumber dapat digabungkan untuk menghasilkan gambaran yang lebih lengkap tentang pengguna, memunculkan pertanyaan tentang sejauh mana privasi dapat dijaga.

2. Pengawasan yang Tidak Dikenali

   Pengguna mungkin tidak menyadari sejauh mana data mereka digunakan dan berpindah, menciptakan masalah dalam pengendalian privasi.

3. Kontrol Pengguna

Privasi pengguna dapat terancam jika mereka tidak memiliki kendali atas bagaimana data mereka diakses dan digunakan.

12.4. Pembuatan dan Implementasi Kecerdasan Buatan yang Etis

Mengembangkan algoritma AI yang tidak diskriminatif adalah tantangan utama dalam memastikan etika dalam kecerdasan buatan:

a. Bias Data

   Algoritma AI dapat menjadi diskriminatif jika dilatih dengan data yang tidak representatif atau berisi bias tertentu.

b. Reproduksi Bias

   Algoritma yang mempelajari data historis dapat memperkuat bias yang ada dalam data tersebut.

c. Interpretabilitas

   Algoritma kompleks seperti jaringan saraf dapat sulit dijelaskan, membuat sulit untuk mengidentifikasi bagaimana diskriminasi terjadi.

Implementasi AI yang mandiri memunculkan berbagai pertanyaan etis:

1. Kontrol Pengguna

Bagaimana menghadapi situasi di mana AI membuat keputusan tanpa campur tangan manusia? Bagaimana memastikan bahwa pengguna memiliki kontrol atas keputusan yang dibuat AI?

2. Akuntabilitas

   Siapa yang bertanggung jawab jika AI mengambil tindakan yang merugikan? Bagaimana mengembangkan mekanisme akuntabilitas yang jelas?

3. Kepentingan Manusia

   Bagaimana memastikan bahwa AI yang mandiri tidak bertentangan dengan nilai-nilai manusia dan kepentingan masyarakat?

12.5. Etika dalam Interaksi Manusia dengan Teknologi

Dalam interaksi manusia mesin yang semakin dekat, ada beberapa tantangan etika yang perlu diatasi:

a. Kendali dan Kepercayaan

   Bagaimana membangun sistem yang memungkinkan manusia untuk memegang kendali dan merasa percaya terhadap keputusan yang diambil oleh mesin?

b. Transparansi Algoritma

Bagaimana menjelaskan algoritma dan proses pengambilan keputusan mesin kepada manusia agar dapat dipahami dan diverifikasi?

c. Peran Manusia

Bagaimana memastikan bahwa manusia tetap memiliki peran aktif dalam interaksi dengan mesin tanpa merasa tergantikan?

Pertimbangan etis dalam menghadapi potensi penggantian pekerjaan manusia oleh mesin meliputi:

1. Pembangunan Keahlian

   Bagaimana menciptakan peluang untuk pengembangan keahlian baru bagi individu yang mungkin terkena dampak penggantian pekerjaan?

2. Dampak Sosial

   Bagaimana memitigasi dampak sosial dari penggantian pekerjaan, seperti pengangguran struktural dan kerugian ekonomi?Kesejahteraan Manusia: Bagaimana memprioritaskan kesejahteraan dan kualitas hidup manusia dalam menghadapi perubahan signifikan dalam ekonomi dan pekerjaan?

12.6. Tanggung Jawab Sosial Teknologi Terhadap Pengguna

Tanggung jawab sosial teknologi terhadap pengg dalam era digital yang terus berkembang, terdapat beberapa tantangan dalam menjaga kesejahteraan pengguna:

a. Ketergantungan Teknologi

   Bagaimana memastikan pengguna tidak terlalu bergantung pada teknologi dan tetap menjaga keseimbangan dalam kehidupan sehari-hari?

b. Gangguan dan Stres

   Bagaimana mencegah dampak negatif teknologi, seperti gangguan yang mengganggu produktivitas dan stres yang timbul dari terlalu banyak informasi digital?

c. Isolasi Sosial

   Bagaimana teknologi dapat membantu menjaga hubungan sosial dan mencegah isolasi, terutama di tengah konektivitas digital yang meningkat?

Perusahaan teknologi memiliki tanggung jawab etis terhadap pengaruh psikologis pengguna:

1. Desain Etis

Bagaimana mendesain produk dan layanan yang meminimalkan risiko dampak psikologis negatif, seperti adiksi digital?

2. Transparansi dan Kontrol

   Bagaimana memberikan pengguna kontrol atas bagaimana data mereka digunakan dan bagaimana mengurangi ketidaktransparan dalam algoritma yang dapat mempengaruhi keputusan pengguna?

3. Pendidikan Pengguna

   Bagaimana mendidik pengguna tentang pengaruh psikologis potensial dari teknologi, sehingga mereka dapat mengambil keputusan yang lebih bijak?

12.7. Etika dalam Algoritma Pengambilan Keputusan Otomatis

Menghindari bias dan diskriminasi dalam algoritma pengambilan keputusan otomatis adalah tantangan utama dalam etika teknologi:

a. Bias Data

   Bagaimana memastikan bahwa data yang digunakan untuk melatih algoritma bebas dari bias, yang dapat menyebabkan keputusan yang tidak adil?

b. Reproduksi Bias

   Bagaimana mencegah algoritma menghasilkan keputusan yang lebih berat sebelah berdasarkan bias yang ada dalam data pelatihan?

c. Transparansi Algoritma

   Bagaimana menjelaskan bagaimana algoritma mengambil keputusan dan apa yang mempengaruhinya sehingga dapat diaudit dan diperiksa

Dalam algoritma pengambilan keputusan otomatis, peran manusia masih relevan dan memiliki tanggung jawab etis:

1. Pengawasan Manusia

   Bagaimana memastikan bahwa keputusan yang dibuat oleh algoritma masih diawasi dan dapat diperbaiki oleh manusia jika diperlukan?

2. Pelatihan Algoritma

   Bagaimana memastikan bahwa algoritma dilatih dengan panduan etika yang sesuai dan mendukung nilai-nilai manusia?

3. Koreksi Kekeliruan

   Bagaimana mengelola situasi di mana algoritma membuat keputusan yang keliru atau tidak

sesuai, dan mengambil tindakan korektif yang tepat?

12.8. Norma dan Etika dalam Dunia Digital yang Terus Berkembang

Mengembangkan norma digital yang memadai dan sesuai adalah tantangan yang kompleks:

a. Keanekaragaman Kultural

   Bagaimana memastikan norma yang diatur dalam dunia digital mencerminkan keanekaragaman budaya dan nilai-nilai masyarakat yang beragam?

b. Perubahan Cepat

   Bagaimana menghadapi tantangan norma yang terus berkembang seiring dengan perubahan teknologi dan tren digital yang cepat?

c. Kemampuan Penegakan

   Bagaimana memastikan norma digital yang ditetapkan dapat ditegakkan dengan efektif tanpa mengorbankan kebebasan dan fleksibilitas?

Menjaga keseimbangan antara kebebasan ekspresi dan kebijakan normatif merupakan hal penting dalam etika digital:

1. Kebebasan Berbicara

   Bagaimana memastikan kebebasan berbicara dan ekspresi online tanpa merugikan orang lain atau menyebarkan konten berbahaya?

2. Regulasi Konten

   Bagaimana mengembangkan kebijakan regulasi konten yang adil tanpa mengabaikan hak kebebasan ekspresi dan menghindari penyalahgunaan kekuasaan?

3. Responsibilitas Platform

   Bagaimana mengatur tanggung jawab platform digital dalam menjaga norma dan etika dalam konten yang dipublikasikan oleh pengguna?

DAFTAR PUSTAKA

ABBATE, JANET ELLEN. (1994). From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966–1988.

ACM (2018) *ACM Code of Ethics and Professional Conduct*, *Advancing Computing as a Science & Profession*. Available at: https://www.acm.org/code-of-ethics.

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. Computer Science Review, 43, 100452.

Allen, C., & Wallach, W. (2011). Moral machines: Teaching robots right from wrong. Oxford University Press.

Alrefaei AF, Hawsawi YM, Almaleki D et al (2022) *Genetic data sharing and artificial intelligence in the era of personalized medicine based on a cross-sectional analysis of the Saudi human genome program*. Sci Rep 12:1405. https://doi.org/10.1038/s41598-022-05296-7

Al-Saqqa, S., Sawalha, S., & AbdelNabi, H. (2020). Agile software development: Methodologies and trends. International Journal of Interactive Mobile Technologies, 14(11).

Amnesty International. (2022). THE RIGHT TO PRIVACY IN THE DIGITAL AGE. Amnesty International Report.

Anderson, M., & Anderson, S. L. (2011). Machine ethics: Creating an ethical intelligent agent. AI Magazine, 32(4), 74-85.

Anderson, R. (2019). "Ethics and computing." Routledge.

Anderson, R., & Moore, T. (2006). The Cambridge Handbook of Computational Psychology. Cambridge University Press.

Asaro, P. M. (2016). What should we want from a robot ethic?. International Review of Information Ethics, 25, 9-16.

Atzori, L., Iera, A., & Morabito, G. (2010). The *Internet of Things*: A survey. Computer Networks, 54(15), 2787-2805.

Bandyopadhyay, D., & Sen, J. (2011). *Internet of Things*: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and Machine Learning. Course Materials.

Becker HA (2001) *Social impact assessment.* Eur J Oper Res 128:311–321. https://doi.org/10.1016/S0377-2217(00)00074-6

Becker HA, Vanclay F (eds) (2003) *The international handbook of social impact assessment: conceptual and methodological advances*. Edward Elgar Publishing, Cheltenham

Bélanger, F., & Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Q., 35, 1017-1041.

Bello-Orgaz, G., Jung, J. J., & Camacho, D. (2016). Social *big data*: Recent achievements and new challenges. Information Fusion, 28, 45-59.

Bengio Y, Lecun Y, Hinton G (2021) *Deep learning for AI*. Commun ACM 64:58–65. https://doi.org/10.1145/3448250

BERNERS-LEE, TIM, ET AL. (1993). The World Wide Web initiative. [Online] Available from: http://info.cern.ch/hypertext/WWW/TheProject.html

BERNERS-LEE, TIM., CAILLIAU, R., GROFF, J.F., & POLLERMANN, B. (1992). World-Wide Web: the

information universe. Internet Research 2.1. pp. 52–58.

Bishop, M. (2005). Introduction to computer security (Vol. 50). Boston: Addison-Wesley.

Borenstein J, Grodzinsky FS, Howard A et al (2021) *AI ethics: a long history and a recent burst of attention.* Computer 54:96–102. https://doi.org/10.1109/MC.2020.3034950

Borenstein, J., & Townsend, A. (2020). Towards AI ethics: Integrating social concepts into ethical guidelines. *Big data* & Society, 7(2), 2053951720943906.

Borenstein, N. S., & Davis, G. B. (2008). Applying the principles of user-centered design to create a more ethical internet. Journal of Business Ethics, 80(4), 707-715.

Bovaird, T., & Löffler, E. (Eds.). (2003). Public management and governance. Routledge.

Boyd, D., & Crawford, K. (2012). Critical questions for *big data*: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662–679.

Brandenburg, D. (2021). Consequentialism and the Responsibility of Children: A Forward-Looking Distinction between the Responsibility of

Children and Adults. *Monist*, *104*(4), 471–483. https://doi.org/10.1093/monist/onab013

Broy, M. (2016). Engineering and the double edge of technical artifacts. Science and Engineering Ethics, 22(3), 791-806.

Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company.

Brynjolfsson, E., & McAfee, A. (2017). The business of *artificial* intelligence. Harvard Business Review, 95(1), 61-70.

Brynjolfsson, E., Rock, D., & Syverson, C. (2017). *Artificial* intelligence and the modern productivity paradox: A clash of expectations and statistics. NBER Working Paper.

Bryson, J. (2023). The Past Decade and Future of AI's Impact on Society. Towards a New Enlightenment? A Transcendent Decade, 1, 102-119.

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., ... & Henke, N. (2016). Where machines could replace humans—and where they can't (yet). McKinsey Quarterly.

Burton, E., Goldsmith, J., Mattei, N., Siler, C., & Swiatek, S. J. (2023). Computing and Technology Ethics: Engaging through Science Fiction. MIT Press.

Buttarelli G (2017) *Privacy matters: updating human rights for the digital society.* Health Technol 7:325–328. https://doi.org/10.1007/s12553-017-0198-y

Bynum, T. (2016) 'Computer and information ethics', *Stanford Encyclopedia of Philosophy*. Available at: https://plato.stanford.edu/Archives/Fall2012/entries/ethics-computer/.

Bynum, T. W. (2006) 'Flourishing ethics', *Ethics and Information Technology*, 8(4), pp. 157–173. doi: 10.1007/s10676-006-9107-1.

Bynum, T. W., & Rogerson, S. (2003). Computer ethics and professional responsibility: introductory text and readings. Blackwell Publishers, Inc..

California Consumer Privacy Act of 2018. (2018). California Legislative Information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

Calo, R. (2015). Robots and privacy. Harvard Law Review, 2140-2202.

Cavalier, R. J. (2005). Impact of the Internet on Our Moral Lives, The. SUNY Press.

Chui, M., Manyika, J., & Miremadi, M. (2016). Where machines could replace humans—and where they can't (yet). McKinsey Quarterly.

CORBATO FERNANDO, J. & VICTOR A. VYSSOTSKY. (1965). Introduction and overview of the Multics system. Proceedings of the November 30–December 1, 1965, fall joint computer conference, part I. ACM.

Crawford, K., & Schultz, J. (2014). *Big data* and due process: Toward a framework to redress predictive privacy harms. Boston College Law Review, 55(1), 93-128.

Davis, M., & Nathan, L. P. (2018). A new culture of learning: Cultivating the imagination for a world of constant change. Parallax Press.

Dehaye, P., & Zimmer, M. (2019). Privacy and data protection in the digital era: In search of a holistic approach. Journal of Information Policy, 9, 3-37.

Diakopoulos, N. (2016). Accountability in algorithmic decision making. Communications of the ACM, 59(2), 56-62.

DiEugenio, B., & Glass, M. (2018). Ethics in Software Engineering. ACM Inroads, 9(3), 74-78.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the

protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. (2016). Official Journal of the European Union, L 119/89.

Dohr, A., Modre-Osprian, R., Drobics, M., Hayn, D., & Schreier, G. (2010). The *Internet of Things* for Ambient Assisted Living. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 804-809). IEEE.

Edmondson, A. C., & Nembhard, I. M. (2009). Product development and learning in project teams: The challenges are the benefits. Journal of Product Innovation Management, 26(2), 123-138.

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: concepts, technology & architecture*. Pearson Education.

Ess, C. (2017). Digital Media Ethics. John Wiley & Sons.

Ess, C., & Thorseth, M. (2019). Ethical IT innovation: A value-based system design approach. Information Systems Journal, 29(5), 1145-1172.

European Commission. (2021). Data Protection. https://ec.europa.eu/info/law/law-topic/data-protection_en

European Data Protection Supervisor (EDPS). (2018). Privacy and competitiveness in the age of *big data*: The interplay between data protection, competition law and consumer protection in the Digital Economy.

Flanagan, M., Howe, D. C. and Nissenbaum, H. (2008) 'Embodying Values in Technology: Theory and Practice', in *Information Technology and Moral Philosophy*. Cambridge University Press, pp. 322–353. doi: 10.1017/CBO9780511498725.017.

Fleischmann, K. R., Wallace, W. A., & Lawrence, J. A. (Eds.). (2017). Ethics, law, and aging review, Volume 11: De-Identification. Springer Publishing Company.

Floridi, L. (2010). Information: A very short introduction. Oxford University Press.

Floridi, L. (2019). The Ethics of Virtuality. Dalam The Routledge Handbook of Philosophy of Information (pp. 425-435). Routledge.

Metzinger, T. (2018). The Ego Tunnel: The Science of the Mind and the Myth of the Self. Basic Books.

Floridi, L. (Ed.). (2010). The Cambridge Handbook of Information and Computer Ethics. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511845239

Floridi, L. and Sanders, J. W. (2005) *Internet Ethics: the Constructionist Values of Homo Poieticus*, *The Impact of the Internet on Our Moral Lives*. Suny. Available at: http://web.comlab.ox.ac.uk/oucl/research/areas/ie.

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360.

Friedman, B., & Kahn Jr, P. H. (2003). Human values, ethics, and design. ACM interactions, 10(2), 38-53.

Friedman, B., & Nissenbaum, H. (2016). Bias in computer systems. ACM Transactions on Information Systems (TOIS), 14(3), 330-347.

Gotterbarn, D. (1991) 'Computer ethics: responsibility regained', *National Forum*, 71(3), p. 26. Available at: https://www.proquest.com/openview/fdd917c9e0dbb6018e73d2e11d53229f/1?pq-origsite=gscholar&cbl=1820941.

Gotterbarn, D. (2001). Software engineering code of ethics. ACM SIGCAS Computers and Society, 31(1), 5-32.

Gotterbarn, D. (2012). Software engineering code of ethics. Encyclopedia of Applied Ethics, 3, 311-320.

Gotterbarn, D. *et al.* (2018) 'THINKING PROFESSIONALLYThe continual evolution of interest in computing ethics', *ACMInroads*, 9(2), pp. 10–12. doi: 10.1145/3204466.

Gotterbarn, D. W., Miller, K., & Rogerson, S. (2017). Software engineering code of ethics: The evolution of a living document. Journal of Software: Evolution and Process, 29(8), e1866.

Gotterbarn, D., & Rogerson, S. (2011). "Software Engineering Code of Ethics." ACM SIGCAS Computers and Society, 41(1), 16-27.

Gotterbarn, D., Miller, K., Rogerson, S., Barber, S., Barnes, P., Burnstein, I., ... & Fulghum, M. (2001). Software engineering code of ethics and professional practice.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). *Internet of Things* (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

Gürses, S., van Hoboken, J., & Micklitz, H. (Eds.). (2018). Understanding the GDPR: A practical guide to data protection law. Intersentia.

Hall, M. (2020). Research ethics: Deontological perspectives. Shanlax Int. J. Arts Sci. Humanit, 7, 1-6.

Harris, T. (2016). How Technology Hijacks People's Minds — from a Magician and Google's Design Ethicist. Medium Article.

Helbing, D. *et al.* (2019) 'Will Democracy Survive *Big data* and *Artificial* Intelligence?: Essays on the Dark and Light Sides of the Digital Revolution', in Helbing, D. (ed.) *Towards Digital Enlightenment*.

Springer, pp. 73–98. Available at: https://www.research-collection.ethz.ch/handle/20.500.11850/338754.

Hesselgreaves, H., & Robertson, I. (Eds.). (2014). User engagement in public transport. Emerald Group Publishing.

Himma, K. E., & Tavani, H. T. (Eds.). (2015). The handbook of information and computer ethics. John Wiley & Sons.

https://www.instagram.com/p/CtS9hiDpogs/?igshid=MzRlODBiNWFlZA==

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2009). Risk IT Practitioner Guide. [Online] Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

INFORMATION SYSTEMS SECURITY ASSOCIATION & DONN B. PARKER. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. Volume 8 Issue 7, July 2010. ISSA Journal. [Online] Available from: http://www.bluetoad.com/publication/?i=41813&page=1

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2014). ISO/IEC 27000:2014 -Information technology—Security techniques—Information security management systems—Overview and vocabulary. [Online] Available from: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

Johnson, D. (2008) *Computer Ethics*. 4th edn. Pearson.

Johnson, D. G. (2016). Computer ethics (4th ed.). Pearson.

Johnson, D. G. (2019). Computer Ethics. Stanford Encyclopedia of Philosophy.

Johnson, D. G., & Nissenbaum, H. (1995). "Computer Ethics." Prentice Hall.

Koontz, L. (2017). Information privacy in the evolving healthcare environment. CRC Press.

Koshy, P., & Waterman, H. (2013). Engaging service users in health and social care: a critical perspective. Oxford University Press.

Kranzberg, M. (2020) *Ethics In An Age Of Pervasive Technology*. 1st edn. Routledge.

Kumar, A. and Braud, T. (2020) 'Trustworthy AI in the Age of Pervasive Computing and *Big data*', in *2020 IEEE International Conference on Pervasive*

Computing and Communications Workshops (PerCom Workshops). Computer Science, pp. 1–6. doi: 10.1109/percomworkshops48775.2020.9156127.

Lacity, M. C., & Janson, M. A. (2018). Robotic process automation at Xchanging. Journal of Information Technology Teaching Cases, 8(1), 5-13.

Lee, I., & Lee, K. (2015). The *Internet of Things* (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

Lessig, L. (2006). Code: Version 2.0. Basic Books.

Leurs, K., Ponzanesi, S., & Salman, S. (Eds.). (2018). Digital migration and the margins of Europe: Media, place and belonging. Rowman & Littlefield International.

Levesque, M. J., Etherington, C., Lalonde, M., & Stacey, D. (2022). Interprofessional Collaboration in the OR: A Qualitative Study of Nurses' Perspectives. AORN journal, 116(4), 300-311.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2012). NIST cloud computing reference architecture: Recommendations of the National Institute of Standards and Technology (Special

Publication 500-292). CreateSpace Independent Publishing Platform.

loridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). Unlocking the potential of the *Internet of Things*. McKinsey Global Institute.

Martin, M., & Brown, N. (2013). The Ethical Challenges of Ubiquitous Computing. Ethics and Information Technology, 15(2), 83-96.

Martin, M., & Martin, R. (2017). Agile principles, patterns, and practices in C# (Vol. 1). Pearson Education.

Martin, R. C. (2009). Clean code: A handbook of agile software craftsmanship. Pearson Education.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Metzinger, T. (2018). The Ego Tunnel: The Science of the Mind and the Myth of the Self. Basic Books.

Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big data* & Society, 3(2), 2053951716679679.

Moor, J. H. (1985) 'What is computer ethics', *Metaphilosophy*, 16(4), pp. 266–275. doi: 10.1111/j.1467-9973.1985.tb00173.x.

Munawar, Z. (2023) 'Konsep Dasar Pengkodean', in *Pengantar Tekonologi Informasi*. 1st edn. Bandung: Indie Press, p. 230.

Munawar, Z. and Indah Putri, N. (2020) 'Keamanan Jaringan Komputer Pada Era *Big data*', *J-SIKA|Jurnal Sistem Informasi Karya Anak Bangsa*, 2(1), pp. 14–20. Available at: https://ejournal.unibba.ac.id/index.php/j-sika/article/view/275.

Munawar, Z. and Sastradipraja, C. K. (2023) *Visi Komputer : Konsep, Metode, dan Aplikasi*. 1st edn. Edited by R. Komalasari. Bandung: Kaizen Media Publishing.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2007). Special Publication 800-100: Information Security Handbook: A Guide for Managers–Chapter 8. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Nijssen, S., & Willaert, T. (2019). "The benefits of IT certification: A literature review." Computers in Human Behavior, 101, 57-64.

Nurudin, (2013). Pengantar Komunikasi Massa

Olayinka, O., & Win, T. (2022). Cybersecurity and Data Privacy in the Digital Age: Two Case Examples. In Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies (pp. 117-131). IGI Global.

O'Malley, L., & Hall, T. (2010). Community engagement and public participation in planning: A review of the literature. Cities, 27(6), 416-427.

O'Neil, C. (2016). Weapons of Math Destruction: How *Big data* Increases Inequality and Threatens Democracy. *Big data* & Society, 8(2), 205395172110100.

Prabhumoye, S., Boldt, B., Salakhutdinov, R., & Black, A. W. (2020). Case study: Deontological ethics in NLP. arXiv preprint arXiv:2010.04658.

Pressman, R. S. (2014). "Software Engineering: A Practitioner's Approach." McGraw-Hill Education.

Pretty, J., & Ward, H. (2001). Social capital and the environment. World Development, 29(2), 209-227.

Putri, N. I. *et al.* (2021) 'Teknologi Pendidikan dan Transformasi Digital di Masa', *Jurnal ICT :*

Information Communication & Technology, 20(7), pp. 53–57. Available at: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/306/pdf.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Official Journal of the European Union, L 119/1.

Regulation, G. D. P. (2018). General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October*, *24*(1).

Reidenberg, J. R. (2012). Technology and Internet Law. West Academic.a

Robbins, Scott (2020). AI and the path to envelopment: knowledge as a first step towards the responsible regulation and use of AI-powered machines. AI and Society 35 (2):391-400.

Sastradipraja, C. K. and Munawar, Z. (2022) *Konsep Dasar Teknologi Web*. 1st edn. Bandung: Kaizen Media Publishing.

Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company.A

Schulz-Knappe, C., Koch, T., & Beckert, J. (2019). The importance of communicating change: Identifying predictors for support and resistance toward organizational change processes. Corporate Communications: An International Journal, 24(4), 670-685.

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. Fordham Law Review, 87(3), 1085-1124.

SOFTWARE ENGINEERING INSTITUTE. (2005). OCTAVE–S Implementation Guide, Version 1. [Online] Available from: http://resources.sei.cmu.edu/library/assetview.cfm?assetid=6795

Solove, D. J. (2012). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880-1969.

Sommerville, I., & Craig, N. (2012). Software engineering (9th ed.). Pearson.

Spinello, R. A., & Tavani, H. T. (Eds.). (2007). Readings in cyberethics (2nd ed.). Jones & Bartlett Learning.

Staff, E. (2020) *Five Data Ethics Considerations for 2020*, *eWeek*. Available at: https://www.eweek.com/it-management/five-data-ethics-considerations-for-2020/.

Stahl BC, Rodrigues R, Santiago N, Macnish K (2022) *A European agency for artificial intelligence: protecting fundamental rights and ethical values. Comput Law Secur* Rev45:105661. https://doi.org/10.1016/j.clsr.2022.105661

Stallings, W., & Brown, L. (2013). Computer Security: Principles and Practice (4th ed.). Pearson.

Stephen W, L & Foss, K. (2022). Enklopedia Teori Komunikasi.

Steuer, J. (1992). Defining virtual reality: Dimensions determining telepresence. Journal of Communication, 42(4), 73-93.

Slater, M., & Wilbur, S. (1997). A framework for immersive virtual environments (FIVE): Speculations on the role of presence in virtual environments. Presence: Teleoperators and Virtual Environments, 6(6), 603-616.

Stewart, M. M., & Mueller, M. P. (2015). Engaging the public in transportation decision making: Effective practices from around the world.

Transportation Research Circular, (E-C197), 1-18.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the *Internet of Things*. Cluster of European Research Projects on the *Internet of Things*.

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.

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

Telefonica, R. (2018) *Engineering Science : Fundamentals of Computing*, *UNIVERSITA' DEGLI STUDI ROMA*. Available at: https://engineering-sciences.uniroma2.it/wp-content/uploads/2020/01/Fundamentals-of-Computing.png.

Thomas, E., Zaigham, M., & Ricardo, P. (2013). *Cloud computing concepts, technology & architecture*. Prentice Hall.

Tsarova, Y., Alekseiko, V., Sabadosh, Y., Kushnir, A., & Yaroshuk, D. (2023). The role of information technologies in education. *Revista Amazonia Investiga*, *12*(61), 122–130. https://doi.org/10.34069/ai/2023.61.01.13

Uchjana Onong, E. (2005). Ilmu, Teori dan Filsafat Komunikasi.

UMESH R HODEGHATTA, UMESHA NAYAK (2014). *The InfoSec Handbook: An Introduction to Information Security 1st ed. Edition,* Publisher Apress New York

United Nations Human Rights Council. (2019). The right to privacy in the digital age. A/HRC/RES/34/7.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., & Bassi, A. (2011). *Internet of Things* Strategic Research Roadmap. The IoT European Research Cluster (IERC).

Voigt, T., Schlieter, H., Zibuschka, J., & Feldhorst, S. (2018). The dark side of IoT: The social, economic, and psychological consequences of the IoT revolution. In Proceedings of the 51st Hawaii International Conference on System Sciences.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Wandersman, A., & Florin, P. (2000). Citizen participation and community organizations. Annual Review of Psychology, 51(1), 427-451.

Warburton, J., & Hughey, K. F. (Eds.). (2017). Participation in community work: International perspectives. Routledge.

Webb, H., Ceppi, S. and Patel, M. (2018) 'It would be pretty immoral to choose a random algorithm', *Information, Communication and Ethics in Society*, 17(2), p. 25. doi: 10.1108/JICES-11-2018-0092.

Weizenbaum, J. (1976) *Computer Power and Human Reason: From Judgment to Calculation*. 1st edn. W H Freeman & Co.

Wilkins, L & Christians, C. (2008). The Handbook of mass Media Ethics.

World Bank. (2020). World Development Report 2021: Data for Better Lives. Washington, DC: World Bank.

Young, K. S., & de Abreu, C. N. (2011). Internet Addiction: A Handbook and Guide to Evaluation and Treatment. John Wiley & Sons.

Brey, P. (2016). Ethical reflections on the good life with emerging technologies. In The Good Life in a Technological Age (pp. 77-90). Routledge.

Zhang, C., Zhu, W., Dai, J., Wu, Y., & Chen, X. (2023). Ethical impact of *artificial* intelligence in managerial

accounting. International Journal of Accounting Information Systems, 49, 100619.

Zhao, L., Wang, Q., Zou, Q., Zhang, Y., & Chen, Y. (2019). Privacy-preserving collaborative deep learning with unreliable participants. IEEE Transactions on Information Forensics and Security, 15, 1486-1500.

Zikopoulos, P., & Eaton, C. (2011). *Understanding big data: Analytics for enterprise class hadoop and streaming data*. McGraw-Hill Osborne Media.

Zuber, N., Kacianka, S., & Gogoll, J. (2022). *Big data* ethics, machine ethics or information ethics? Navigating the maze of applied ethics in IT. arXiv preprint arXiv:2203.13494.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zwitter, A. (2014). *Big data* ethics. *Big data & Society*, *1*(2), 2053951714559253.

Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. Journal of International Humanitarian Action, 3(1), 16.

ETIKA DALAM ILMU KOMPUTER

Dalam dunia yang semakin terhubung dan didorong oleh teknologi, peran ilmu komputer tidak dapat diragukan lagi. Namun, di tengah kemajuan yang pesat ini, terbangun pula pertanyaan etika yang mendalam.

Buku ini lahir dari keinginan kami untuk merangkai pemahaman tentang etika dalam konteks ilmu komputer, sebuah perpaduan antara etika klasik dan tantangan yang unik di dunia digital. Kami menjelajahi pertanyaan-pertanyaan kompleks tentang privasi data, kecerdasan buatan, keamanan siber, hak kekayaan intelektual, dan dampak sosial dari teknologi informasi.

Kami membuka jendela ke dunia refleksi moral dan keputusan etis yang harus dihadapi oleh para profesional dan pengguna teknologi. Kami berharap bahwa buku ini akan membantu para pembaca, baik itu mahasiswa ilmu komputer, praktisi teknologi, atau masyarakat umum, untuk menggali sudut pandang yang mendalam tentang implikasi etis dalam dunia yang semakin terhubung ini.

IKAPI
IKATAN PENERBIT INDONESIA

Penerbit Yayasan Cendikia Mulia Mandiri

ISBN 978-623-8382-11-8