
Digital Citizenship,
Privasi, dan
Jejak Digital
Oleh: Rudy C Tarumingkeng

Oleh:
Prof Ir Rudy C Tarumingkeng, PhD
Guru Besar Manajemen NUP: 9903252922
Rektor, Universitas Cenderawasih, Papua (1978-1988, dan
Rektor, Kampus AGRO Manokwari sekarang Universitas Papua Manokwari)
Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991
Rektor, Universitas Kristen Krida Wacana, Jakarta (1991-2000)
Ketua Dewan Guru Besar, IPB-University, Bogor (2005-2006)
AI - Data Analyst, dan Ketua Senat Akademik, IBM-ASMI, Jakarta 2024-

---

rudyct75@gmail.com
15 Maret 2026

DIGITAL CITIZENSHIP, PRIVASI, DAN JEJAK DIGITAL

Pendahuluan

Kehidupan modern semakin sulit dipisahkan dari ruang digital. Belajar, bekerja, berbelanja, berkomunikasi, mencari hiburan, mengurus layanan publik, hingga membangun identitas sosial kini berlangsung melalui perangkat, platform, dan jaringan yang terus aktif. Dalam situasi demikian, pertanyaan tentang kewargaan tidak lagi hanya terkait dengan partisipasi di ruang fisik, tetapi juga menyangkut bagaimana seseorang hadir, bertindak, berinteraksi, dan bertanggung jawab di ruang digital. Council of Europe mendefinisikan *digital citizenship* sebagai kapasitas untuk berpartisipasi secara aktif, berkelanjutan, dan bertanggung jawab dalam komunitas daring maupun luring melalui keterlibatan yang kompeten dan positif dengan teknologi digital. Lembaga yang sama juga menekankan bahwa pendidikan kewargaan digital bertujuan memberdayakan peserta didik untuk menjalankan hak dan tanggung jawab demokratis mereka secara daring serta melindungi hak asasi manusia, demokrasi, dan *rule of law* di ruang siber. (Portal)

Dengan demikian, *digital citizenship* bukan sekadar kemampuan menggunakan gawai atau aplikasi. Ia adalah gabungan antara literasi, etika, partisipasi, tanggung jawab sosial, kesadaran hak, dan kemampuan mengambil keputusan yang bijaksana di ruang digital. UNESCO, melalui panduan pendidikan kewargaan global di era digital, menegaskan bahwa pendidikan kewargaan digital diperlukan untuk menyiapkan warga yang lebih terinformasi, terlibat, dan bertanggung jawab, serta untuk membantu peserta didik bertindak secara etis dan bertanggung jawab baik di lingkungan fisik maupun digital. (UNESCO)

Di dalam diskusi itu, dua tema menjadi sangat penting, yaitu privasi dan jejak digital. Privasi menyangkut ruang perlindungan diri: informasi apa

yang boleh diketahui orang lain, oleh siapa, untuk tujuan apa, dan dalam batas apa. Jejak digital adalah bekas data yang ditinggalkan seseorang ketika beraktivitas secara daring. Keduanya saling terkait erat. Tanpa kesadaran privasi, jejak digital dapat berkembang menjadi sumber risiko: profil perilaku, pencurian identitas, manipulasi komersial, kerusakan reputasi, diskriminasi algoritmik, hingga ancaman keamanan. UNESCO dalam modul literasi media dan informasi menempatkan privasi, informasi personal, jejak digital, reputasi daring, dan pengelolaan pengaturan privasi sebagai kompetensi dasar yang harus dipahami warga digital. (UNESCO)

Dalam konteks Indonesia, urgensi topik ini semakin besar karena transformasi digital berlangsung sangat cepat, sementara literasi perlindungan data masyarakat belum selalu tumbuh sebanding. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi secara tegas menyatakan bahwa pelindungan data pribadi merupakan bagian dari hak asasi manusia dan dimaksudkan untuk menjamin hak warga negara atas pelindungan diri pribadi. Undang-undang itu juga mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun nonelektronik. (JDIH Kemkomdigi)

Esai ini membahas *digital citizenship*, privasi, dan jejak digital sebagai satu kesatuan. Argumen utamanya adalah bahwa kewargaan digital yang dewasa tidak mungkin dibangun tanpa kesadaran privasi dan pengelolaan jejak digital. Orang yang aktif bermedia, produktif berjejaring, dan mahir memakai teknologi belum tentu menjadi warga digital yang baik apabila ia abai pada hak dirinya sendiri, hak orang lain, dan dampak jangka panjang dari data yang ia tinggalkan. Sebaliknya, warga digital yang matang bukan hanya pandai memanfaatkan teknologi, melainkan juga mampu menimbang konsekuensi, melindungi martabat diri, menghormati orang lain, dan bertanggung jawab atas kehadirannya di ruang digital. (Portal)

1. Memahami Digital Citizenship

Konsep *digital citizenship* lahir dari kesadaran bahwa ruang digital telah menjadi bagian dari ruang publik. Di sana orang tidak hanya menjadi konsumen informasi, tetapi juga produsen, penyebar, pengomentar, pengorganisasi komunitas, dan kadang penggerak opini. Karena itu, perilaku digital tidak bisa dipahami hanya sebagai kebiasaan teknis; ia adalah tindakan sosial dan bahkan tindakan kewargaan. Council of Europe menjelaskan bahwa warga digital adalah orang yang mampu terlibat secara kompeten dan positif dengan teknologi digital, berpartisipasi aktif dan bertanggung jawab dalam kehidupan sosial dan sipil, terus belajar, dan berkomitmen membela hak asasi manusia serta martabat. (Portal)

Definisi ini penting karena memperluas pemahaman kita. Seorang warga digital yang baik bukan hanya orang yang tahu cara membuat akun, mengunggah konten, atau memakai aplikasi konferensi video. Ia adalah orang yang mengerti bahwa ruang digital memiliki dimensi etis, politis, kultural, dan hukum. Ia sadar bahwa ujaran kebencian, fitnah, pelecehan, doxing, penyebaran data pribadi, pembajakan karya, dan penyebaran hoaks bukan sekadar "aktivitas online", tetapi tindakan yang dapat merusak komunitas, melukai orang lain, dan mengganggu demokrasi. UNESCO juga menekankan bahwa pendidikan kewargaan global di era digital harus memperkuat kemampuan berpikir kritis, partisipasi etis, dan tanggung jawab terhadap dunia yang lebih inklusif, adil, dan damai. (UNESCO)

Dengan demikian, *digital citizenship* memiliki dua dimensi besar. Dimensi pertama adalah hak: hak atas akses, ekspresi, perlindungan data, keamanan, dan partisipasi. Dimensi kedua adalah tanggung jawab: kewajiban untuk tidak menyalahgunakan teknologi, tidak merugikan orang lain, memverifikasi informasi, menghormati privasi, dan menjaga kualitas interaksi publik. Di sinilah *digital citizenship* bersinggungan langsung dengan privasi dan jejak digital. Hak digital tanpa tanggung

jawab akan melahirkan kekacauan. Sebaliknya, tanggung jawab digital tanpa perlindungan hak akan melahirkan pengawasan dan ketimpangan kuasa. (Portal)

2. Privasi sebagai Fondasi Kewargaan Digital

Privasi sering disalahpahami sebagai keinginan untuk "menyembunyikan sesuatu". Padahal, secara normatif, privasi adalah prasyarat kebebasan dan martabat. Orang membutuhkan ruang privat agar dapat membangun identitas, bereksperimen dengan pikiran, mengambil keputusan, dan menjalin relasi tanpa terus-menerus diawasi. OECD menempatkan privasi dan perlindungan data sebagai fondasi ekosistem data yang berbasis kepercayaan, dan merumuskan delapan prinsip dasar: pembatasan pengumpulan, kualitas data, spesifikasi tujuan, pembatasan penggunaan, perlindungan keamanan, keterbukaan, partisipasi individu, dan akuntabilitas. (OECD)

Prinsip-prinsip itu memperlihatkan bahwa privasi bukan isu sempit. Ia mencakup pertanyaan: data apa yang dikumpulkan, apakah data itu benar, untuk tujuan apa ia digunakan, siapa yang dapat mengaksesnya, bagaimana ia diamankan, apakah individu tahu apa yang terjadi terhadap datanya, apakah ia bisa mengoreksi atau menolak, dan siapa yang bertanggung jawab jika terjadi pelanggaran. NIST melalui *Privacy Framework* juga memandang privasi sebagai persoalan manajemen risiko yang perlu diidentifikasi, dinilai, diprioritaskan, dan dikomunikasikan oleh organisasi sambil tetap melindungi individu. Pada April 2025, NIST merilis *Initial Public Draft* Privacy Framework 1.1 untuk merespons kebutuhan manajemen risiko privasi yang lebih mutakhir serta menyelaraskannya dengan kerangka keamanan siber yang baru. (NIST)

Dari sudut kewargaan digital, privasi adalah kondisi yang memungkinkan warga berpartisipasi tanpa takut disalahgunakan. Jika setiap aktivitas digital selalu dimonetisasi, diprofilkan, diawasi, atau dipakai untuk manipulasi perilaku, maka partisipasi digital tidak lagi sepenuhnya bebas.

UNESCO dalam materi literasi media dan informasi menautkan privasi dengan pemahaman tentang jenis informasi yang aman dibagikan, informasi yang sebaiknya tetap privat, pengelolaan pengaturan privasi, dan pemahaman mengenai permanensi informasi yang dibagikan secara daring. Artinya, privasi tidak hanya bergantung pada hukum atau platform, tetapi juga pada kompetensi warga digital itu sendiri. (UNESCO)

Dalam konteks Indonesia, UU PDP menegaskan bahwa pelindungan data pribadi merupakan keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesannya guna menjamin hak konstitusional subjek data. Penjelasan umumnya juga menyebut bahwa pelindungan data pribadi adalah manifestasi pengakuan dan pelindungan atas hak dasar manusia, serta diperlukan untuk membangun kepercayaan masyarakat agar data pribadi dapat digunakan untuk kepentingan yang lebih besar tanpa disalahgunakan atau melanggar hak pribadi. Ini menunjukkan bahwa privasi bukan hambatan bagi inovasi digital, melainkan syarat legitimasi sosial bagi ekonomi dan layanan digital. (JDIH Kemkomdigi)

3. Jejak Digital: Definisi dan Sifat Dasarnya

Jika privasi berbicara tentang batas perlindungan diri, maka jejak digital berbicara tentang bekas yang terus tertinggal dari aktivitas kita. Pemerintah Australia melalui *cyber.gov.au* mendefinisikan jejak digital sebagai himpunan unik dari aktivitas, tindakan, kontribusi, dan komunikasi yang dapat ditelusuri yang termanifestasi di internet atau pada perangkat digital. eSafety Commissioner Australia menambahkan bahwa internet mengingat lebih banyak tentang seseorang daripada yang sering disadari; jejak digital dapat mencakup foto lama, komentar pada unggahan publik, dan hal-hal lain yang menjadi salah satu pengalaman pertama orang lain tentang diri kita di internet. (Cyber.gov.au)

UNESCO menjelaskan bahwa jejak digital adalah data yang ditinggalkan pengguna pada perangkat digital, dapat tercipta secara aktif maupun pasif, dan biasanya dikumpulkan secara sistematis oleh layanan internet serta perusahaan untuk berbagai penggunaan, sering kali komersial, yang kemudian memengaruhi pengalaman navigasi, profil daring, hasil pencarian, bahkan privasi dan keamanan pengguna. Definisi ini sangat penting karena menunjukkan bahwa jejak digital bukan hanya apa yang sengaja kita unggah, tetapi juga apa yang dikumpulkan tentang kita ketika kita sekadar menjelajah, mengklik, atau berpindah aplikasi. (UNESCO)

Di sinilah letak paradoks dunia digital. Seseorang mungkin merasa hanya "iseng melihat-lihat", namun di balik itu terbentuk data perilaku: lokasi, durasi kunjungan, preferensi, perangkat yang dipakai, pola klik, waktu aktif, dan kemungkinan minat. Dalam skala besar, data seperti ini menjadi bahan untuk profil komersial, rekomendasi konten, penargetan iklan, optimasi platform, atau bahkan penilaian risiko. Jejak digital dengan demikian tidak hanya bersifat dokumentatif, tetapi juga produktif: ia dipakai untuk menghasilkan keputusan baru tentang kita. (UNESCO)

Secara umum, jejak digital memiliki empat sifat utama. Pertama, ia kumulatif: sedikit demi sedikit, data kecil membentuk gambaran besar. Kedua, ia persisten: informasi lama dapat muncul kembali. Ketiga, ia dapat digabungkan: data dari banyak sumber bisa disatukan. Keempat, ia dapat ditafsirkan oleh pihak lain di luar kontrol kita. Karena itu, jejak digital bukan sekadar "arsip diri", melainkan sumber makna sosial dan ekonomi yang dapat menguntungkan atau merugikan. UNICEF bahkan mengingatkan bahwa setiap klik, komentar, berbagi, dan unggahan menciptakan catatan digital yang dapat sangat sulit dihapus, sehingga anak-anak pun menghadapi risiko terhadap privasi, identitas, reputasi, dan keselamatan. (UNICEF)

4. Jejak Digital Aktif dan Pasif

Untuk memahami jejak digital lebih jelas, berguna membedakan antara jejak aktif dan jejak pasif. UNESCO menyatakan bahwa jejak digital dapat tercipta secara aktif atau pasif. Pemerintah Kanada melalui *cyber.gc.ca* memberi penjelasan yang lebih operasional: jejak digital aktif adalah data yang ditinggalkan melalui tindakan sengaja, seperti mengunggah di media sosial, mengisi formulir daring, atau menyetujui kuki peramban; sedangkan jejak digital pasif adalah data yang tertinggal secara tidak sengaja atau tanpa disadari, sering dikumpulkan melalui pemantauan yang terkait dengan alamat IP, kuki, pelacakan lokasi, atau pencatatan aktivitas oleh situs dan aplikasi. (UNESCO)

Jejak aktif relatif lebih mudah dipahami masyarakat karena ia tampak jelas. Ketika seseorang mengunggah foto, menulis komentar, menyukai konten, mengisi biodata, mengirim email, atau membuat profil profesional, ia sadar sedang menghasilkan data tentang dirinya. Aktivitas ini sering dipandang sebagai ekspresi diri, partisipasi sosial, atau kerja profesional. Dalam banyak hal, jejak aktif memang dapat berguna. Ia bisa membangun reputasi, memperluas jejaring, menampilkan karya, atau mendukung identitas akademik dan profesional. Namun karena ia disaksikan, disimpan, dan dapat disebarkan ulang, jejak aktif juga membawa risiko jika dilakukan tanpa pertimbangan. (eSafety Commissioner)

Jejak pasif justru lebih problematis karena sering tidak terlihat. Seseorang membuka aplikasi cuaca, lalu lokasinya direkam. Ia mengunjungi toko daring, lalu preferensinya dipelajari. Ia menonton video tertentu, lalu algoritma menyimpulkan profil minat dan emosinya. Ia tidak merasa sedang "membagikan data", padahal data tentangnya terus diproduksi. Di sinilah asimetri kuasa antara warga digital dan platform menjadi nyata. Platform mengetahui jauh lebih banyak tentang pengguna daripada sebaliknya, sedangkan pengguna sering tidak mengerti kedalaman dan implikasi pengumpulan data tersebut. (UNESCO)

Bagi kewargaan digital, pembedaan ini penting karena menunjukkan bahwa tanggung jawab pribadi saja tidak cukup. Seseorang memang dapat berhati-hati dalam apa yang ia unggah, tetapi ia tetap terpapar pada pengumpulan data pasif oleh ekosistem digital. Oleh karena itu, perlindungan privasi membutuhkan dua hal sekaligus: literasi pengguna dan tata kelola kelembagaan. OECD berbicara tentang akuntabilitas, keterbukaan, dan pembatasan penggunaan; NIST berbicara tentang manajemen risiko privasi organisasi; sedangkan UNESCO menekankan perlunya tata kelola platform yang berbasis prinsip hak asasi manusia dan proses yang inklusif. (OECD)

5. Privasi, Reputasi, dan Identitas Diri

Salah satu dampak paling nyata dari jejak digital adalah pembentukan reputasi. eSafety Commissioner menegaskan bahwa jejak digital bisa menjadi salah satu hal pertama yang dialami orang lain tentang diri kita secara daring. Artinya, sebelum orang bertemu secara langsung, mereka sering lebih dahulu bertemu dengan data kita: foto, komentar, unggahan, arsip organisasi, tulisan blog, atau jejak pencarian nama. Dalam dunia kerja, pendidikan, dan hubungan sosial, reputasi digital semakin memengaruhi persepsi orang terhadap kompetensi, karakter, dan kredibilitas seseorang. (eSafety Commissioner)

Reputasi digital tidak selalu dibentuk oleh diri sendiri. UNICEF mengingatkan bahwa jejak seseorang juga mencakup apa yang orang lain unggah dan bagikan tentang dirinya. Karena itu, hak atas privasi berhubungan erat dengan hak atas reputasi dan kehormatan. Ketika foto seseorang dibagikan tanpa izin, ketika data pribadinya dipublikasikan, atau ketika rumor menyebar di media sosial, yang terancam bukan hanya kenyamanan sementara, tetapi juga identitas sosial jangka panjang. Dalam banyak kasus, konten yang tampak sepele ketika diunggah dapat memperoleh makna baru bertahun-tahun kemudian ketika konteks berubah. (UNICEF)

Pada tingkat yang lebih dalam, identitas digital bukan hanya representasi netral dari siapa kita, tetapi juga hasil negosiasi antara apa yang kita tampilkan, apa yang platform tonjolkan, dan apa yang orang lain tafsirkan. Karena itu, *digital citizenship* yang dewasa menuntut kemampuan reflektif: apa yang saya bagikan, mengapa saya bagikan, siapa audiensnya, bagaimana data itu mungkin dipakai, dan bagaimana itu memengaruhi orang lain? UNESCO dalam modul privasi dan MIL menempatkan pengelolaan reputasi daring serta pemahaman tentang permanensi informasi sebagai bagian penting dari kompetensi warga digital. (UNESCO)

6. Anak, Remaja, dan Kelompok Rentan

Isu privasi dan jejak digital menjadi lebih genting ketika menyangkut anak dan remaja. UNICEF menjelaskan bahwa anak-anak yang tumbuh dalam teknologi digital menghadapi risiko terhadap privasi, identitas, reputasi, dan keselamatan seperti belum pernah terjadi sebelumnya. Mereka bukan hanya pengguna aktif media digital, tetapi juga sering menjadi subjek data sejak sangat dini, bahkan sebelum mampu memberikan persetujuan yang bermakna. Unggahan orang tua, penggunaan aplikasi belajar, gim daring, perangkat pintar, dan media sosial semuanya dapat membentuk jejak digital anak. (UNICEF)

UNICEF menganjurkan agar orang tua memeriksa pengaturan privasi perangkat dan aplikasi, membatasi izin akses yang berlebihan, meminimalkan pengumpulan data, memakai kata sandi kuat dan autentikasi multi-faktor, serta—yang sangat penting—membantu anak memahami privasi sebagai hak dan sebagai bagian dari keselamatan daring. UNICEF juga menekankan bahwa anak perlu diajari sejak dini bahwa apa yang dilakukan secara daring meninggalkan catatan atau jejak digital yang bertahan lama. (UNICEF)

Hal ini menunjukkan bahwa literasi privasi tidak bisa menunggu sampai seseorang dewasa. Di sekolah, universitas, dan keluarga, kewargaan digital perlu diajarkan sebagai pendidikan karakter dan kecakapan hidup.

Bukan hanya bagaimana memakai teknologi, tetapi juga bagaimana mengelola diri, berempati, meminta izin sebelum membagikan informasi orang lain, menghormati privasi, dan berpikir sebelum memposting sesuatu. UNICEF secara eksplisit mengingatkan bahwa tidak boleh masuk ke akun orang lain tanpa izin atau membagikan informasi serta foto mereka tanpa persetujuan. (UNICEF)

Kelompok rentan lain juga perlu mendapat perhatian, misalnya penyandang disabilitas, komunitas minoritas, korban kekerasan, aktivis, atau warga dengan literasi digital rendah. Bagi kelompok-kelompok ini, kebocoran privasi dan jejak digital yang buruk dapat menimbulkan risiko yang tidak proporsional: penguntitan, diskriminasi, pelecehan, atau pengucilan. Karena itu, kewargaan digital yang adil harus memperhitungkan bukan hanya perilaku ideal warga, tetapi juga struktur perlindungan bagi mereka yang paling rentan. UNESCO dalam pedoman tata kelola platform digital menekankan pentingnya prinsip hak asasi manusia dan proses yang inklusif dalam perumusan kebijakan platform. (UNESCO)

7. Data sebagai Sumber Kekuasaan

Jejak digital memiliki nilai ekonomi dan politik yang sangat besar. Platform digital, pengiklan, perusahaan analitik, dan kadang lembaga publik menggunakan data untuk memprediksi perilaku, menyegmentasi audiens, menargetkan pesan, dan mengoptimalkan layanan. Karena itu, pembahasan privasi tidak hanya soal keamanan teknis, tetapi juga soal relasi kuasa. Siapa yang mengumpulkan data, siapa yang menggabungkannya, siapa yang dapat menjual atau mengalihgunakannya, dan siapa yang memiliki kemampuan untuk menolak? OECD sejak lama menekankan bahwa perlindungan privasi harus berjalan beriringan dengan arus data lintas batas dan ekosistem digital yang berbasis kepercayaan. (OECD)

Dalam ekonomi digital, jejak digital kerap menjadi bahan baku utama. Data preferensi, lokasi, riwayat pencarian, hubungan pertemanan, dan

pola interaksi dipakai untuk membangun profil. Profil ini kemudian memengaruhi iklan yang tampil, rekomendasi konten, harga yang ditawarkan, bahkan kemungkinan seseorang dilihat "layak" atau "berisiko" oleh sistem tertentu. Di titik ini, jejak digital tidak lagi sekadar masa lalu yang tertinggal, tetapi menjadi alat untuk membentuk masa depan seseorang. Karena itu, privasi bukan hanya hak pasif untuk dilindungi, melainkan hak aktif untuk tidak direduksi menjadi objek pengamatan dan manipulasi. (UNESCO)

Pemahaman semacam ini penting bagi warga digital karena banyak orang hanya melihat dampak mikro—misalnya iklan yang terasa "mengikuti" mereka—tanpa memahami dampak makro seperti profilisasi, segmentasi politik, atau reproduksi ketimpangan melalui data. Dalam kerangka ini, *digital citizenship* mengharuskan warga tidak hanya berhati-hati secara personal, tetapi juga kritis terhadap arsitektur digital yang mereka gunakan. UNESCO menghubungkan pembelajaran privasi dengan konsep reputasi daring, pengaturan privasi, dan bahkan apa yang disebut beberapa ahli sebagai *surveillance capitalism*, yakni ekonomi yang bertumpu pada ekstraksi dan pemanfaatan data perilaku. (UNESCO)

8. Hak, Persetujuan, dan Akuntabilitas

Salah satu konsep kunci dalam perlindungan privasi adalah persetujuan. Namun dalam praktik digital, persetujuan sering menjadi formalitas. Pengguna dihadapkan pada syarat dan ketentuan panjang, tombol "setuju", serta desain antarmuka yang mendorong persetujuan cepat. Secara hukum, persetujuan mungkin tercatat. Secara etis, belum tentu ia bermakna. Karena itu, OECD menekankan prinsip keterbukaan, pembatasan tujuan, partisipasi individu, dan akuntabilitas, bukan sekadar adanya persetujuan nominal. (OECD)

Di Indonesia, UU PDP mengatur hak subjek data dan kewajiban pengendali maupun prosesor data, termasuk soal pemrosesan dan transfer data pribadi. Undang-undang ini dirancang sebagai standar

umum perlindungan data pribadi yang dapat diterapkan lintas sektor. Penjelasannya menekankan keseimbangan antara hak individu dan kepentingan masyarakat yang diwakili negara, sekaligus pentingnya membangun kepercayaan masyarakat dalam masyarakat informasi. Ini berarti warga digital Indonesia tidak hanya perlu tahu cara menjaga akun, tetapi juga perlu menyadari bahwa mereka memiliki hak normatif terhadap data pribadinya. (JDIH Kemkomdigi)

Akuntabilitas sama pentingnya. Jika data bocor, dipakai di luar tujuan, atau menyebabkan kerugian, harus ada pihak yang bertanggung jawab. Di sinilah pendekatan NIST bermanfaat: privasi dipahami sebagai risiko yang harus dikelola oleh organisasi, bukan sekadar beban individu. Semakin besar kekuasaan lembaga dalam mengumpulkan dan mengolah data, semakin besar pula kewajiban mereka untuk mengidentifikasi risiko, melindungi individu, menjelaskan proses, dan membangun mekanisme perbaikan. (NIST)

9. Privasi dan Kebebasan Berekspresi

Ada anggapan bahwa privasi dan kebebasan berekspresi saling bertentangan: semakin besar perlindungan privasi, semakin kecil kebebasan berbicara; atau sebaliknya, semakin luas ekspresi, semakin kecil ruang privat. UNESCO menunjukkan bahwa hubungan keduanya lebih kompleks. Dalam kajiannya tentang privasi, kebebasan berekspresi, dan transparansi internet, UNESCO justru mengajak melihat bagaimana ketiganya dapat saling mendukung sekaligus kadang saling bersaing, sehingga kebijakan yang baik harus menyeimbangkan hak-hak tersebut. (UNESCO Digital Library)

Dalam konteks kewargaan digital, keseimbangan ini sangat penting. Warga digital perlu bebas menyampaikan pendapat, mengkritik, dan berpartisipasi dalam debat publik. Namun kebebasan itu tidak boleh dijadikan alasan untuk membuka data pribadi orang lain, menyebarkan foto tanpa izin, mempublikasikan alamat rumah, nomor telepon, atau informasi sensitif. Dengan kata lain, kebebasan berekspresi yang sehat

justru membutuhkan budaya menghormati privasi. Tanpa itu, ruang digital akan dipenuhi intimidasi, doxing, dan kekerasan simbolik yang membuat banyak warga takut berpartisipasi. (Portal)

Ini juga berlaku dalam kehidupan akademik dan profesional. Seorang dosen atau mahasiswa boleh aktif berdiskusi dan beropini, tetapi tetap harus memikirkan apakah unggahan tertentu melanggar privasi orang lain atau menimbulkan jejak digital yang dapat merusak kepercayaan profesional. Di sini terlihat bahwa privasi bukan lawan dari partisipasi publik, melainkan syarat bagi partisipasi publik yang aman dan bermartabat. (UNESCO)

10. Jejak Digital dan Dunia Pendidikan

Sekolah dan universitas kini menghasilkan sangat banyak data: absensi, aktivitas di platform pembelajaran, hasil kuis, tugas, rekaman video, diskusi kelas, bahkan pola perilaku belajar. UNESCO dalam publikasinya tentang privasi dan keamanan pelajar menegaskan perlunya keseimbangan antara penggunaan teknologi untuk transformasi pendidikan dan perlindungan terhadap privasi serta keamanan peserta didik. Ini penting karena digitalisasi pendidikan dapat mempercepat pembelajaran, tetapi juga memperluas risiko pengawasan, kebocoran data, dan komersialisasi data belajar. (UNESCO Digital Library)

Dalam konteks ini, *digital citizenship* di pendidikan tidak cukup diajarkan sebagai etika bermedia sosial. Ia harus mencakup pemahaman tentang data pembelajaran, hak privasi peserta didik, risiko platform, dan reputasi digital akademik. Mahasiswa perlu memahami bahwa plagiarisme, penghinaan daring, penyebaran materi teman tanpa izin, atau pengunggahan rekaman kelas tanpa persetujuan semuanya berkaitan dengan kewargaan digital. Dosen juga perlu menyadari bahwa penggunaan aplikasi pendidikan harus mempertimbangkan data apa yang dikumpulkan dan bagaimana data itu diproses. (UNESCO)

Lebih jauh, pendidikan memiliki fungsi pembentukan kebiasaan. Jika sejak dini peserta didik dibiasakan berpikir sebelum memposting, meminta izin sebelum membagikan foto orang lain, memeriksa pengaturan privasi, memakai kata sandi kuat, dan menilai jejak digitalnya sendiri, maka mereka sedang dibekali bukan hanya keterampilan teknis, tetapi juga karakter kewargaan. UNICEF menyarankan agar anak-anak diajak memahami privasi sebagai hak, belajar sejak dini tentang jejak digital, dan diajak berdialog terbuka mengenai platform yang mereka gunakan. (UNICEF)

11. Jejak Digital dalam Dunia Kerja dan Profesional

Di dunia kerja, jejak digital memiliki pengaruh yang makin nyata terhadap reputasi profesional. Rekruter, kolega, mitra, dan klien dapat dengan mudah menemukan profil, tulisan, unggahan, atau arsip digital seseorang. eSafety Commissioner menekankan bahwa pencarian nama seseorang dapat menunjukkan apa yang orang lain—termasuk calon pemberi kerja atau teman—dapat ketahui tentang dirinya. Ini membuat jejak digital menjadi bentuk modal sosial baru, tetapi sekaligus juga risiko baru. (eSafety Commissioner)

Bagi akademisi, profesional, dan pemimpin organisasi, jejak digital dapat mendukung kredibilitas bila dikelola baik: artikel yang konsisten, presentasi publik, reputasi ilmiah, atau interaksi yang elegan. Namun jejak digital juga dapat melemahkan posisi profesional bila berisi serangan personal, unggahan emosional yang tidak proporsional, pembocoran data, atau kebiasaan mengomentari isu tanpa tanggung jawab. Dalam ruang digital, batas antara personal dan profesional semakin tipis. Karena itu, *digital citizenship* profesional menuntut disiplin diri yang lebih tinggi dibanding sekadar "bebas berekspresi". (eSafety Commissioner)

Pada tingkat organisasional, perusahaan dan institusi juga memiliki jejak digital. Jejak itu terdiri atas situs resmi, akun media sosial, arsip berita, kebijakan privasi, respons terhadap insiden, dan perilaku karyawan di

ruang publik digital. Jika organisasi lalai mengelola data, gagal melindungi privasi pelanggan, atau merespons kebocoran data secara buruk, kerusakan reputasinya bisa sangat luas. Karena itu, privasi dan jejak digital bukan hanya urusan individu, tetapi juga bagian dari tata kelola organisasi dan kepercayaan publik. NIST menempatkan hal ini sebagai bagian dari manajemen risiko privasi organisasi. (NIST)

12. Strategi Mengelola Privasi dan Jejak Digital

Walaupun jejak digital tidak mungkin dihapus sepenuhnya, ia dapat dikelola. UNICEF menyarankan beberapa langkah praktis: memeriksa dan memperbarui perangkat, meninjau pengaturan privasi aplikasi dan media sosial, membatasi izin akses kamera, mikrofon, kontak, foto, dan lokasi, memilih layanan yang meminimalkan pelacakan, menggunakan kata sandi kuat serta autentikasi multi-faktor, dan secara berkala mengecek perubahan fitur privasi. Rekomendasi ini menunjukkan bahwa perlindungan privasi adalah proses yang berkelanjutan, bukan tindakan sekali jadi. (UNICEF)

eSafety Commissioner juga menekankan pentingnya "memeriksa apa yang ada di luar sana", termasuk mencari nama sendiri di internet untuk melihat apa yang dapat ditemukan orang lain. Langkah ini tampak sederhana, tetapi sangat edukatif karena membantu seseorang menyadari bahwa jejak digital bukan sesuatu yang abstrak. Ia hadir nyata dalam hasil pencarian, arsip media sosial, unggahan organisasi, dan foto lama. Kesadaran ini sering menjadi titik awal pembentukan perilaku digital yang lebih reflektif. (eSafety Commissioner)

Dari sudut akademik, strategi pengelolaan jejak digital dapat dirumuskan dalam tiga lapis. Lapis pertama adalah pengendalian diri: pikir sebelum unggah, batasi data yang dibagikan, gunakan pengaturan privasi, dan pisahkan ruang personal serta profesional bila perlu. Lapis kedua adalah pengendalian teknis: kata sandi kuat, autentikasi multi-faktor, pembaruan perangkat lunak, pengelolaan izin aplikasi, dan pengurangan pelacakan. Lapis ketiga adalah pengendalian struktural: memilih platform

yang lebih menghormati privasi, memahami kebijakan data, dan mendukung regulasi serta tata kelola yang lebih adil. OECD dan NIST memberikan kerangka penting untuk lapis ketiga ini melalui prinsip-prinsip dan kerangka manajemen risiko privasi. (OECD)

13. Menuju Budaya Kewargaan Digital yang Dewasa

Pada akhirnya, isu *digital citizenship*, privasi, dan jejak digital tidak dapat diselesaikan hanya dengan nasihat moral kepada individu. Ia membutuhkan budaya digital yang lebih dewasa. Budaya itu harus dibangun melalui pendidikan, hukum, tata kelola platform, praktik organisasi, dan kebiasaan sehari-hari warga. UNESCO menempatkan kewargaan digital dalam kerangka yang lebih luas: membentuk warga yang terinformasi, terlibat, bertanggung jawab, dan sanggup berkontribusi pada masyarakat yang lebih inklusif dan adil. (UNESCO)

Budaya semacam ini menuntut tiga perubahan mendasar. Pertama, dari spontanitas ke refleksi: warga tidak langsung mengunggah atau membagikan sesuatu tanpa memikirkan akibatnya. Kedua, dari kepemilikan semu ke kesadaran struktural: warga memahami bahwa ruang digital bukan ruang netral, melainkan ruang yang diatur algoritma, kepentingan bisnis, dan kebijakan data. Ketiga, dari individualisme ke tanggung jawab bersama: privasi bukan hanya hak saya, tetapi juga hak orang lain; jejak digital saya tidak hanya memengaruhi saya, tetapi juga keluarga, institusi, dan komunitas saya. (Portal)

Bila tiga perubahan ini berkembang, maka *digital citizenship* tidak lagi dipahami sebagai etiket online semata, melainkan sebagai bagian dari pembentukan manusia modern. Warga digital yang matang adalah orang yang menggabungkan literasi teknologi dengan kebijaksanaan moral, kesadaran hak dengan tanggung jawab sosial, dan partisipasi publik dengan penghormatan terhadap privasi. Dalam masyarakat data, justru kualitas-kualitas inilah yang akan menentukan apakah teknologi memperkuat martabat manusia atau malah menggerusnya. (Portal)

Kesimpulan

Digital citizenship, privasi, dan jejak digital adalah tiga konsep yang tidak dapat dipisahkan. Kewargaan digital yang sejati tidak hanya menuntut kemampuan memakai teknologi, tetapi juga kemampuan berpartisipasi secara aktif, bertanggung jawab, dan etis. Privasi menjadi fondasinya karena tanpa privasi, warga tidak memiliki ruang aman untuk membangun identitas, mengambil keputusan, dan berpartisipasi tanpa rasa takut. Jejak digital menjadi ujian konkretnya karena di situlah tampak bagaimana tindakan-tindakan kecil di ruang digital dapat berakumulasi menjadi reputasi, profil, peluang, atau risiko. (Portal)

Dari pembahasan ini terlihat bahwa tantangan utama era digital bukan hanya banjir informasi, melainkan banjir data tentang manusia. Setiap klik, komentar, lokasi, unggahan, dan interaksi membentuk jejak yang dapat ditafsirkan dan dimanfaatkan oleh banyak pihak. Karena itu, warga digital perlu memiliki kesadaran baru: bahwa kehadiran digital selalu meninggalkan bekas, bahwa privasi adalah hak yang harus dijaga, dan bahwa platform serta organisasi juga harus dimintai akuntabilitas. OECD, NIST, UNESCO, UNICEF, serta kerangka hukum Indonesia sama-sama menunjukkan bahwa perlindungan data dan privasi bukan agenda pinggiran, melainkan syarat kepercayaan dalam masyarakat digital. (OECD)

Bagi pendidikan, pesan utamanya ialah bahwa kewargaan digital harus diajarkan sejak dini sebagai gabungan literasi, etika, keamanan, dan refleksi diri. Bagi organisasi, pesannya adalah bahwa data bukan sekadar aset, tetapi amanat tanggung jawab. Bagi individu, pesannya sederhana namun mendalam: apa yang kita lakukan di ruang digital bukan sesuatu yang hilang begitu saja. Ia tinggal, berkembang, dan dapat kembali memengaruhi hidup kita. Karena itu, menjadi warga digital yang baik berarti belajar hidup dengan sadar di hadapan teknologi—bukan takut padanya, tetapi juga tidak menyerahkan diri sepenuhnya kepadanya. (UNESCO)

Berikut **Glosarium** dan **Daftar Pustaka (APA 7)** untuk topik **"Digital Citizenship, Privasi, dan Jejak Digital."** Glosarium ini disusun dengan menekankan sumber normatif, pendidikan, dan perlindungan data dari Council of Europe, UNESCO, OECD, NIST, UNICEF, serta regulasi Indonesia. (Portal)

Glosarium

1. Digital citizenship / kewargaan digital
Kemampuan untuk berpartisipasi secara aktif, bertanggung jawab, dan etis dalam masyarakat digital, sambil menjalankan dan membela hak serta tanggung jawab demokratis di ruang daring. (Portal)

2. Pendidikan kewargaan digital
Proses pendidikan yang memberdayakan peserta didik agar mampu menggunakan teknologi digital secara kompeten, aman, kritis, dan bertanggung jawab dalam kehidupan sosial, sipil, dan demokratis. (Portal)

3. Privasi
Kondisi perlindungan yang memungkinkan individu mengendalikan informasi tentang dirinya, termasuk bagaimana data dikumpulkan, digunakan, dibagikan, dan diamankan. Dalam kerangka NIST, privasi dipandang sebagai risiko yang harus dikelola organisasi sambil melindungi individu. (NIST)

4. Data pribadi
Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun nonelektronik. (JDIH Kemkomdigi)

5. Pelindungan data pribadi
Keseluruhan upaya untuk melindungi data pribadi dalam seluruh rangkaian pemrosesannya guna menjamin hak konstitusional subjek data. (JDIH Kemkomdigi)

6. Jejak digital / digital footprint
Kumpulan aktivitas, tindakan, kontribusi, dan komunikasi yang dapat ditelusuri pada internet atau perangkat digital; secara sederhana, ia adalah jejak data yang terbentuk saat seseorang menggunakan internet. (Cyber.gov.au)

7. Jejak digital aktif
Data yang ditinggalkan melalui tindakan sadar atau disengaja, misalnya mengunggah di media sosial, mengisi formulir daring, atau menyetujui kuki. (Canadian Centre for Cyber Security)

8. Jejak digital pasif
Data yang tertinggal tanpa disadari atau tanpa niat langsung, misalnya melalui pelacakan alamat IP, lokasi, log aktivitas, atau pemasangan kuki oleh situs dan aplikasi. (Canadian Centre for Cyber Security)

9. Reputasi digital
Citra atau penilaian tentang seseorang yang terbentuk dari apa yang ia lakukan di internet dan juga dari apa yang orang lain unggah atau bagikan tentang dirinya. Reputasi digital dapat memengaruhi relasi sosial, pendidikan, dan peluang kerja. (eSafety Commissioner)

10. Persetujuan (consent)
Izin dari individu atas pengumpulan atau pemrosesan data pribadinya. Dalam praktik perlindungan data modern, persetujuan perlu dibaca bersama prinsip keterbukaan, pembatasan tujuan, dan akuntabilitas agar tidak menjadi formalitas semata. (OECD Legal Instruments)

11. Akuntabilitas
Prinsip bahwa organisasi atau pihak yang mengumpulkan dan mengolah

data harus bertanggung jawab atas praktik perlindungan privasi, keamanan, dan penggunaan data yang sah. (OECD Legal Instruments)

12. Pembatasan tujuan (purpose specification)
Prinsip bahwa data pribadi harus dikumpulkan untuk tujuan yang jelas dan sah, lalu tidak digunakan secara bebas di luar tujuan tersebut tanpa dasar yang tepat. (OECD Legal Instruments)

13. Keamanan data
Langkah teknis dan organisasional untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi dari kebocoran, pencurian, atau penyalahgunaan. (NIST)

14. Literasi privasi
Kemampuan memahami apa itu informasi pribadi, risiko pembagiannya, cara mengatur privasi pada platform, dan bagaimana mengelola jejak digital secara sadar. UNESCO menempatkannya sebagai bagian dari kompetensi literasi media dan informasi. (UNESCO)

15. Pengaturan privasi (privacy settings)
Fitur pada aplikasi, platform, atau perangkat yang memungkinkan pengguna mengontrol siapa yang dapat melihat data, aktivitas, lokasi, atau kontennya. Pengelolaan pengaturan ini merupakan praktik dasar perlindungan diri di ruang digital. (UNESCO)

16. Permanensi digital
Sifat informasi daring yang dapat bertahan lama, tersimpan, tersalin, atau muncul kembali meskipun pengguna merasa unggahan itu sudah lewat atau dihapus. (UNICEF)

17. Doxing
Tindakan menyebarkan informasi pribadi seseorang di internet tanpa izin, biasanya dengan maksud mempermalukan, mengintimidasi, atau membahayakan. Sebagai praktik, ini bertentangan dengan prinsip privasi dan kewargaan digital yang bertanggung jawab. (Portal)

18. Risiko privasi

Potensi kerugian terhadap individu yang timbul dari pengumpulan, pemrosesan, pembagian, atau analisis data pribadi. Dalam kerangka NIST, risiko ini perlu diidentifikasi, diprioritaskan, dan dikelola. (NIST)

Daftar Pustaka (APA 7)

Australian Signals Directorate. (n.d.). *Glossary: Digital footprint*. Cyber.gov.au. (Cyber.gov.au)

Canadian Centre for Cyber Security. (2024, February). *Digital footprint (ITSAP.00.133)*. Government of Canada. (Canadian Centre for Cyber Security)

Council of Europe. (n.d.). *Digital citizenship education*. Council of Europe. (Portal)

eSafety Commissioner. (2026, February 10). *Digital footprint*. Australian Government. (eSafety Commissioner)

eSafety Commissioner. (2025, December 10). *Digital reputation*. Australian Government. (eSafety Commissioner)

National Institute of Standards and Technology. (n.d.). *Privacy Framework*. U.S. Department of Commerce. (NIST)

National Institute of Standards and Technology. (2025, April 14). *Privacy Framework 1.1 initial public draft*. U.S. Department of Commerce. (NIST Publications)

Organisation for Economic Co-operation and Development. (2013). *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*. OECD Legal Instruments. (OECD Legal Instruments)

Organisation for Economic Co-operation and Development. (2024). *Explanatory memoranda of the OECD Privacy Guidelines*. OECD. (OECD)

UNESCO. (2024). *Global citizenship education in a digital age: Teacher guidelines*. UNESCO. (UNESCO)

UNESCO. (2024). *Unit 1: Understanding privacy in MIL*. UNESCO Media and Information Literacy for Teachers. (UNESCO)

UNESCO. (2024). *Unit 4: Media and information literacy footprints*. UNESCO Media and Information Literacy for Teachers. (UNESCO)

UNESCO. (2022). *Part 2, Module 8: Privacy, data protection and you*. UNESCO. (UNESCO Digital Library)

UNESCO. (2022). *Minding the data: Protecting learners' privacy and security*. UNESCO. (UNESCO Digital Library)

UNESCO. (2016). *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*. UNESCO. (UNESCO Digital Library)

UNICEF. (n.d.). *How to keep your child safe online*. UNICEF Parenting. (UNICEF)

UNICEF. (n.d.). *Online privacy checklist for parents*. UNICEF Parenting. (UNICEF)

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). JDIH Komdigi. (JDIH Kemkomdigi)

Copilot for this article - Chatgpt 5.2 Thinking. Access date: 15 Maret 2026 Prompting on Writer's account (Rudy C Tarumingkeng)

https://chatgpt.com/c/69b6138d-6df0-839d-b6f5-8878599c9c14