

DIGITAL CITIZENSHIP

Etika, Literasi, dan Tanggung Jawab di Dunia Maya

Oleh

Prof Ir Rudy C Tarumingkeng, PhD

www.rudycr.com/cv.pdf

Institut Bisnis dan Multimedia (IBM ASMI)

RudyCT Academic Series 2026

ARTIKEL ILMIAH

Digital Citizenship

Etika, Literasi, dan Tanggung Jawab di Dunia Maya

“Menjadi warga digital yang cerdas berarti menggunakan teknologi dengan etika, memahami informasi dengan kritis, melindungi privasi, serta berkontribusi positif bagi masyarakat.”

4 PILAR KEWARGANEGARAAN DIGITAL



Etika Digital

Bersikap jujur, sopan, dan bertanggung jawab dalam berinteraksi di dunia maya.



Literasi Media & AI

Memahami, menganalisis, dan memverifikasi informasi secara kritis serta bijak menggunakan AI.



Privasi dan Keamanan

Melindungi data pribadi, menjaga keamanan akun, dan waspada terhadap ancaman digital.



Tanggung Jawab Sosial

Berpartisipasi positif, menghargai perbedaan, dan membangun komunitas digital yang sehat.



Oleh:

Prof Ir Rudy C Tarumingkeng, PhD



www.rudycr.com/cv.pdf



IBM-ASMI (Institut Bisnis dan Multimedia)



Pakar di bidang Teknologi, Bisnis,
dan Transformasi Digital



Abstrak

Digital citizenship atau kewargaan digital adalah kapasitas individu dan komunitas untuk hidup, belajar, bekerja, berpartisipasi, dan mengambil keputusan secara bermakna dalam lingkungan yang semakin dimediasi teknologi digital. Konsep ini melampaui kemampuan teknis menggunakan perangkat. Ia mencakup literasi informasi, literasi media dan AI, etika komunikasi, perlindungan privasi, keamanan siber, kesehatan digital, penghormatan terhadap hak orang lain, partisipasi publik, tanggung jawab hukum, serta kemampuan menilai dampak sosial dari algoritma dan platform. Artikel ini mengembangkan kerangka naratif-komprehensif yang menempatkan digital citizenship sebagai kompetensi abad ke-21 sekaligus sebagai bagian dari pembentukan karakter warga. Pembahasan menautkan perspektif pendidikan, manajemen, komunikasi, hukum, psikologi, tata kelola platform, demokrasi, dan kecerdasan artifisial. Dalam konteks Indonesia, urgensinya diperkuat oleh perluasan konektivitas, meningkatnya aktivitas ekonomi digital, tantangan disinformasi, perlindungan data pribadi, perubahan Undang-Undang Informasi dan Transaksi Elektronik, serta kebutuhan literasi digital yang lebih merata. Artikel menegaskan bahwa warga digital yang baik bukan sekadar pengguna yang patuh, tetapi subjek yang kritis, etis, aman, produktif, inklusif, dan mampu mempertanggungjawabkan jejak serta konsekuensi tindakannya di ruang digital.

Kata Kunci

digital citizenship; kewargaan digital; etika digital; literasi digital; literasi media dan informasi; privasi; keamanan siber; kecerdasan artifisial; disinformasi; tanggung jawab digital; pendidikan; tata kelola platform.

Pendahuluan

Kehidupan manusia kontemporer tidak lagi dapat dipisahkan secara tegas antara dunia “daring” dan “luring”. Komunikasi keluarga, pendidikan, pekerjaan, transaksi ekonomi, pelayanan publik, hiburan, ekspresi politik, bahkan pembentukan identitas berlangsung melalui ekosistem yang saling terhubung. Dalam situasi demikian, istilah digital citizenship menjadi penting karena teknologi tidak hanya menyediakan alat, tetapi membentuk ruang sosial baru tempat hak, kewajiban, nilai, konflik, reputasi, dan kekuasaan diproduksi serta dinegosiasikan. Seorang warga digital bukan hanya seseorang yang memiliki telepon pintar atau akun media sosial. Ia adalah individu yang memahami konsekuensi dari tindakan digitalnya terhadap diri sendiri, orang lain, organisasi, dan masyarakat luas.

Perubahan ini semakin terasa ketika kecerdasan artifisial generatif memasuki aktivitas sehari-hari. Teks, gambar, audio, dan video dapat dibuat atau dimodifikasi dengan sangat cepat; pekerjaan intelektual dapat dibantu mesin; rekomendasi platform semakin personal; dan keputusan yang dahulu diambil manusia mulai didukung atau dimediasi algoritma. Di satu sisi, kondisi ini

memperluas akses pengetahuan, kreativitas, dan produktivitas. Di sisi lain, muncul persoalan baru: atribusi karya, bias algoritmik, deepfake, manipulasi informasi, ketergantungan kognitif, pelanggaran privasi, serta kesulitan membedakan autentisitas dari sintesis. Karena itu literasi digital perlu bergerak dari sekadar “mampu memakai teknologi” menuju “mampu menilai, mengendalikan, dan mempertanggungjawabkan penggunaan teknologi”.

Dalam pendidikan kewargaan digital, salah satu kerangka yang berpengaruh adalah pendekatan yang menggabungkan akses, komunikasi, literasi, etiket, hukum, hak dan tanggung jawab, kesehatan, keamanan, dan aktivitas ekonomi digital. Perkembangan literatur kemudian memperluas perhatian dari kepatuhan dan keselamatan menuju partisipasi kritis, keadilan, pemberdayaan, serta kemampuan warga memahami arsitektur kekuasaan platform. Definisi mutakhir juga menekankan bahwa digital citizenship merupakan norma yang terus berkembang tentang penggunaan teknologi yang tepat, bertanggung jawab, dan memberdayakan. Dengan demikian, kewargaan digital bersifat dinamis: standar perilaku yang memadai hari ini dapat menjadi tidak cukup ketika teknologi, regulasi, dan norma sosial berubah.

Bagi Indonesia, pembicaraan mengenai kewargaan digital mempunyai dimensi strategis. Negara kepulauan dengan keragaman sosial, ekonomi, pendidikan, dan geografis menghadapi paradoks digital: konektivitas dapat mempersempit jarak tetapi juga menciptakan kesenjangan baru; media sosial dapat memperkuat partisipasi tetapi juga polarisasi; ekonomi digital dapat membuka peluang namun memperbesar risiko penipuan; dan AI dapat meningkatkan produktivitas tetapi berpotensi menimbulkan ketimpangan kompetensi. Karena itu pembangunan masyarakat digital perlu memadukan infrastruktur, literasi, pemberdayaan, kesempatan kerja, etika, serta perlindungan hak. Indeks Masyarakat Digital Indonesia 2025 sendiri menggunakan pilar Infrastruktur dan Ekosistem, Literasi Digital, Pemberdayaan, serta Pekerjaan sebagai dimensi utama pengukuran masyarakat digital.

Artikel ini bertolak dari tesis bahwa kewargaan digital harus dipahami sebagai kemampuan etis-kritis untuk menjadi manusia yang bertanggung jawab di lingkungan yang dimediasi teknologi. Tanggung jawab itu memiliki sedikitnya empat arah: tanggung jawab kepada diri sendiri, kepada orang lain, kepada institusi atau komunitas, dan kepada ruang publik. Pada tingkat individu, ia menyangkut keamanan, kesehatan, dan integritas. Pada tingkat relasional, ia menyangkut empati, penghormatan, dan persetujuan. Pada tingkat organisasi, ia menyangkut tata kelola data, transparansi, dan akuntabilitas. Pada tingkat publik, ia menyangkut kebenaran informasi, partisipasi demokratis, inklusi, serta keadilan digital. Kerangka empat arah ini digunakan sepanjang artikel untuk menghubungkan konsep dengan praktik.

Peta Konseptual Artikel

Dimensi	Pertanyaan Utama	Contoh Isu
Etika	Apa yang seharusnya dilakukan?	empati, integritas, consent, keadilan, atribusi

Literasi	Apa yang perlu dipahami dan diuji?	sumber, algoritma, AI, data, bias, verifikasi
Tanggung jawab	Siapa menanggung konsekuensi?	jejak digital, keamanan, hukum, akuntabilitas
Hak	Apa yang harus dilindungi?	privasi, kebebasan berekspresi, akses, keamanan
Partisipasi	Bagaimana warga berkontribusi?	dialog publik, kolaborasi, civic engagement
Kesejahteraan	Bagaimana teknologi dijaga tetap manusiawi?	atensi, screen time, kesehatan mental

1. Hakikat Digital Citizenship

Pembahasan mengenai hakikat digital citizenship perlu dimulai dari digital citizenship sebagai status sosial, kompetensi, praktik, dan karakter. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Choi, Glassman, & Cristol, 2017). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah reduksi kewargaan digital menjadi sekadar kemampuan teknis menggunakan gawai. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan,

menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, hakikat digital citizenship memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ng, 2012).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan mahasiswa yang mahir aplikasi tetapi tidak memeriksa sumber, tidak menjaga privasi, dan mudah membagikan konten. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah pendidikan tinggi perlu menggabungkan kecakapan digital dengan penalaran etis dan refleksi kewargaan. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta,

identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, hakikat digital citizenship sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

2. Dari Digital Literacy ke Digital Citizenship

Pembahasan mengenai dari digital literacy ke digital citizenship perlu dimulai dari peralihan dari keterampilan operasional menuju pemahaman kritis dan tanggung jawab. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Jones & Mitchell, 2016). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah anggapan bahwa kemampuan mencari informasi identik dengan kemampuan menilai kebenaran. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, dari digital literacy ke digital citizenship memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (UNESCO, 2024).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pengguna yang cepat menemukan jawaban melalui mesin pencari atau AI tetapi gagal membedakan bukti, opini, iklan, dan manipulasi. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif:

memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah kurikulum perlu menilai proses verifikasi, bukan hanya kecepatan memperoleh informasi. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, dari digital literacy ke digital citizenship sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital

bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

3. Etika sebagai Fondasi Perilaku Digital

Pembahasan mengenai etika sebagai fondasi perilaku digital perlu dimulai dari prinsip martabat manusia, tidak merugikan, keadilan, otonomi, kejujuran, dan kepedulian. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Livingstone, 2004). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah jarak psikologis di ruang daring yang dapat menurunkan empati dan meningkatkan perilaku impulsif. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, etika sebagai fondasi perilaku digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan

sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (OECD, 2025).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan komentar agresif terhadap orang yang tidak dikenal karena pengguna merasa tidak berhadapan langsung dengan korban. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah organisasi perlu memiliki kode perilaku digital yang diterjemahkan menjadi kebiasaan, bukan sekadar dokumen. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak

digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, etika sebagai fondasi perilaku digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

4. Literasi Informasi dan Verifikasi Kebenaran

Pembahasan mengenai literasi informasi dan verifikasi kebenaran perlu dimulai dari kemampuan menemukan, menilai, membandingkan, menafsirkan, dan menggunakan informasi secara bertanggung jawab. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ng, 2012). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah information overload dan kecenderungan memilih informasi yang menguatkan keyakinan awal. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-

gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, literasi informasi dan verifikasi kebenaran memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ribble, 2015).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan berita viral dengan judul provokatif dibagikan sebelum pengguna membuka sumber asli. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata

sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah setiap keputusan penting memerlukan disiplin verifikasi lintas sumber dan penelusuran bukti primer. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, literasi informasi dan verifikasi kebenaran sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

5. Literasi Media dan Ekonomi Perhatian

Pembahasan mengenai literasi media dan ekonomi perhatian perlu dimulai dari pemahaman tentang bagaimana media membingkai realitas dan bagaimana platform mengoptimalkan keterlibatan.

Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (UNESCO, 2024). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah insentif ekonomi platform yang mendorong konten sensasional, emosional, dan mudah dibagikan. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, literasi media dan ekonomi perhatian memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Floridi et al., 2018).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pengguna mengira linimasa adalah cerminan netral masyarakat padahal merupakan hasil seleksi algoritmik. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang

hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah pendidikan media perlu mengajarkan model bisnis platform, desain persuasif, dan mekanisme rekomendasi. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik

dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, literasi media dan ekonomi perhatian sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

6. Literasi Algoritmik

Pembahasan mengenai literasi algoritmik perlu dimulai dari kemampuan memahami bahwa keputusan digital sering dipengaruhi sistem rekomendasi dan pemeringkatan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (OECD, 2025). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah ketidakjelasan kriteria algoritmik dan kecenderungan pengguna menganggap hasil sistem sebagai objektif. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering

memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, literasi algoritmik memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Choi, Glassman, & Cristol, 2017).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pelamar kerja atau konsumen menerima rekomendasi yang berbeda akibat profil perilaku yang dibentuk dari data. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah manajer perlu memahami bias data, keterbatasan model, dan kebutuhan human oversight. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko,

pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, literasi algoritmik sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

7. Literasi AI dan Generative AI

Pembahasan mengenai literasi ai dan generative ai perlu dimulai dari kemampuan menggunakan AI secara produktif sambil memahami probabilitas, bias, halusinasi, dan keterbatasan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ribble, 2015). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah anthropomorphism dan automation bias yang membuat keluaran AI dianggap sebagai pengetahuan pasti. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, literasi AI dan generative AI memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Jones & Mitchell, 2016).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan mahasiswa menyerahkan tugas yang dibuat AI tanpa verifikasi, sitasi, atau kontribusi intelektual yang jelas. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif:

memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah AI perlu diposisikan sebagai alat bantu penalaran dan produktivitas, bukan pengganti tanggung jawab manusia. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, literasi ai dan generative ai sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata

pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

8. Privasi dan Pelindungan Data Pribadi

Pembahasan mengenai privasi dan pelindungan data pribadi perlu dimulai dari hak individu mengendalikan konteks pengumpulan, penggunaan, pembagian, dan penyimpanan data. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Floridi et al., 2018). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah normalisasi pengumpulan data berlebihan karena layanan digital tampak gratis dan nyaman. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, privasi dan pelindungan data pribadi memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data,

keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Livingstone, 2004).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan aplikasi meminta akses kontak, lokasi, kamera, atau mikrofon yang tidak sebanding dengan fungsi layanan. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah organisasi harus menerapkan minimisasi data, tujuan yang jelas, keamanan, dan akuntabilitas pemrosesan. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan

multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, privasi dan perlindungan data pribadi sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

9. Keamanan Siber sebagai Kebiasaan Warga

Pembahasan mengenai keamanan siber sebagai kebiasaan warga perlu dimulai dari praktik melindungi identitas, perangkat, akun, data, dan jaringan dari penyalahgunaan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Choi, Glassman, & Cristol, 2017). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah keamanan diperlakukan sebagai urusan teknis padahal banyak insiden bermula dari perilaku pengguna. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas

untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, keamanan siber sebagai kebiasaan warga memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ng, 2012).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan tautan phishing menyerupai pesan resmi dan memanfaatkan urgensi psikologis untuk mencuri kredensial. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata

sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah budaya keamanan perlu dibangun melalui autentikasi kuat, pembaruan, verifikasi, dan pelaporan insiden. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, keamanan siber sebagai kebiasaan warga sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

10. Jejak Digital, Reputasi, dan Identitas

Pembahasan mengenai jejak digital, reputasi, dan identitas perlu dimulai dari kesadaran bahwa tindakan digital meninggalkan rekam yang dapat direplikasi, dikontekstualkan ulang, dan dipakai

menilai seseorang. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Jones & Mitchell, 2016). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah perbedaan antara spontanitas komunikasi dan persistensi arsip digital. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijakan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, jejak digital, reputasi, dan identitas memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (UNESCO, 2024).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan unggahan lama seorang calon pemimpin organisasi kembali muncul dan memengaruhi penilaian publik. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan

ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah setiap pengguna perlu mengelola jejak digital sebagai bagian dari integritas dan reputasi jangka panjang. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang

memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, jejak digital, reputasi, dan identitas sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

11. Etiket Digital dan Empati

Pembahasan mengenai etiket digital dan empati perlu dimulai dari norma interaksi yang menjaga penghormatan, konteks, kesantunan, dan kemanusiaan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Livingstone, 2004). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah komunikasi berbasis teks mengurangi isyarat nonverbal sehingga salah tafsir mudah terjadi. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, etiket digital dan empati memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (OECD, 2025).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan kritik yang seharusnya mengenai gagasan berubah menjadi serangan personal karena percakapan memanas. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah netiquette perlu dipahami sebagai mekanisme menjaga kualitas dialog, bukan formalitas kesopanan. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, etiket digital dan empati sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

12. Cyberbullying, Harassment, dan Kekerasan Berbasis Digital

Pembahasan mengenai cyberbullying, harassment, dan kekerasan berbasis digital perlu dimulai dari perlindungan individu dari penghinaan berulang, intimidasi, doxing, ancaman, dan eksploitasi. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ng, 2012). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah skalabilitas serangan digital yang memungkinkan satu tindakan menyebar kepada ribuan orang. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir

mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, cyberbullying, harassment, dan kekerasan berbasis digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ribble, 2015).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pelajar mengalami tekanan karena meme penghinaan beredar lintas kelompok dan tidak berhenti di lingkungan sekolah. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung

jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah institusi perlu memiliki mekanisme pencegahan, pelaporan, dukungan korban, dan pemulihan yang jelas. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, cyberbullying, harassment, dan kekerasan berbasis digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

13. Disinformasi, Misinformasi, dan Manipulasi

Pembahasan mengenai disinformasi, misinformasi, dan manipulasi perlu dimulai dari kemampuan membedakan kesalahan informasi, manipulasi sengaja, propaganda, satire, dan konteks yang menyesatkan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (UNESCO, 2024). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah kecepatan distribusi informasi sering melampaui kecepatan verifikasi. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, disinformasi, misinformasi, dan manipulasi memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Floridi et al., 2018).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan potongan video tanpa konteks memicu kemarahan, lalu narasi koreksi tidak pernah menjangkau audiens yang sama. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif

kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah warga digital perlu mengembangkan kebiasaan berhenti, memeriksa, membandingkan, dan menilai motif. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut

pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, disinformasi, misinformasi, dan manipulasi sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

14. Deepfake dan Krisis Autentisitas

Pembahasan mengenai deepfake dan krisis autentisitas perlu dimulai dari tantangan verifikasi ketika audio-visual sintetik makin sulit dibedakan dari rekaman asli. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (OECD, 2025). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah erosinya kepercayaan tidak hanya karena konten palsu, tetapi karena konten asli pun dapat dituduh palsu. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika

juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, deepfake dan krisis autentisitas memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Choi, Glassman, & Cristol, 2017).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan rekaman suara tiruan digunakan untuk menipu staf keuangan agar mentransfer dana. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah organisasi perlu menggabungkan prosedur verifikasi identitas, provenance, dan literasi media sintetik. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana

merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, deepfake dan krisis autentisitas sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

15. Hak Digital dan Kebebasan Berekspresi

Pembahasan mengenai hak digital dan kebebasan berekspresi perlu dimulai dari keseimbangan antara kebebasan menyampaikan pandangan, hak atas keamanan, martabat, dan tanggung jawab hukum. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar

daftar keterampilan (Ribble, 2015). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah anggapan bahwa kebebasan berekspresi berarti kebebasan dari konsekuensi sosial maupun institusional. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, hak digital dan kebebasan berekspresi memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Jones & Mitchell, 2016).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan perdebatan publik berubah menjadi konflik ketika batas antara kritik, fitnah, ancaman, dan satire tidak dipahami. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan

digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah pendidikan kewargaan digital harus mengajarkan hak bersamaan dengan kewajiban dan proportionality. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, hak digital dan kebebasan berekspresi sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap

melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

16. Hukum Digital dan Tanggung Jawab di Indonesia

Pembahasan mengenai hukum digital dan tanggung jawab di Indonesia perlu dimulai dari pemahaman bahwa tindakan daring berada dalam kerangka hukum, bukan ruang tanpa aturan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Floridi et al., 2018). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah ketidaktahuan pengguna terhadap konsekuensi hukum pemrosesan data, transaksi, penghinaan, penipuan, dan akses ilegal. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, hukum digital dan tanggung jawab di Indonesia memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna

menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Livingstone, 2004).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan organisasi menyimpan data pelanggan tanpa tata kelola yang jelas atau membagikan informasi melalui kanal tidak aman. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah kepatuhan perlu dipadukan dengan etika karena tidak semua tindakan yang legal otomatis bijaksana. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan

kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, hukum digital dan tanggung jawab di Indonesia sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

17. Kesehatan dan Kesejahteraan Digital

Pembahasan mengenai kesehatan dan kesejahteraan digital perlu dimulai dari pengelolaan waktu, perhatian, tidur, emosi, postur, relasi, dan keseimbangan aktivitas. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Choi, Glassman, & Cristol, 2017). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah desain platform dapat mendorong penggunaan berkepanjangan melalui notifikasi dan infinite scroll. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat

menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, kesehatan dan kesejahteraan digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ng, 2012).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pekerja sulit memutuskan keterhubungan karena pesan pekerjaan masuk hingga larut malam. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata

sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah organisasi perlu membangun norma digital well-being dan hak untuk memiliki waktu pemulihan. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, kesehatan dan kesejahteraan digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

18. Digital Citizenship di Pendidikan Dasar dan Menengah

Pembahasan mengenai digital citizenship di pendidikan dasar dan menengah perlu dimulai dari pembentukan kebiasaan aman, etis, kritis, dan bertahap sesuai perkembangan usia. Dalam

kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Jones & Mitchell, 2016). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah larangan tanpa pendidikan dapat memindahkan risiko tanpa membangun kemampuan. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, digital citizenship di pendidikan dasar dan menengah memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (UNESCO, 2024).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan murid dilarang menggunakan ponsel tetapi tidak pernah belajar mengenali manipulasi, phishing, atau privasi. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan

ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah sekolah perlu menggabungkan pengajaran eksplisit, keteladanan, praktik, dan keterlibatan keluarga. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang

memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, digital citizenship di pendidikan dasar dan menengah sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

19. Digital Citizenship di Perguruan Tinggi

Pembahasan mengenai digital citizenship di perguruan tinggi perlu dimulai dari integritas akademik, kebebasan intelektual, kolaborasi, penelitian, data, dan penggunaan AI. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Livingstone, 2004). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah kemudahan reproduksi informasi dapat mengaburkan batas antara belajar, mengutip, merangkum, dan plagiarisme. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan,

menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, digital citizenship di perguruan tinggi memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (OECD, 2025).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan mahasiswa memakai AI untuk menyusun tinjauan pustaka dengan referensi yang tidak pernah diverifikasi. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah universitas memerlukan kebijakan AI yang jelas sekaligus pedagogi yang menilai proses berpikir. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko,

pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, digital citizenship di perguruan tinggi sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

20. Digital Citizenship di Tempat Kerja

Pembahasan mengenai digital citizenship di tempat kerja perlu dimulai dari perilaku profesional dalam komunikasi, data, keamanan, AI, kolaborasi, dan representasi organisasi. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ng, 2012). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah batas antara akun pribadi dan identitas profesional semakin kabur. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, digital citizenship di tempat kerja memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ribble, 2015).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pegawai mengunggah foto layar rapat yang tanpa sengaja memperlihatkan informasi rahasia. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah perusahaan perlu mengembangkan digital code of conduct dan pelatihan berbasis skenario. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, digital citizenship di tempat kerja sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

21. Kepemimpinan dan Tata Kelola Digital

Pembahasan mengenai kepemimpinan dan tata kelola digital perlu dimulai dari tanggung jawab pemimpin memastikan teknologi selaras dengan nilai, risiko, hukum, dan tujuan organisasi. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (UNESCO, 2024). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah transformasi digital sering diperlakukan sebagai proyek teknologi dan mengabaikan tata kelola manusia. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, kepemimpinan dan tata kelola digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Floridi et al., 2018).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan sistem AI diadopsi karena efisiensi tanpa evaluasi dampak terhadap kelompok yang dirugikan. Secara teknis, tindakan awal

mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah pemimpin perlu membentuk struktur akuntabilitas, evaluasi risiko, dan jalur eskalasi. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut

pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, kepemimpinan dan tata kelola digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

22. Inklusi, Akses, dan Kesenjangan Digital

Pembahasan mengenai inklusi, akses, dan kesenjangan digital perlu dimulai dari keadilan dalam memperoleh konektivitas, perangkat, keterampilan, aksesibilitas, dan kesempatan. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (OECD, 2025). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah kesenjangan digital tidak berhenti setelah seseorang terkoneksi karena kualitas akses dan kompetensi berbeda. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya,

dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, inklusi, akses, dan kesenjangan digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Choi, Glassman, & Cristol, 2017).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan pelayanan publik dipindahkan daring tetapi sebagian warga tidak memiliki perangkat, jaringan, atau kemampuan memadai. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah transformasi digital harus menyediakan alternatif, desain universal, dan dukungan bagi kelompok rentan. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu

informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, inklusi, akses, dan kesenjangan digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

23. Budaya Digital Indonesia

Pembahasan mengenai budaya digital Indonesia perlu dimulai dari penerapan nilai kebangsaan, gotong royong, penghormatan terhadap keberagaman, dan tanggung jawab komunal. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital

citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ribble, 2015). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah platform global membawa norma interaksi yang tidak selalu selaras dengan konteks lokal. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, budaya digital Indonesia memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Jones & Mitchell, 2016).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan perbedaan agama, etnis, wilayah, dan pilihan politik mudah dipolitisasi dalam percakapan digital. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan

digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah budaya digital perlu menggabungkan keterbukaan global dengan etika hidup bersama dalam masyarakat majemuk. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, budaya digital Indonesia sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data

meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

24. Partisipasi Demokratis dan Civic Engagement

Pembahasan mengenai partisipasi demokratis dan civic engagement perlu dimulai dari penggunaan teknologi untuk memperoleh informasi publik, berdialog, mengorganisasi, mengawasi, dan berpartisipasi. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Floridi et al., 2018). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah partisipasi dapat menjadi dangkal ketika hanya diukur melalui klik, like, atau kemarahan viral. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, partisipasi demokratis dan civic engagement memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media,

data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Livingstone, 2004).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan petisi daring menghasilkan perhatian tetapi tidak selalu diikuti pemahaman kebijakan atau tindakan berkelanjutan. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah kewargaan digital yang matang menghubungkan ekspresi daring dengan deliberasi, bukti, dan tindakan nyata. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan

multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, partisipasi demokratis dan civic engagement sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

25. Ekonomi Digital dan Konsumen Bertanggung Jawab

Pembahasan mengenai ekonomi digital dan konsumen bertanggung jawab perlu dimulai dari kecakapan bertransaksi, memahami hak konsumen, menjaga keamanan pembayaran, dan menilai praktik platform. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Choi, Glassman, & Cristol, 2017). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah kenyamanan one-click purchase dapat mengurangi kehati-hatian dan meningkatkan impulsivitas. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas

untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, ekonomi digital dan konsumen bertanggung jawab memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ng, 2012).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan konsumen tertipu toko palsu karena harga ekstrem dan tekanan waktu promosi. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata

sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah literasi ekonomi digital harus mencakup verifikasi penjual, perlindungan akun, privasi, dan jejak transaksi. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, ekonomi digital dan konsumen bertanggung jawab sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

26. Keluarga dan Pengasuhan Digital

Pembahasan mengenai keluarga dan pengasuhan digital perlu dimulai dari peran keluarga membangun dialog, batas, keteladanan, kepercayaan, dan kemampuan menghadapi risiko. Dalam

kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Jones & Mitchell, 2016). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah pengawasan total dapat merusak kepercayaan sedangkan kebebasan tanpa pendampingan meningkatkan risiko. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, keluarga dan pengasuhan digital memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (UNESCO, 2024).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan orang tua memberikan perangkat kepada anak tanpa aturan privasi, waktu, konten, atau pelaporan masalah. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang

hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah pendampingan digital perlu berkembang sejalan dengan usia dan peningkatan otonomi anak. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik

dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, keluarga dan pengasuhan digital sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

27. Menuju Kerangka Digital Citizenship 5.0

Pembahasan mengenai menuju kerangka digital citizenship 5.0 perlu dimulai dari integrasi human-centered technology, AI literacy, etika, keberlanjutan, dan kecerdasan sosial. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Livingstone, 2004). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah kecepatan inovasi membuat kurikulum keterampilan cepat usang jika tidak dibangun di atas prinsip yang tahan lama. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan,

menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, menuju kerangka digital citizenship 5.0 memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (OECD, 2025).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan organisasi mengejar otomatisasi tetapi kemudian menghadapi krisis kepercayaan karena keputusan tidak transparan. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif: memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah kerangka masa depan harus berorientasi pada manusia, adaptif, berbasis hak, dan mampu diaudit. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta,

identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, menuju kerangka digital citizenship 5.0 sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

28. Agenda Strategis Indonesia 2030-2045

Pembahasan mengenai agenda strategis indonesia 2030-2045 perlu dimulai dari penguatan masyarakat digital yang inklusif, aman, produktif, kritis, dan demokratis. Dalam kerangka kewargaan digital, kompetensi tidak pernah berdiri sendiri. Pengetahuan teknis memperoleh makna ketika dihubungkan dengan pertimbangan moral, konteks sosial, dan konsekuensi tindakan. Karena itu, ukuran keberhasilan bukan sekadar apakah seseorang dapat melakukan sesuatu dengan teknologi, tetapi apakah ia memahami kapan tindakan tersebut layak dilakukan, kepada siapa dampaknya tertuju, risiko apa yang timbul, dan bagaimana ia dapat mempertanggungjawabkan keputusan itu. Perspektif ini sejalan dengan literatur yang melihat digital citizenship sebagai kombinasi praktik, norma, partisipasi, dan kemampuan kritis, bukan sekadar daftar keterampilan (Ng, 2012). Di titik inilah teknologi berubah dari benda netral menjadi bagian dari ekologi kehidupan manusia.

Tantangan utama pada tema ini adalah pembangunan infrastruktur yang tidak diikuti literasi dan tata kelola dapat memperluas skala risiko. Masalah tersebut memperlihatkan adanya jarak antara kompetensi instrumental dan kebijaksanaan penggunaan. Orang dapat sangat mahir mengoperasikan platform tetapi tetap rentan terhadap bias, manipulasi, impulsivitas, atau keputusan yang merugikan. Dalam banyak kasus, teknologi justru memperbesar efek dari kebiasaan manusia yang sudah ada: prasangka dapat diperluas oleh algoritma rekomendasi, gosip dapat menjadi viral, kecerobohan dapat berubah menjadi kebocoran data, dan keputusan yang tergesa-gesa dapat terdokumentasi permanen. Karena itu, kewargaan digital harus membangun kapasitas untuk berhenti sejenak, membaca konteks, menguji asumsi, dan mempertimbangkan dampak sebelum bertindak.

Dimensi etis menuntut pertanyaan yang lebih mendalam daripada “boleh atau tidak boleh”. Warga digital perlu bertanya apakah sebuah tindakan menghormati martabat dan otonomi orang lain, apakah distribusi manfaat dan risikonya adil, apakah informasi yang dipakai cukup dapat dipercaya, dan apakah pihak yang terkena dampak memiliki kesempatan untuk memahami serta menolak. Etika juga mengharuskan perhatian pada asimetri kekuasaan: platform, institusi, dan pemilik data sering memiliki kemampuan yang jauh lebih besar daripada pengguna biasa untuk mengumpulkan, menganalisis, dan memengaruhi perilaku. Karena itu tanggung jawab tidak boleh dibebankan hanya kepada individu; desain sistem dan tata kelola organisasi juga harus dinilai.

Dari sudut literasi, agenda strategis Indonesia 2030-2045 memerlukan kemampuan membaca bukan hanya isi pesan tetapi juga struktur yang memproduksinya. Pengguna perlu memahami sumber, konteks, tujuan, model bisnis, data yang dikumpulkan, kemungkinan bias, dan cara algoritma menyusun pengalaman digital. Literasi semacam ini bersifat reflektif: pengguna menyadari bahwa apa yang muncul di layar bukan representasi lengkap dunia. Ia merupakan hasil seleksi teknis dan sosial. Literasi digital yang matang karena itu menggabungkan keterampilan informasi, media, data, keamanan, dan AI, serta kemampuan menghubungkan semuanya dengan penilaian etis (Ribble, 2015).

Sebuah ilustrasi sederhana dapat memperjelas persoalan. Bayangkan desa dengan konektivitas baru memperoleh peluang ekonomi namun sekaligus menghadapi penipuan, informasi palsu, dan eksploitasi data. Secara teknis, tindakan awal mungkin tampak biasa dan bahkan efisien. Namun ketika dianalisis dengan perspektif kewargaan digital, muncul pertanyaan tentang akurasi, persetujuan, privasi, fairness, keamanan, dan dampak jangka panjang. Kasus seperti ini penting dalam pendidikan karena dilema digital jarang hadir dalam bentuk hitam-putih. Sering kali pengguna menghadapi trade-off antara kecepatan dan ketelitian, kenyamanan dan privasi, keterbukaan dan keamanan, kebebasan berekspresi dan penghormatan terhadap orang lain, atau inovasi dan kehati-hatian.

Tanggung jawab personal pada tema ini berarti mengakui bahwa tindakan digital mempunyai jejak dan konsekuensi. Prinsip sederhana yang berguna adalah memperlakukan setiap unggahan, klik, keputusan berbagi, dan penggunaan AI sebagai tindakan yang berpotensi dilihat kembali, direplikasi, diinterpretasikan ulang, atau dipakai oleh pihak lain. Ini bukan alasan untuk hidup dalam ketakutan digital. Sebaliknya, kesadaran tersebut membantu pengguna membangun kebiasaan deliberatif:

memeriksa penerima, menilai sensitivitas informasi, menyimpan bukti ketika perlu, menggunakan kanal yang tepat, dan membedakan ruang privat dari ruang publik.

Tanggung jawab institusional lebih luas. Sekolah, universitas, perusahaan, pemerintah, media, dan platform memiliki kewajiban membentuk lingkungan yang memungkinkan perilaku bertanggung jawab. Kebijakan yang baik tidak cukup berisi larangan, karena pengguna akan menghadapi situasi baru yang tidak tercantum dalam aturan. Institusi perlu menyediakan prinsip, contoh kasus, prosedur pelaporan, dukungan teknis, dan mekanisme evaluasi. Yang terpenting, kebijakan harus konsisten dengan praktik pimpinan. Organisasi yang menyerukan keamanan tetapi membiarkan kata sandi dibagi bersama, atau yang mengajarkan privasi tetapi mengumpulkan data secara berlebihan, sedang mengirim pesan etis yang kontradiktif.

Dalam konteks pendidikan dan manajemen, implikasinya adalah agenda nasional perlu menyatukan pendidikan, regulasi, industri, keluarga, masyarakat sipil, dan riset. Pendekatan berbasis skenario lebih efektif untuk banyak topik digital karena mahasiswa atau karyawan dipaksa menimbang beberapa nilai sekaligus. Misalnya, mereka dapat diminta memutuskan apakah suatu informasi boleh dibagikan, bagaimana memverifikasi klaim, kapan AI boleh dipakai, atau bagaimana merespons percakapan yang berubah menjadi agresif. Tujuan latihan bukan menghasilkan satu jawaban mekanis, melainkan membangun pola berpikir: identifikasi pihak terkait, cek fakta, identifikasi risiko, pertimbangkan hak, cari pilihan yang paling proporsional, dokumentasikan alasan, lalu evaluasi dampaknya.

Pengukuran kompetensi juga harus melampaui tes pengetahuan. Seseorang dapat mengetahui bahwa phishing berbahaya tetapi tetap mengklik tautan ketika berada di bawah tekanan waktu. Ia dapat memahami privasi tetapi menerima semua izin aplikasi karena ingin segera menggunakan layanan. Karena itu indikator kewargaan digital perlu mencakup pengetahuan, sikap, kebiasaan, dan kemampuan menerapkan prinsip dalam situasi nyata. Portofolio, simulasi, refleksi kasus, audit jejak digital, dan observasi perilaku dapat melengkapi kuesioner. Dalam penelitian, pendekatan multidimensi membantu membedakan antara apa yang orang katakan mereka lakukan dan apa yang benar-benar mereka lakukan.

Perkembangan AI memperkuat urgensi tema ini. Sistem generatif dapat meningkatkan kecepatan pembuatan konten, tetapi juga menurunkan biaya produksi manipulasi. Sistem rekomendasi dapat membantu menemukan informasi relevan, tetapi sekaligus mempersempit paparan pada sudut pandang alternatif. Otomatisasi dapat meningkatkan konsistensi keputusan, tetapi juga mewariskan bias dari data historis. Dalam situasi tersebut, warga digital memerlukan sikap yang tidak teknofobik dan tidak pula teknoutopis. Teknologi harus dinilai berdasarkan tujuan, bukti, risiko, siapa yang memperoleh manfaat, siapa yang mungkin dirugikan, dan apakah tersedia mekanisme koreksi ketika sistem keliru.

Akhirnya, agenda strategis Indonesia 2030-2045 sebaiknya dipandang sebagai bagian dari pembentukan karakter kewargaan. Karakter digital tercermin ketika seseorang tetap jujur meskipun plagiarisme mudah dilakukan, tetap menghormati orang lain ketika anonimitas memberi perlindungan, tetap memverifikasi informasi ketika berita sesuai dengan preferensinya, dan tetap melindungi data meskipun prosedur keamanan terasa merepotkan. Pada level ini, kewargaan digital

bukan mata pelajaran tambahan, melainkan cara hidup dalam masyarakat yang makin terdigitalisasi. Ia menggabungkan kecakapan dengan kebijaksanaan dan kebebasan dengan tanggung jawab.

29. Model Kompetensi Digital Citizenship Terpadu

Model terpadu yang diusulkan dalam artikel ini terdiri atas enam domain yang saling mengunci: ACCESS, LITERACY, ETHICS, SAFETY, PARTICIPATION, dan WELL-BEING. ACCESS mencakup kemampuan memperoleh akses yang layak dan menggunakan layanan secara inklusif. LITERACY mencakup informasi, media, data, algoritma, dan AI. ETHICS mencakup integritas, empati, fairness, consent, dan penghormatan terhadap martabat manusia. SAFETY mencakup privasi, keamanan akun, perlindungan perangkat, serta mitigasi risiko. PARTICIPATION menyangkut kontribusi produktif, kolaborasi, demokrasi, dan tanggung jawab dalam komunitas. WELL-BEING menempatkan kesehatan fisik, mental, sosial, dan keseimbangan atensi sebagai bagian dari kompetensi, bukan urusan tambahan.

Keenam domain tersebut perlu dinilai melalui empat tingkat kematangan. Tingkat pertama adalah awareness, ketika individu mengenali istilah dan risiko dasar. Tingkat kedua adalah competent use, ketika ia dapat menerapkan prosedur dalam situasi umum. Tingkat ketiga adalah critical judgment, ketika ia mampu menangani situasi ambigu, konflik nilai, dan informasi tidak lengkap. Tingkat keempat adalah stewardship, ketika ia tidak hanya bertanggung jawab terhadap dirinya tetapi juga membantu membangun ekosistem yang lebih aman, etis, inklusif, dan produktif. Konsep stewardship penting bagi dosen, pemimpin, manajer, orang tua, dan pembuat kebijakan karena mereka memiliki pengaruh terhadap pilihan orang lain.

Kematangan kewargaan digital juga dapat dibaca melalui empat lingkaran tanggung jawab. Lingkaran diri menekankan keamanan, kesehatan, identitas, dan integritas. Lingkaran relasi menekankan consent, empati, penghormatan, dan komunikasi. Lingkaran organisasi menekankan governance, keamanan, data, transparansi, dan akuntabilitas. Lingkaran masyarakat menekankan keadilan, demokrasi, budaya, hak asasi, dan kepentingan publik. Banyak kegagalan digital terjadi ketika keputusan hanya dianalisis pada lingkaran pertama. Contohnya, seseorang mungkin merasa aman membagikan foto kelompok, tetapi mengabaikan hak privasi orang lain atau kebijakan institusi.

Dari perspektif pedagogis, model ini dapat diterjemahkan ke dalam siklus belajar lima langkah: EXPLORE, VERIFY, REFLECT, ACT, dan REVIEW. Peserta didik mula-mula mengeksplorasi teknologi dan konteks; kemudian memverifikasi sumber, data, dan klaim; setelah itu merefleksikan nilai dan pihak yang terdampak; berikutnya bertindak dengan pilihan yang proporsional; terakhir meninjau hasil dan memperbaiki kebiasaan. Siklus ini cocok untuk pembelajaran berbasis proyek karena tidak memisahkan literasi dari etika. Misalnya, mahasiswa yang menggunakan AI untuk riset tidak cukup diminta menghasilkan tulisan, tetapi harus menjelaskan sumber, prompt, verifikasi, kontribusi manusia, dan keterbatasan hasil.

Dalam organisasi, kerangka yang sama dapat dikembangkan menjadi governance cycle: DEFINE, ASSESS, CONTROL, MONITOR, dan LEARN. Organisasi mendefinisikan tujuan penggunaan

teknologi; menilai risiko dan pihak terdampak; menerapkan kontrol; memantau hasil; lalu belajar dari insiden dan umpan balik. Kerangka ini membantu menjembatani kewargaan digital individu dengan tanggung jawab korporasi. Ketika perusahaan menggunakan sistem otomatis untuk menilai pelanggan atau pegawai, misalnya, tanggung jawab tidak dapat dialihkan kepada vendor atau algoritma. Manajemen tetap berkewajiban memahami tujuan, data, fairness, mekanisme banding, dan kemungkinan konsekuensi yang tidak diinginkan.

30. Instrumen Praktis untuk Pendidikan dan Organisasi

- **Checklist sebelum membagikan informasi:** Apakah sumbernya jelas? Apakah informasi sudah dibaca utuh? Apakah ada bukti primer? Apakah konteksnya lengkap? Apakah pembagian informasi dapat merugikan orang lain? Apakah saya bersedia mempertanggungjawabkannya bila dilihat publik?
- **Checklist penggunaan AI:** Apa tujuan penggunaan AI? Data apa yang dimasukkan? Apakah ada data sensitif? Bagaimana keluaran diverifikasi? Apakah sumber dapat ditelusuri? Bagaimana kontribusi manusia dijelaskan? Apakah ada bias atau kelompok yang mungkin dirugikan?
- **Checklist keamanan akun:** Gunakan kata sandi unik, pengelola kata sandi bila memungkinkan, autentikasi multi-faktor, pembaruan perangkat lunak, kewaspadaan terhadap phishing, dan prosedur pemulihan akun.
- **Checklist komunikasi digital:** Periksa penerima, nada, konteks, sensitivitas lampiran, kebutuhan membalas semua orang, serta kemungkinan pesan ditafsirkan tanpa isyarat nonverbal.
- **Checklist privasi:** Kumpulkan dan bagikan data minimum; pahami tujuan; tinjau izin aplikasi; hindari membagikan identitas sensitif tanpa kebutuhan; dan hapus data ketika tidak lagi diperlukan.

Instrumen di atas tidak dimaksudkan sebagai aturan kaku. Tujuannya adalah membangun friction yang sehat sebelum tindakan digital yang berisiko. Dalam desain teknologi modern, banyak antarmuka justru berusaha mengurangi friction agar pengguna cepat mengklik, membeli, mengunggah, atau menyetujui. Dalam konteks kewargaan digital, sedikit jeda dapat menjadi mekanisme etis. Jeda memungkinkan verifikasi, koreksi penerima, pembacaan izin, atau pertimbangan ulang terhadap komentar emosional. Karena itu organisasi dan pendidik dapat merancang “moment of reflection” dalam prosedur kerja maupun aktivitas belajar.

Evaluasi dapat dilakukan dengan rubrik empat dimensi: accuracy, ethics, safety, dan accountability. Accuracy menilai kualitas bukti dan verifikasi. Ethics menilai penghormatan terhadap hak, fairness, dan dampak. Safety menilai privasi serta keamanan. Accountability menilai apakah individu dapat menjelaskan proses dan menerima koreksi. Rubrik seperti ini lebih sesuai untuk era AI dibanding penilaian yang hanya melihat produk akhir. Dua tulisan dapat sama baiknya secara bahasa, tetapi kualitas kewargaan digitalnya berbeda bila satu dibuat dengan verifikasi dan atribusi yang jujur sedangkan yang lain mengandalkan keluaran AI tanpa pemeriksaan.

Bagi perguruan tinggi, kewargaan digital idealnya tidak diajarkan hanya dalam satu mata kuliah. Prinsip-prinsipnya perlu diintegrasikan ke metodologi penelitian, komunikasi bisnis, manajemen SDM, pemasaran, sistem informasi, kewirausahaan, dan strategi. Mahasiswa manajemen, misalnya, perlu memahami bahwa keputusan digital menyangkut stakeholders, reputasi, data, bias, risiko operasional, dan kepercayaan. Dengan demikian digital citizenship menjadi bagian dari professional formation: bagaimana seseorang menggunakan kekuasaan, informasi, dan teknologi secara bertanggung jawab ketika kelak memimpin organisasi.

31. Rekomendasi Kebijakan dan Implementasi

1. Menempatkan kewargaan digital sebagai kompetensi lintas kurikulum dari pendidikan dasar hingga perguruan tinggi, dengan tingkat kompleksitas yang berkembang sesuai usia dan konteks.
2. Memperkuat literasi media, informasi, data, algoritma, dan AI secara terintegrasi; bukan sebagai program terpisah yang saling tidak terhubung.
3. Menjadikan etika digital sebagai praktik berbasis kasus, refleksi, dan kebiasaan; bukan sekadar sosialisasi aturan.
4. Memperluas edukasi perlindungan data pribadi dan keamanan siber kepada masyarakat, UMKM, organisasi pendidikan, dan aparaturnya publik.
5. Mendorong tata kelola AI yang human-centered, transparan, dapat diaudit, memperhatikan fairness, privasi, keamanan, dan mekanisme koreksi.
6. Memperkuat kolaborasi pemerintah, platform, sekolah, universitas, keluarga, dunia usaha, media, dan masyarakat sipil untuk menghadapi disinformasi dan kekerasan digital.
7. Mengembangkan indikator kewargaan digital yang mengukur perilaku dan kemampuan memecahkan dilema, bukan hanya pengetahuan deklaratif.
8. Menjamin inklusi melalui aksesibilitas, dukungan bagi kelompok rentan, pilihan layanan non-digital bila diperlukan, dan penguatan kompetensi di daerah.
9. Mengembangkan budaya organisasi yang memberi contoh keamanan, privasi, integritas akademik/profesional, serta penggunaan AI yang bertanggung jawab.
10. Memperbarui program literasi digital secara berkala mengikuti perubahan teknologi, namun mempertahankan prinsip dasar: martabat manusia, kebenaran, keadilan, keamanan, kebebasan yang bertanggung jawab, dan kepentingan publik.

Penutup

Digital citizenship adalah proyek pendidikan dan kebudayaan jangka panjang. Ia tidak selesai ketika masyarakat memiliki koneksi internet, mampu mengoperasikan aplikasi, atau terbiasa bertransaksi secara daring. Kewargaan digital baru matang ketika kemampuan teknis terhubung dengan nalar kritis, karakter etis, kesadaran hukum, keamanan, empati, kesehatan, dan tanggung jawab publik. Dengan cara pandang ini, teknologi tidak ditempatkan sebagai pusat, melainkan sebagai lingkungan yang harus ditata agar memperkuat kemanusiaan.

Tantangan masa depan justru akan semakin kompleks karena batas antara konten manusia dan konten mesin menjadi kabur, algoritma semakin menentukan visibilitas informasi, dan data menjadi sumber daya ekonomi serta politik. Dalam kondisi tersebut, kebijakan saja tidak cukup; literasi saja tidak cukup; etika personal saja juga tidak cukup. Yang diperlukan adalah ekosistem yang menyatukan individu cakap, institusi bertanggung jawab, platform yang dapat dimintai akuntabilitas, regulasi yang adaptif, dan budaya publik yang menghargai kebenaran serta martabat manusia.

Bagi Indonesia, kewargaan digital dapat menjadi salah satu fondasi penting menuju masyarakat maju pada 2045. Konektivitas yang luas perlu ditransformasikan menjadi kapabilitas; kapabilitas perlu diarahkan oleh etika; dan etika perlu diwujudkan dalam tanggung jawab bersama. Pada akhirnya pertanyaan terpenting bukan seberapa canggih teknologi yang dimiliki, melainkan manusia seperti apa yang dibentuk ketika teknologi itu digunakan setiap hari. Warga digital yang baik adalah warga yang mampu menggunakan teknologi untuk belajar, bekerja, mencipta, berdialog, dan berpartisipasi tanpa kehilangan integritas, empati, kebebasan berpikir, serta tanggung jawab terhadap sesama.

Lampiran Analitis: Studi Kasus Digital Citizenship

Kasus 1: AI Generatif dan Integritas Akademik

Kasus 1: AI Generatif dan Integritas Akademik memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah seorang mahasiswa program pascasarjana menggunakan AI generatif untuk menyusun rancangan makalah. AI menghasilkan struktur yang baik, tetapi beberapa referensi ternyata tidak ada dan beberapa klaim terlalu umum. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: integritas akademik, verifikasi sumber, atribusi, transparansi penggunaan AI, dan tanggung jawab intelektual. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam perguruan tinggi, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip *stewardship* menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi,

membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 1: ai generatif dan integritas akademik adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur

kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 2: Phishing dan Social Engineering di Organisasi

Kasus 2: Phishing dan Social Engineering di Organisasi memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah seorang pegawai menerima email yang tampak berasal dari direktur keuangan dan diminta membuka dokumen pembayaran melalui tautan yang menyerupai portal perusahaan. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: keamanan siber, tekanan psikologis, verifikasi identitas, budaya pelaporan, dan desain prosedur. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam perusahaan, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat

mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 2: phishing dan social engineering di organisasi adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 3: Deepfake Suara dan Fraud

Kasus 3: Deepfake Suara dan Fraud memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah staf keuangan menerima panggilan suara yang sangat mirip dengan pimpinan dan diminta melakukan transfer mendesak kepada rekening baru. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: autentisitas, verifikasi berlapis, deepfake, tata kelola transaksi, dan human oversight. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam organisasi, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 3: deepfake suara dan fraud adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 4: Cyberbullying di Sekolah

Kasus 4: Cyberbullying di Sekolah memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah sebuah foto siswa diedit menjadi meme penghinaan lalu beredar di grup kelas, akun anonim, dan platform video pendek. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: martabat, keselamatan psikologis, tanggung jawab saksi, mekanisme pelaporan, pemulihan korban, dan pendidikan empati. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam sekolah, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai

dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 4: cyberbullying di sekolah adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 5: Data Pelanggan dan Personalisasi

Kasus 5: Data Pelanggan dan Personalisasi memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah sebuah perusahaan ritel digital ingin menggabungkan data transaksi, lokasi, dan perilaku penelusuran untuk membuat promosi yang sangat personal. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: *privacy by design*, minimisasi data, tujuan pemrosesan, *fairness*, transparansi, dan kepercayaan. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam perusahaan, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip *stewardship* menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, *proportionality* sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip *safety by design* dan *privacy by design* lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem

yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 5: data pelanggan dan personalisasi adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 6: Dosen, Media Sosial, dan Reputasi Profesional

Kasus 6: Dosen, Media Sosial, dan Reputasi Profesional memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah seorang dosen menulis komentar emosional di media sosial pribadi mengenai isu publik; potongan komentar kemudian disebarluaskan tanpa konteks dan dikaitkan dengan institusinya. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: kebebasan berekspresi, identitas profesional, konteks, reputasi, hak institusi, dan proporsionalitas. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam perguruan tinggi, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi

keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip *stewardship* menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, *proportionality* sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip *safety by design* dan *privacy by design* lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan *agency* sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa

yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 6: dosen, media sosial, dan reputasi profesional adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 7: Misinformasi Kesehatan dalam Grup Keluarga

Kasus 7: Misinformasi Kesehatan dalam Grup Keluarga memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah pesan berantai tentang terapi kesehatan tanpa bukti ilmiah dibagikan oleh anggota keluarga yang dipercaya, disertai testimoni dan klaim bahwa informasi sengaja disembunyikan. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: literasi informasi, otoritas semu, lateral reading, tanggung jawab berbagi, dan komunikasi korektif yang empatik. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam keluarga, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 7: misinformasi kesehatan dalam grup keluarga adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 8: Algorithmic Bias dalam Rekrutmen

Kasus 8: Algorithmic Bias dalam Rekrutmen memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah sebuah organisasi menggunakan sistem AI untuk menyaring pelamar berdasarkan pola dari data rekrutmen historis, lalu menemukan bahwa kelompok tertentu lebih sering tersisih. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: bias data, fairness, explainability, audit, human review, dan akuntabilitas manajemen. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam perusahaan, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara

berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 8: algorithmic bias dalam rekrutmen adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 9: Aktivisme Digital dan Polarisasi

Kasus 9: Aktivisme Digital dan Polarisasi memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah sebuah isu kebijakan publik menjadi viral. Pengguna membentuk kubu, potongan informasi dipakai sebagai senjata retorik, dan akun yang berbeda pandangan diserang secara massal. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: deliberasi, kebebasan berekspresi, disinformasi, pluralisme, empati, dan civic engagement. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam ruang publik, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang

memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip *stewardship* menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, *proportionality* sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip *safety by design* dan *privacy by design* lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang

perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 9: aktivisme digital dan polarisasi adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 10: Anak, Game Daring, dan Pembelian Digital

Kasus 10: Anak, Game Daring, dan Pembelian Digital memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah anak menggunakan game daring yang menawarkan pembelian berulang, komunikasi dengan pemain lain, dan hadiah berbasis waktu; orang tua baru menyadari adanya transaksi setelah tagihan membesar. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: literasi ekonomi digital, desain persuasif, perlindungan anak, parental mediation, dan tanggung jawab platform. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam keluarga, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 10: anak, game daring, dan pembelian digital adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 11: UMKM Masuk Ekonomi Platform

Kasus 11: UMKM Masuk Ekonomi Platform memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah pelaku UMKM di daerah mulai berjualan melalui marketplace dan media sosial, memperoleh pasar baru, tetapi juga menghadapi penipuan, akun palsu, ulasan manipulatif, dan ketergantungan pada algoritma platform. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: akses, pemberdayaan, keamanan transaksi, reputasi, literasi platform, dan ketahanan bisnis. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam UMKM, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip stewardship menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, proportionality sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip safety by design dan privacy by design lahir dari cara

berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan agency sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 11: umkm masuk ekonomi platform adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Kasus 12: Pelayanan Publik Digital dan Inklusi

Kasus 12: Pelayanan Publik Digital dan Inklusi memperlihatkan bagaimana konsep kewargaan digital bekerja ketika teknologi berhadapan dengan situasi nyata. Skenarionya adalah sebuah layanan administrasi dipindahkan ke portal digital untuk efisiensi, namun warga lanjut usia dan sebagian masyarakat berakses internet terbatas mengalami kesulitan. Pada permukaan, persoalan tersebut dapat terlihat sebagai kesalahan individual atau masalah teknis sederhana. Namun analisis yang lebih teliti menunjukkan bahwa terdapat beberapa lapisan sekaligus: inklusi, aksesibilitas, keadilan pelayanan, desain universal, alternatif layanan, dan dukungan literasi. Pendekatan kewargaan digital berguna karena ia mencegah kita mencari satu penyebab tunggal. Perilaku individu memang penting, tetapi desain sistem, norma organisasi, relasi kekuasaan, insentif, dan kompetensi juga menentukan hasil. Dalam pemerintah, penyelesaian yang hanya menyalahkan pengguna sering gagal mencegah kejadian berulang.

Langkah pertama dalam menganalisis kasus adalah memetakan para pemangku kepentingan. Siapa yang mengambil keputusan, siapa yang memperoleh manfaat, siapa yang memikul risiko, siapa yang

memiliki informasi lebih banyak, dan siapa yang mempunyai kemampuan untuk mengoreksi keadaan? Pertanyaan ini penting karena ruang digital sering menciptakan asimetri. Pihak yang memiliki sistem, data, atau otoritas dapat memengaruhi pengguna tanpa pengguna memahami sepenuhnya proses tersebut. Sebaliknya, individu juga dapat memperbesar dampak melalui fitur berbagi, otomatisasi, atau anonimitas. Prinsip *stewardship* menuntut pihak yang memiliki kapasitas lebih besar untuk memikul tanggung jawab yang sebanding.

Langkah kedua adalah membedakan fakta, asumsi, dan interpretasi. Dalam konflik digital, ketiganya cepat bercampur. Pengguna dapat menganggap pesan yang tampak resmi sebagai fakta, hasil AI sebagai kebenaran, atau popularitas sebagai bukti. Karena itu verifikasi perlu dilakukan secara lateral: keluar dari sumber awal, mencari sumber primer, memeriksa reputasi pembuat informasi, membaca konteks yang lebih luas, dan mencari bukti yang dapat menyangkal dugaan awal. Cara ini penting karena bias konfirmasi membuat manusia cenderung menerima informasi yang sesuai dengan harapan atau ketakutan mereka. Digital citizenship menuntut keberanian untuk mengoreksi diri ketika bukti berubah.

Langkah ketiga adalah menilai hak dan kewajiban. Hak atas privasi, keamanan, kebebasan berekspresi, akses informasi, dan partisipasi tidak bersifat tanpa batas. Hak seseorang berinteraksi dengan hak orang lain dan dengan kepentingan yang sah dari komunitas. Karena itu keputusan yang baik perlu proporsional. Pembatasan harus mempunyai tujuan yang jelas, menggunakan cara yang paling sedikit merugikan, dan menyediakan mekanisme keberatan atau koreksi. Dalam konteks digital, *proportionality* sangat penting karena respons berlebihan—misalnya pengawasan total untuk mencegah satu risiko—dapat menciptakan pelanggaran baru yang lebih luas.

Langkah keempat adalah menganalisis arsitektur teknologi. Fitur default, desain notifikasi, kemudahan berbagi, model rekomendasi, izin aplikasi, atau mekanisme pembayaran dapat mengarahkan perilaku tanpa disadari. Perspektif ini mengubah pertanyaan dari “mengapa pengguna ceroboh?” menjadi “bagaimana sistem membuat kecerobohan lebih mungkin terjadi, dan kontrol apa yang dapat mengurangi risiko?” Prinsip *safety by design* dan *privacy by design* lahir dari cara berpikir tersebut. Organisasi tidak menunggu pengguna sempurna; organisasi merancang sistem yang membantu manusia membuat keputusan lebih aman dan memberikan peringatan ketika tindakan berisiko.

Langkah kelima adalah menentukan respons berlapis. Respons individu dapat berupa verifikasi, perubahan kata sandi, koreksi informasi, permintaan persetujuan, atau penghentian tindakan. Respons institusional dapat berupa prosedur, pelatihan, kontrol teknis, audit, dukungan korban, dan penegakan kebijakan. Respons sistemik dapat melibatkan standar industri, regulasi, desain platform, atau kerja sama lintas lembaga. Pendekatan berlapis menghindari dua ekstrem: menganggap semua masalah dapat diselesaikan dengan literasi pengguna, atau sebaliknya menganggap pengguna tidak mempunyai peran sama sekali. Kewargaan digital membutuhkan *agency* sekaligus struktur yang bertanggung jawab.

Dari sudut pembelajaran, kasus ini dapat dijadikan bahan diskusi berbasis keputusan. Peserta tidak cukup diminta menyebutkan aturan, tetapi perlu memilih tindakan dan menjelaskan alasan. Misalnya: informasi apa yang masih kurang; tindakan apa yang harus dihentikan segera; siapa yang

perlu dihubungi; bagaimana bukti disimpan; bagaimana hak pihak lain dijaga; dan perubahan apa yang perlu dibuat agar insiden tidak berulang. Rubrik penilaian dapat melihat kualitas verifikasi, ketepatan etis, keamanan, dan akuntabilitas. Dengan demikian mahasiswa atau karyawan belajar bahwa kompetensi digital adalah kemampuan bertindak di bawah ketidakpastian.

Pelajaran utama dari kasus 12: pelayanan publik digital dan inklusi adalah bahwa kepercayaan merupakan aset digital yang sangat penting. Pengguna mempercayai identitas, institusi, informasi, sistem pembayaran, rekomendasi, dan komunikasi. Ketika kepercayaan rusak, biaya transaksi sosial meningkat: semua hal harus diverifikasi lebih keras, inovasi dicurigai, dan partisipasi menurun. Karena itu membangun kewargaan digital pada dasarnya juga membangun infrastruktur kepercayaan. Kepercayaan yang sehat bukan kepercayaan buta; ia bertumpu pada transparansi, kompetensi, integritas, mekanisme koreksi, dan bukti yang dapat diperiksa.

Roadmap Implementasi Digital Citizenship 2026-2030

Roadmap implementasi perlu dimulai dengan pemetaan tingkat kematangan. Institusi dapat menilai kebijakan yang sudah ada, perilaku pengguna, jenis insiden, kemampuan keamanan, praktik pengelolaan data, penggunaan AI, mekanisme pelaporan, dan kualitas pendidikan literasi. Pemetaan sebaiknya membedakan antara keberadaan dokumen dan efektivitas praktik. Banyak organisasi telah memiliki kebijakan kata sandi, privasi, atau media sosial, tetapi kepatuhan aktual rendah karena prosedur tidak realistis atau pimpinan tidak memberi contoh. Baseline yang jujur lebih penting daripada skor tinggi yang tidak mencerminkan keadaan.

Tahap berikutnya adalah menetapkan kompetensi minimum berdasarkan peran. Semua pengguna membutuhkan dasar keamanan, privasi, verifikasi informasi, etiket, dan kesadaran AI. Namun dosen, mahasiswa, pemimpin, administrator data, staf keuangan, dan pengembang sistem menghadapi risiko berbeda. Pendekatan berbasis peran memungkinkan pelatihan menjadi relevan. Staf keuangan memerlukan simulasi fraud dan deepfake; dosen memerlukan integritas akademik dan AI literacy; pengelola data memerlukan governance dan perlindungan data; pimpinan memerlukan risk oversight serta mekanisme akuntabilitas.

Tahap ketiga adalah mengintegrasikan pembelajaran ke dalam aktivitas rutin. Pelatihan satu kali mudah dilupakan. Organisasi dapat menggunakan microlearning, simulasi phishing, diskusi kasus bulanan, audit kecil, reminder kontekstual, dan evaluasi setelah insiden. Di perguruan tinggi, dosen dapat menambahkan komponen verifikasi sumber, disclosure penggunaan AI, atau refleksi etis dalam tugas yang sudah ada. Integrasi ini membuat kewargaan digital menjadi praktik, bukan kampanye. Perubahan perilaku terjadi ketika prinsip diulang dalam konteks yang relevan dan didukung oleh lingkungan.

Tahap keempat adalah membangun mekanisme pelaporan yang aman dan tidak menghukum kesalahan jujur secara berlebihan. Dalam keamanan siber, misalnya, pegawai yang cepat melaporkan bahwa ia mengklik tautan phishing membantu organisasi membatasi kerusakan. Jika budaya organisasi memalukan orang yang melapor, insiden akan disembunyikan. Prinsip serupa berlaku pada cyberbullying, penyalahgunaan AI, dan kebocoran data. Accountability harus

dibedakan dari blame. Tujuannya adalah mengetahui apa yang terjadi, memulihkan dampak, mencegah pengulangan, dan menegakkan konsekuensi secara proporsional ketika ada kesengajaan atau kelalaian berat.

Tahap kelima adalah mengembangkan metrik yang berarti. Indikator dapat mencakup tingkat penyelesaian pelatihan, kemampuan verifikasi dalam simulasi, tingkat adopsi MFA, jumlah insiden yang dilaporkan cepat, kualitas disclosure penggunaan AI, kepatuhan minimisasi data, pengalaman korban dalam proses pemulihan, serta kesenjangan kompetensi antarunit. Metrik tidak boleh mendorong perilaku defensif. Jika keberhasilan hanya diukur dari sedikitnya insiden, organisasi dapat terdorong menyembunyikan masalah. Lebih baik mengukur kemampuan mendeteksi, merespons, belajar, dan mengurangi dampak.

Tahap keenam adalah melakukan review berkala terhadap teknologi baru. Setiap adopsi platform atau AI sebaiknya disertai pertanyaan tentang data, keamanan, vendor, bias, transparansi, dampak pekerjaan, aksesibilitas, dan exit strategy. Prinsip ini sangat penting karena teknologi berubah lebih cepat daripada siklus kebijakan. Organisasi memerlukan governance yang cukup stabil untuk menjaga nilai, tetapi cukup adaptif untuk menghadapi inovasi. Dengan begitu, digital citizenship tidak menjadi kurikulum yang cepat usang, melainkan kapasitas organisasi untuk menilai perubahan secara bertanggung jawab.

Pada tingkat nasional, roadmap perlu menghubungkan literasi digital dengan kebijakan pendidikan, transformasi ekonomi, pelayanan publik, perlindungan data, keamanan siber, dan pembangunan AI. Program masyarakat digital sebaiknya tidak hanya mengukur jumlah orang yang terhubung, tetapi juga kualitas partisipasi dan kemampuan memperoleh manfaat. Ketimpangan kompetensi dapat menjadi bentuk baru ketimpangan sosial. Warga yang tidak mampu memverifikasi informasi, mengamankan akun, menggunakan AI secara produktif, atau melindungi data akan berada pada posisi yang semakin lemah di pasar kerja dan ruang publik.

Sasaran akhirnya adalah masyarakat yang memiliki technological agency: kemampuan menggunakan teknologi untuk mencapai tujuan manusia tanpa kehilangan kendali kritis. Agency ini mencakup kemampuan memilih kapan menggunakan teknologi dan kapan tidak, kapan mempercayai sistem dan kapan memeriksa, kapan berbagi informasi dan kapan menahan, kapan otomatisasi membantu dan kapan keputusan perlu dikembalikan kepada manusia. Inilah bentuk kematangan digital yang paling penting. Warga tidak sekadar mengikuti arus inovasi, melainkan mampu ikut menentukan arah penggunaan teknologi sesuai nilai dan kepentingan masyarakat.

Glossarium

Algorithmic literacy: Kemampuan memahami peran algoritma dalam memilih, memeringkat, merekomendasikan, atau memprediksi informasi serta perilaku.

AI literacy: Kemampuan memahami, menggunakan, mengevaluasi, dan mengkritisi sistem kecerdasan artifisial secara efektif dan bertanggung jawab.

Authentication: Proses memverifikasi identitas pengguna sebelum akses diberikan.

Automation bias: Kecenderungan terlalu mempercayai rekomendasi sistem otomatis meskipun terdapat alasan untuk meragukannya.

Consent: Persetujuan yang diberikan secara sadar, spesifik, dan dapat dipahami terhadap suatu tindakan atau pemrosesan data.

Cyberbullying: Perundungan yang dilakukan melalui media digital secara berulang atau berdampak luas.

Cybersecurity: Praktik melindungi sistem, jaringan, perangkat, akun, dan data dari gangguan atau akses tidak sah.

Data minimization: Prinsip mengumpulkan dan memproses data hanya sebanyak yang benar-benar diperlukan untuk tujuan yang sah.

Deepfake: Konten audio, gambar, atau video sintetik/manipulatif yang dibuat agar tampak autentik.

Digital citizenship: Norma, pengetahuan, keterampilan, sikap, dan tanggung jawab untuk berpartisipasi secara aman, etis, kritis, dan produktif dalam lingkungan digital.

Digital divide: Kesenjangan akses, kualitas koneksi, perangkat, keterampilan, dukungan, dan manfaat yang diperoleh dari teknologi digital.

Digital footprint: Rekam data yang ditinggalkan oleh aktivitas digital seseorang, baik sengaja maupun tidak sengaja.

Digital identity: Representasi identitas individu atau organisasi di lingkungan digital.

Digital literacy: Kemampuan mengakses, memahami, menilai, mencipta, dan menggunakan informasi serta teknologi digital secara efektif.

Digital well-being: Kondisi penggunaan teknologi yang mendukung kesehatan fisik, mental, sosial, dan keseimbangan hidup.

Disinformation: Informasi salah atau menyesatkan yang dibuat atau disebarkan secara sengaja untuk menipu atau memengaruhi.

Doxing: Mempublikasikan informasi pribadi seseorang tanpa izin dengan tujuan mengintimidasi, merugikan, atau mengekspos.

Echo chamber: Lingkungan informasi yang memperkuat pandangan serupa dan mengurangi paparan terhadap perspektif berbeda.

Filter bubble: Kondisi personalisasi algoritmik yang membatasi variasi informasi yang dilihat pengguna.

Information literacy: Kemampuan mengenali kebutuhan informasi, menemukan sumber, menilai kredibilitas, dan menggunakan informasi secara etis.

Media literacy: Kemampuan mengakses, menganalisis, mengevaluasi, mencipta, dan memahami pesan media beserta konteks serta kepentingannya.

Misinformation: Informasi salah yang dibagikan tanpa niat menipu.

Multi-factor authentication: Metode autentikasi yang menggunakan dua atau lebih bukti identitas.

Netiquette: Norma kesantunan dan perilaku yang layak dalam interaksi digital.

Phishing: Upaya penipuan untuk memperoleh kredensial atau data sensitif dengan menyamar sebagai pihak tepercaya.

Platform governance: Aturan, proses, dan mekanisme yang mengatur perilaku, konten, data, dan keputusan pada platform digital.

Privacy: Kemampuan individu mengendalikan akses terhadap diri, data, dan konteks kehidupannya.

Provenance: Informasi mengenai asal-usul, riwayat, dan proses pembuatan atau perubahan suatu konten/data.

Stewardship: Tanggung jawab menjaga dan mengelola sumber daya atau ekosistem agar bermanfaat secara berkelanjutan bagi pihak terkait.

Two-factor authentication: Bentuk autentikasi multi-faktor yang menggunakan dua jenis bukti identitas.

Daftar Pustaka

- Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. *Computers & Education*, 107, 100–112. <https://doi.org/10.1016/j.compedu.2017.01.002>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28, 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1), eaau4586. <https://doi.org/10.1126/sciadv.aau4586>
- Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New Media & Society*, 18(9), 2063–2079. <https://doi.org/10.1177/1461444815577797>
- Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, 7(1), 3–14. <https://doi.org/10.1080/10714420490280152>
- Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078. <https://doi.org/10.1016/j.compedu.2012.04.016>

- Tadlaoui-Brahmi, A., et al. (2022). Digital citizenship in primary education: A systematic literature review. *Social Sciences & Humanities Open*, 6, 100348.
<https://doi.org/10.1016/j.ssaho.2022.100348>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Webster, J. (2025). Defining digital citizenship and digital citizenship education. *Journal of Research on Technology in Education*. <https://doi.org/10.1080/15391523.2025.2536564>
- Li, L. (2025). Digital citizenship education at the early childhood level: How is it implemented? A systematic review. *International Journal of Child Care and Education Policy*, 19.
<https://doi.org/10.1186/s40723-025-00153-2>
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.
- UNESCO. (2024). *Global citizenship education in a digital age: Teacher guidelines*. UNESCO.
- UNESCO. (2024). *Q&A: Why digital global citizenship education is essential*. UNESCO.
- UNESCO. (2025). *Media and information literacy and digital competencies*. UNESCO.
- OECD. (2024). *OECD Digital Economy Outlook 2024 (Volume 2)*. OECD Publishing.
- OECD. (2025). *How's life for children in the digital age?* OECD Publishing.
- Kementerian Komunikasi dan Digital Republik Indonesia. (2025). *Indeks Masyarakat Digital Indonesia 2025*. BPSDM Komdigi.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
- Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial*.
- boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- Jenkins, H., Clinton, K., Purushotma, R., Robison, A. J., & Weigel, M. (2009). *Confronting the challenges of participatory culture: Media education for the 21st century*. MIT Press.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press.

Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record*, 121(11), 1–40. <https://doi.org/10.1177/016146811912101102>

Kozyreva, A., Wineburg, S., Lewandowsky, S., & Hertwig, R. (2022). Critical ignoring as a core competence for digital citizens. *Current Directions in Psychological Science*, 31(1), 81–88. <https://doi.org/10.1177/09637214211061870>

European Commission. (2022). The Digital Competence Framework for Citizens: DigComp 2.2. Publications Office of the European Union. <https://doi.org/10.2760/115376>

Council of Europe. (2019). Digital citizenship education handbook. Council of Europe Publishing.

Catatan Penulis

Artikel ini disusun untuk tujuan akademik dan pendidikan. Rujukan peraturan dan kebijakan perlu selalu dibaca bersama naskah resmi serta pembaruan terbaru. Dalam praktik organisasi, penerapan prinsip kewargaan digital sebaiknya disesuaikan dengan konteks, profil risiko, kelompok pengguna, dan ketentuan hukum yang berlaku.