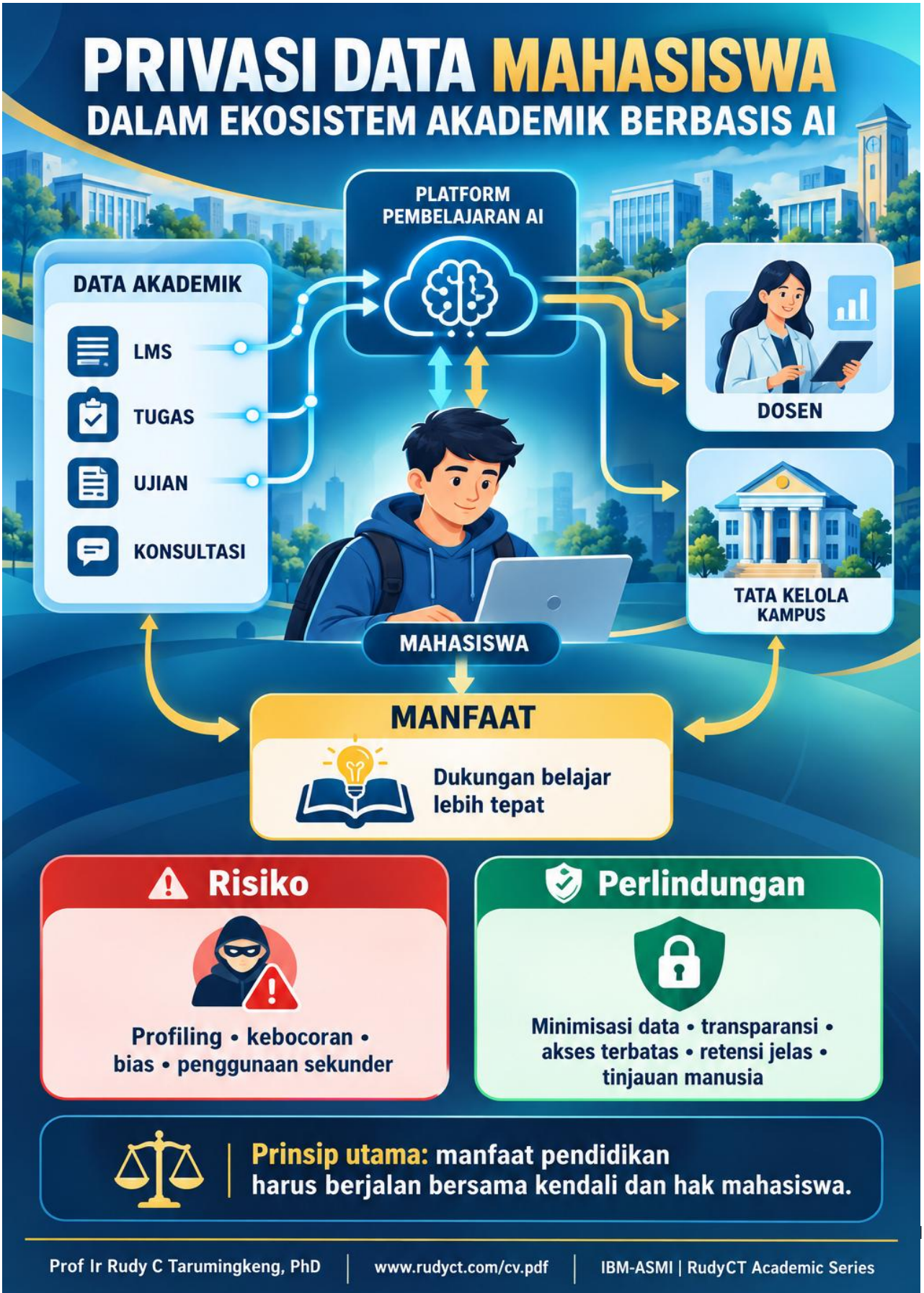

PRIVASI DATA MAHASISWA
DALAM EKOSISTEM AKADEMIK BERBASIS AI
PLATFORM PEMBELAJARAN AI
DATA AKADEMIK
LMS
TUGAS
UJIAN
KONSULTASI
DOSEN
TATA KELOLA KAMPUS
MAHASISWA
MANFAAT
Dukungan belajar lebih tepat
Risiko
Profiling • kebocoran • bias • penggunaan sekunder
Perlindungan
Minimisasi data • transparansi • akses terbatas • retensi jelas • tinjauan manusia
Prinsip utama: manfaat pendidikan harus berjalan bersama kendali dan hak mahasiswa.
Prof Ir Rudy C Tarumingkeng, PhD
www.rudyct.com/cv.pdf
IBM-ASMI | RudyCT Academic Series

Privasi Data Mahasiswa dalam Ekosistem Akademik Berbasis AI

Prof. Ir. Rudy C. Tarumingkeng, PhD
www.rudyct.com/cv.pdf

IBM-ASMI | RudyCT Academic Series | 2026

Abstrak

Artikel ini mengkaji privasi data mahasiswa dalam ekosistem akademik yang semakin bergantung pada kecerdasan buatan (AI), analitik pembelajaran, platform digital, dan layanan komputasi awan. Pembahasan mengikuti siklus data, mulai dari pengumpulan dan inferensi hingga pembagian, retensi, dan penghapusan. Topik yang dibahas mencakup ketimpangan kuasa, data 2ystem2ka, AI 2ystem2kan, pengawasan ujian, profiling, hak mahasiswa, 2ystem2ka otomatis, vendor, keamanan siber, penelitian, dan tata 2ystem perguruan tinggi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi kerangka penting di Indonesia, 2ystem2 aturan terkait yang perlu diterapkan menurut konteks dan perkembangan hukum. Argumen utama artikel ialah perlindungan privasi harus dimulai dari tujuan 2ystem2kan yang spesifik, minimisasi data, transparansi yang dapat dipahami, penilaian dampak, keamanan sejak desain, pembatasan penggunaan sekunder, serta hak koreksi dan peninjauan manusia. AI dapat mendukung pembelajaran dan layanan mahasiswa, tetapi manfaat tersebut hanya layak dipertahankan bila 2ystem dapat dikelola dan mahasiswa memiliki kendali yang bermakna. Artikel menawarkan peta jalan institusional

untuk mengaudit 3ystem, mengelola vendor, melibatkan mahasiswa, merespons insiden, dan mengevaluasi manfaat serta kerugian secara berkelanjutan.

Kata Kunci: privasi data mahasiswa; kecerdasan buatan; pendidikan tinggi; analitik pembelajaran; pelindungan data pribadi; tata kelola AI; hak subjek data; keamanan informasi

1. Pendahuluan: data mahasiswa menjadi bagian dari proses belajar

Perguruan tinggi semakin bergantung pada sistem digital untuk mengelola pendaftaran, pembelajaran, penelitian, layanan mahasiswa, evaluasi, dan komunikasi. Setiap interaksi dapat meninggalkan data: identitas, pilihan mata kuliah, aktivitas pada platform, jawaban tugas, rekaman konsultasi, penggunaan perpustakaan, hingga pola akses jaringan. Kecerdasan buatan (AI) memperluas kemungkinan pengolahan data tersebut. Sistem dapat memprediksi kebutuhan dukungan, menyusun rekomendasi materi, merangkum diskusi, menilai pola kemajuan, atau berinteraksi melalui bahasa alami. Karena data itu berhubungan dengan proses pendidikan dan kehidupan individu, privasi mahasiswa tidak lagi menjadi urusan teknis semata.

Data dapat membantu kampus meningkatkan layanan. Analitik pembelajaran dapat menunjukkan bahwa sejumlah mahasiswa kesulitan pada konsep yang sama; sistem penjadwalan dapat menemukan konflik kelas; alat aksesibilitas dapat membantu mahasiswa memakai materi dalam format yang sesuai. Namun, kemampuan untuk menyimpulkan pola juga menciptakan kuasa untuk mengamati, mengelompokkan, memperkirakan, dan memengaruhi pilihan. Jejak yang semula dikumpulkan untuk membantu belajar dapat digunakan untuk disiplin, evaluasi kinerja, pemasaran, atau keputusan administratif tanpa pemahaman mahasiswa. Pertanyaan kebijakan utamanya

ialah bagaimana manfaat pendidikan diperoleh tanpa mengubah mahasiswa menjadi objek pemantauan yang tidak memiliki kendali.

Artikel ini membahas privasi data mahasiswa dalam ekosistem akademik berbasis AI secara naratif dan komprehensif. Pembahasan mencakup jenis dan siklus data, hubungan kuasa, landasan hukum Indonesia, persetujuan dan hak subjek data, analitik, AI generatif, pengawasan ujian, tata kelola vendor, keamanan, penelitian, serta mekanisme institusi. Tesis tulisan ini ialah bahwa perlindungan privasi perlu dimulai dari tujuan dan desain layanan, bukan hanya dari persetujuan formal atau kebijakan yang dibaca sekali. Kampus harus membuktikan bahwa data yang diproses memang diperlukan, pengguna memahami dampaknya, dan ada tanggung jawab nyata ketika sistem salah.

2. Arti privasi data dalam konteks pendidikan tinggi

Privasi data adalah kemampuan seseorang untuk memahami dan memengaruhi bagaimana informasi yang berkaitan dengannya dikumpulkan, diolah, disimpan, dibagikan, dan digunakan untuk mengambil keputusan. Dalam pendidikan, privasi memiliki dimensi relasional: mahasiswa berinteraksi dengan institusi yang memiliki kewenangan atas nilai, akses layanan, kemajuan studi, dan gelar. Perlindungan tidak cukup dinilai dari apakah data dirahasiakan dari publik. Data yang tidak pernah bocor pun dapat dipakai secara tidak semestinya oleh unit internal atau penyedia layanan apabila tujuan, akses, dan akibatnya tidak dikendalikan.

Privasi berkaitan dengan martabat, otonomi, kebebasan bereksperimen, dan kepercayaan. Mahasiswa perlu ruang untuk bertanya, mencoba, membuat kesalahan, serta mengubah pendapat tanpa setiap tindakan menjadi catatan permanen. Sistem pembelajaran yang mencatat seluruh klik dapat membuat pengguna merasa selalu dinilai. Perasaan itu memengaruhi perilaku:

mahasiswa mungkin tidak membuka materi yang menandakan kesulitan, tidak mencari konseling, atau memilih jawaban yang dianggap aman. Karena itu, dampak privasi mencakup efek psikologis dan sosial selain potensi kerugian finansial atau pencurian identitas.

Privasi juga tidak berarti menutup semua data dari penggunaan yang bermanfaat. Mahasiswa dapat memilih berbagi informasi tertentu untuk memperoleh dukungan, dan institusi memerlukan data administrasi untuk menyelenggarakan pendidikan. Perbedaan penting terletak pada kejelasan tujuan, proporsionalitas, dasar pemrosesan, perlindungan, pembatasan akses, dan kemampuan untuk mengajukan keberatan. Kampus perlu menghindari dua anggapan: bahwa setiap pengumpulan data adalah pelanggaran, atau bahwa semua pengumpulan dapat diterima selama disebut membantu pembelajaran.

3. Ekosistem akademik digital dan aktor yang memproses data

Ekosistem akademik digital terdiri atas sistem informasi mahasiswa, platform manajemen pembelajaran, konferensi video, repositori, layanan perpustakaan, aplikasi ujian, sistem pembayaran, alat identitas, layanan konseling, dan produk AI. Data dapat berpindah di antara sistem melalui integrasi, ekspor, API, akun tunggal, atau unggahan manual. Tiap sambungan menambah titik pemrosesan dan pihak yang mungkin memperoleh akses. Peta ekosistem perlu menunjukkan bukan hanya aplikasi yang terlihat mahasiswa, melainkan layanan di belakangnya, subprosesor, lokasi penyimpanan, dan mekanisme dukungan.

Aktor yang terlibat mencakup mahasiswa, dosen, penasihat akademik, unit teknologi, biro akademik, pusat pembelajaran, perpustakaan, peneliti, vendor, penyedia komputasi awan, serta lembaga pemerintah. Tanggung jawab hukum dan operasional bergantung pada tujuan dan cara pemrosesan

masing-masing, bukan semata pada nama jabatan atau label kontrak. Satu institusi dapat mengendalikan data untuk layanan akademik dan bertindak sebagai prosesor untuk penelitian pihak lain. Pemetaan peran sejak awal menghindari asumsi bahwa vendor otomatis memikul seluruh kewajiban atau kampus dapat melepaskan akuntabilitas.

Sistem AI sering bergantung pada layanan berlapis. Aplikasi kampus mungkin mengirim prompt ke model penyedia, yang menggunakan layanan pemantauan, penyimpanan, dan analitik dari pihak lain. Data dapat dipindahkan melintasi batas organisasi atau negara. Mahasiswa mungkin melihat satu kotak percakapan, sementara pemrosesan melibatkan banyak komponen. Transparansi harus menggambarkan alur tersebut dalam bahasa yang dapat dipahami. Keterbatasan teknis vendor tidak menghapus tanggung jawab institusi untuk memilih alat yang sesuai dan membatasi data yang dibagikan.

4. Siklus hidup data mahasiswa

Siklus data dimulai ketika informasi dibuat atau dikumpulkan, kemudian digunakan, disimpan, dikirim, diubah, digabungkan, diarsipkan, dan akhirnya dihapus atau dimusnahkan. Setiap tahap memiliki risiko dan kebutuhan pengendalian yang berbeda. Formulir pendaftaran dapat meminta data berlebih; penyimpanan dapat tidak menetapkan masa retensi; transfer dapat memakai kanal yang tidak aman; penghapusan dapat gagal karena salinan cadangan. Analisis privasi yang hanya menilai layar aplikasi tidak melihat seluruh siklus tersebut.

Data juga dapat diturunkan dari informasi awal. Sistem mungkin menyimpulkan bahwa mahasiswa berisiko gagal, memiliki preferensi belajar tertentu, atau memerlukan konseling berdasarkan pola aktivitas. Inferensi tetap dapat berdampak pada individu walaupun bukan fakta yang

disampaikan secara langsung. Kampus perlu mencatat sumber, tujuan, ketidakpastian, masa berlaku, dan pihak yang boleh melihat inferensi. Kesimpulan probabilistik tidak semestinya disimpan seolah-olah merupakan fakta biografis yang telah diverifikasi.

Penghapusan harus mencakup salinan aktif, ekspor, log, penyimpanan vendor, dan cadangan menurut jadwal yang dapat dijelaskan. Kewajiban arsip, akreditasi, audit, dan penyelesaian sengketa dapat menuntut retensi tertentu, tetapi alasan tersebut perlu dibatasi pada kategori data dan jangka waktu yang berlaku. Penghapusan tidak selalu berarti menghilangkan setiap catatan resmi yang wajib dipertahankan. Kampus menerangkan pembedaan ini kepada mahasiswa dan mendokumentasikan keputusan retensi.

5. Kategori data yang lazim diproses

Data identitas dapat meliputi nama, nomor mahasiswa, kontak, kewarganegaraan, dan informasi akun. Data akademik mencakup pendaftaran, kehadiran, nilai, tugas, catatan bimbingan, serta keputusan kemajuan studi. Data interaksi digital meliputi log masuk, klik, waktu akses, pencarian, pesan, unggahan, dan penggunaan fitur AI. Data finansial, lokasi, kesehatan, biometrik, disabilitas, latar keluarga, serta catatan disiplin mungkin diproses oleh unit tertentu. Hubungan antarjenis data dapat meningkatkan risiko karena kombinasi yang tampak biasa bisa mengenali individu.

Isi percakapan dengan AI dapat memuat pertanyaan tugas, draf, pandangan politik, informasi kesehatan, pengalaman pribadi, atau data pihak ketiga. Mahasiswa mungkin menempelkan transkrip wawancara, catatan kasus, atau dokumen organisasi tanpa menyadari bahwa layanan menyimpan prompt. Panduan penggunaan harus memberi contoh konkret tentang informasi yang tidak boleh dimasukkan. Institusi juga dapat menyediakan alat yang telah

disaring untuk tugas akademik sehingga mahasiswa tidak harus menebak tingkat perlindungan setiap produk.

Data yang tampak anonim dapat menjadi teridentifikasi kembali jika digabungkan dengan sumber lain. Waktu akses, program studi, pola mata kuliah, dan lokasi dapat membentuk kombinasi unik. Karena itu, institusi tidak menyamakan penghapusan nama dengan anonimisasi yang kuat. Pemisahan kunci, agregasi, pengurangan presisi, dan pembatasan akses dapat menurunkan risiko, tetapi metode perlu diuji sesuai konteks. Data yang tetap memungkinkan identifikasi atau pengaitan harus diperlakukan hati-hati.

6. Data pribadi umum, data spesifik, dan kehati-hatian klasifikasi

Undang-Undang Nomor 27 Tahun 2022 membedakan data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Kelompok spesifik meliputi, antara lain, data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan kategori lain yang ditentukan peraturan. Informasi akademik mahasiswa tidak otomatis seluruhnya masuk kategori spesifik hanya karena berkaitan dengan pendidikan. Namun, catatan nilai, identitas, dan pola belajar tetap dapat menjadi data pribadi ketika mengidentifikasi atau dapat mengidentifikasi seseorang.

Klasifikasi harus mempertimbangkan konteks. Catatan akomodasi mungkin mengungkap disabilitas atau kondisi kesehatan; rekaman ujian dapat mengandung biometrik; daftar penerima bantuan dapat menunjukkan kondisi ekonomi. Penggabungan beberapa atribut dapat menambah sensitivitas walau tiap atribut sendiri tampak biasa. Tim privasi, akademik, dan teknologi membuat inventaris kategori dengan melihat isi, tujuan, kemungkinan inferensi, dan akibat jika data disalahgunakan.

Label internal seperti “data akademik”, “data analitik”, atau “data nonrahasia” bukan penentu tunggal kewajiban. Kampus menggunakan klasifikasi untuk

menetapkan akses, retensi, enkripsi, dan prosedur berbagi. Jika suatu kategori belum jelas, pilihan yang lebih berhati-hati adalah membatasi pemrosesan sampai penilaian hukum dan risiko dilakukan. Klasifikasi yang dapat ditinjau lebih berguna daripada skema rumit yang tidak dipahami pemilik sistem.

7. Ketimpangan informasi dan posisi tawar mahasiswa

Hubungan mahasiswa dengan kampus tidak setara dalam seluruh aspek pemrosesan. Kampus menentukan sistem yang wajib dipakai, mengelola nilai, dan mengatur akses pada pendidikan. Penolakan terhadap sebuah layanan dapat terasa sebagai risiko akademik meskipun institusi menyebutnya opsional. Persetujuan karena itu perlu dinilai dari kebebasan yang nyata, bukan hanya keberadaan kotak centang. Mahasiswa perlu mengetahui alternatif yang dapat digunakan dan apakah pilihan mereka memengaruhi layanan atau penilaian.

Ketimpangan juga muncul karena mahasiswa mungkin tidak mengetahui istilah pemrosesan, subprosesor, profil, atau pelatihan model. Dokumen hukum panjang dapat memenuhi formalitas tetapi gagal memberi pemahaman praktis. Kampus menyediakan pemberitahuan berlapis: penjelasan ringkas saat pengumpulan, rincian kebijakan yang dapat dibuka, dan contoh alur data. Bahasa sederhana tidak mengganti informasi hukum yang diperlukan, tetapi membuat keputusan lebih bermakna.

Mahasiswa internasional, mahasiswa baru, pengguna bahasa kedua, dan mahasiswa yang mengandalkan teknologi bantu dapat menghadapi hambatan tambahan. Mereka memerlukan saluran pertanyaan yang mudah dijangkau dan penjelasan dalam format aksesibel. Perwakilan mahasiswa dilibatkan dalam pengujian pemberitahuan dan proses persetujuan. Bila pengguna tidak dapat memahami pilihan yang ditawarkan, institusi

seharusnya memperbaiki proses, bukan menganggap diam sebagai pemahaman.

8. Tujuan pendidikan dan batas pemantauan

Tujuan penggunaan harus dirumuskan sebelum data dikumpulkan. Tujuan seperti “meningkatkan keberhasilan akademik” terlalu luas untuk menentukan informasi apa yang perlu dihimpun dan bagaimana hasil digunakan. Tujuan yang lebih operasional, misalnya mendeteksi kesulitan konsep pada satu mata kuliah agar dosen menyiapkan dukungan, memiliki batas lebih jelas. Kampus mencatat penerima manfaat, dasar pedagogis, jenis keputusan, pihak yang memperoleh akses, serta ukuran untuk menilai keberhasilan.

Pemantauan dapat bergeser dari dukungan ke pengawasan ketika log aktivitas dipakai untuk mengukur ketekunan, disiplin, atau kesesuaian perilaku tanpa dasar pedagogis kuat. Jumlah klik bukan ukuran yang dapat diandalkan atas perhatian atau pemahaman. Penggunaan kamera, pelacakan mata, analisis emosi, atau keystroke monitoring membawa tingkat intrusi lebih tinggi dan memerlukan justifikasi yang jauh lebih ketat. Institusi harus membandingkannya dengan alternatif yang lebih sedikit mengganggu.

Prinsip proporsionalitas meminta kampus menimbang manfaat yang spesifik terhadap intrusi, risiko, dan dampak pada hubungan belajar. Jika tujuan dapat dicapai melalui survei sukarela atau tugas formatif, pengumpulan sensor multimodal mungkin tidak diperlukan. Beberapa bentuk pemantauan dapat dilarang oleh kebijakan kampus meskipun secara teknis tersedia. Menetapkan batas sejak awal mencegah normalisasi pengumpulan tanpa tujuan yang terukur.

9. Profil, inferensi, dan label risiko

Profiling menggunakan data untuk menilai atau memperkirakan aspek seseorang, misalnya kinerja, preferensi, perilaku, atau risiko. Sistem peringatan dini dapat memperkirakan kemungkinan mahasiswa tidak menuntaskan mata kuliah dan mendorong kontak penasihat. Tujuan dukungan ini dapat bernilai, tetapi inferensi tetap tidak pasti. Model mungkin keliru menganggap akses yang jarang sebagai kurang motivasi, padahal mahasiswa bekerja atau menghadapi kendala jaringan. Informasi kontekstual sering tidak terdapat pada sistem.

Label risiko dapat memengaruhi cara staf memperlakukan mahasiswa. Jika penasihat melihat tanda “berisiko tinggi” tanpa memahami akurasi atau sebabnya, ia mungkin menurunkan ekspektasi atau mengarahkan mahasiswa menjauhi mata kuliah menantang. Kampus memastikan label bersifat sementara, terbatas pada pihak yang membutuhkan, dijelaskan tingkat ketidakpastiannya, dan tidak dijadikan dasar tunggal keputusan yang berdampak besar. Mahasiswa dapat mengetahui bahwa sistem menghasilkan prediksi dan meminta tinjauan.

Prediksi lebih etis ketika memicu tawaran dukungan yang tidak menghukum. Kontak awal dapat menyatakan bahwa kampus menyediakan konsultasi, bukan mengumumkan diagnosis kegagalan. Sistem dievaluasi untuk false positives, false negatives, dampak per kelompok, dan manfaat dukungan setelah peringatan. Bila tidak ada intervensi yang mampu menolong, membuat prediksi saja dapat memperbesar pengawasan tanpa manfaat. Karena itu, sumber daya pendampingan harus dirancang bersama alat prediksi.

10. Sistem AI dan sumber data tambahannya

AI di kampus dapat berupa sistem rekomendasi, tutor cerdas, analitik prediktif, pemrosesan bahasa, penilaian otomatis, pencarian semantik, atau model generatif. Sistem berbeda dalam data masukan, tujuan, logika, risiko kesalahan, dan kemampuan menjelaskan keluaran. Kampus tidak seharusnya menganggap "AI" sebagai satu kategori dengan risiko seragam. Inventaris sistem menjelaskan penggunaan spesifik, tingkat dampak, integrasi, versi model, dan pemilik akademik yang bertanggung jawab.

Model generatif dapat menerima teks, berkas, gambar, audio, atau video. Prompt dapat disimpan untuk pemantauan kualitas atau digunakan sesuai syarat layanan. Sistem mungkin juga memproses metadata tentang akun, perangkat, dan waktu interaksi. Sebelum pemakaian, institusi memeriksa pengaturan retensi dan pelatihan, lokasi layanan, subprosesor, mekanisme penghapusan, serta kontrak. Klaim vendor bahwa data "aman" perlu diterjemahkan ke kontrol teknis dan kewajiban yang dapat diverifikasi.

Sumber data juga dapat mencakup materi kuliah, basis pengetahuan institusi, rekaman kelas, dan dokumen perpustakaan. Data milik dosen, mahasiswa lain, atau pihak ketiga tidak bebas digunakan hanya karena tersedia di platform. Hak cipta, kerahasiaan penelitian, dan privasi orang yang muncul dalam materi perlu dipertimbangkan. Konten AI dapat mengutip atau merekonstruksi informasi yang seharusnya tetap terbatas. Kampus menetapkan sumber yang diizinkan dan proses penyaringan.

11. Analitik pembelajaran dan pendidikan berbasis data

Analitik pembelajaran mengukur dan menganalisis data tentang peserta didik serta konteks belajar untuk memahami dan mengoptimalkan pembelajaran. Analitik deskriptif menjelaskan pola yang terjadi; analitik prediktif memperkirakan kemungkinan hasil; analitik preskriptif menyarankan tindakan.

Semakin jauh keluaran bergerak dari laporan menuju tindakan otomatis, semakin besar kebutuhan pengawasan dan justifikasi. Pardo dan Siemens (2014) mengusulkan prinsip etika dan privasi yang menekankan transparansi, kontrol, akses, dan tanggung jawab terhadap penggunaan data.

Dasbor dapat membantu dosen menemukan konsep yang belum dikuasai banyak mahasiswa. Namun, sistem dapat memberi kesan objektivitas yang tidak sejalan dengan mutu data. Jika platform hanya merekam aktivitas digital, mahasiswa yang belajar melalui buku cetak atau kelompok tatap muka mungkin tampak tidak aktif. Analitik perlu dilengkapi konteks dan verifikasi. Tim kursus menyepakati bahwa hasil digunakan untuk memperbaiki pengajaran, bukan mengawasi kepatuhan secara tersembunyi.

Meta-analisis sistematis tentang AI pendidikan tinggi menunjukkan bahwa bidang ini memerlukan keterlibatan pendidik serta perhatian pada etika, kolaborasi, dan ketelitian riset (Zawacki-Richter et al., 2019; Bond et al., 2024). Kajian human-centred learning analytics dan AI juga menyoroti pentingnya melibatkan pengguna dalam desain dan menjaga keseimbangan kendali manusia dan otomatisasi (Alfredo et al., 2024). Privasi karena itu menyangkut siapa yang menentukan pertanyaan analitik dan siapa yang dapat menolak interpretasinya.

12. AI generatif dan jejak percakapan mahasiswa

Mahasiswa menggunakan AI generatif untuk meminta penjelasan, menyusun ide, memperbaiki bahasa, membuat kode, merangkum bacaan, atau menguji argumen. Percakapan dapat mengungkap pengetahuan, kebingungan, minat, keyakinan, dan kebiasaan kerja. Jika model dioperasikan oleh penyedia eksternal, interaksi mungkin tunduk pada kebijakan retensi dan penggunaan data yang berbeda dari LMS kampus. Institusi menyediakan panduan yang

menunjukkan bagaimana memilih produk dan pengaturan yang sesuai untuk kegiatan akademik.

Log percakapan dapat bernilai bagi penelitian pembelajaran, tetapi pemanfaatan sekunder harus dinilai terpisah dari layanan awal. Mahasiswa yang meminta bantuan untuk belajar belum tentu berharap percakapannya menjadi bahan evaluasi dosen atau penelitian. Kampus menetapkan apakah log diperlukan, berapa lama disimpan, bagaimana identitas dipisahkan, dan siapa yang dapat mengakses. Jika analisis bukan syarat layanan, institusi mempertimbangkan pilihan untuk tidak menyimpan atau memberi pilihan opt-out yang nyata.

AI generatif dapat menghasilkan ringkasan, inferensi, atau klasifikasi baru dari isi percakapan. Keluaran tersebut mungkin lebih sensitif daripada prompt awal, terutama bila menyimpulkan kesehatan mental, kemampuan, atau kepribadian. Model dapat membuat inferensi yang salah tetapi tetap memengaruhi keputusan manusia. Kebijakan membatasi kategori inferensi dan penggunaannya, serta melarang kesimpulan spekulatif dijadikan catatan mahasiswa permanen.

13. Data multimodal, biometrik, dan pengawasan ujian

Sistem ujian jarak jauh dapat memproses rekaman wajah, suara, gerakan, tampilan layar, lokasi, atau pola mengetik. Informasi tersebut dapat melibatkan data biometrik dan menghasilkan peringatan mengenai perilaku yang dianggap mencurigakan. Kesalahan sistem dapat terjadi karena pencahayaan, warna kulit, kondisi ruang, disabilitas, koneksi, atau perangkat. Kampus menilai akurasi menurut kelompok, prosedur banding, dan dampak psikologis sebelum memilih teknologi semacam itu.

Pengawasan yang intrusif tidak otomatis meningkatkan integritas akademik. Tugas autentik, ujian lisan, portofolio, variasi soal, dan desain penilaian yang

menguji proses dapat menjadi alternatif. Pilihan yang lebih ringan sering sekaligus memberi bukti belajar yang lebih baik. Jika proctoring tetap digunakan, kampus menjelaskan data yang direkam, masa simpan, penerima, cara keberatan, serta akomodasi bagi mahasiswa yang tidak dapat menggunakan metode standar.

Mahasiswa harus memiliki saluran untuk mengoreksi flag sistem sebelum keputusan pelanggaran dibuat. Tidak ada skor otomatis yang cukup untuk menyimpulkan kecurangan. Penelaah manusia perlu diberi bukti relevan, pelatihan, waktu, dan kewenangan mengabaikan sistem. Rekaman sensitif tidak disimpan lebih lama dari kebutuhan. Prosedur tersebut penting karena tuduhan dapat menimbulkan konsekuensi akademik dan reputasi yang serius.

14. Penggabungan data dan risiko re-identifikasi

Data yang terpisah dapat berubah makna ketika digabung. Nilai, jadwal, lokasi, penggunaan Wi-Fi, transaksi, dan interaksi perpustakaan dapat membentuk profil terperinci. Penggabungan mungkin dilakukan untuk efisiensi atau personalisasi, tetapi batas tujuan perlu dipertahankan. Setiap permintaan untuk menghubungkan dua sistem menyebut manfaat, atribut yang dibutuhkan, akses, lama penggunaan, serta risiko inferensi baru. Keputusan integrasi ditinjau oleh fungsi akademik, privasi, dan keamanan.

Anonimisasi sulit jika dataset memiliki atribut langka atau deret waktu yang panjang. Pseudonimisasi mengganti pengenal langsung tetapi masih memungkinkan pemulihan identitas melalui kunci atau kombinasi informasi. Karena itu, istilah “data anonim” hanya dipakai setelah penilaian risiko yang memadai. Akses ke kunci identitas dipisahkan, hasil disajikan secara agregat, dan ukuran kelompok kecil ditekan bila dapat mengungkap individu.

Data sintetis dapat mengurangi paparan catatan nyata untuk pengujian, tetapi tidak otomatis bebas risiko. Model dapat menghafal contoh, meniru individu,

atau menghasilkan catatan yang mengungkap pola populasi. Uji kebocoran dan pemeriksaan independen diperlukan sesuai tujuan. Kampus menggunakan data dummy dalam demonstrasi kelas ketika data mahasiswa asli tidak dibutuhkan. Mengurangi data yang dipakai sering lebih sederhana dan lebih efektif daripada berusaha mengamankan salinan yang tidak perlu.

15. Landasan hukum Indonesia dan batas penafsiran

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi kerangka utama pelindungan data di Indonesia. UU ini memuat asas, hak subjek data, pemrosesan, kewajiban pengendali dan prosesor, transfer data, sanksi, kelembagaan, dan penyelesaian sengketa. Masa penyesuaian dua tahun setelah pengundangan telah berlalu pada Oktober 2024. Perguruan tinggi perlu meninjau prosesnya terhadap UU tersebut dan perkembangan aturan pelaksana serta penegakan yang berlaku pada saat kegiatan dilakukan. Naskah ini menjelaskan prinsip secara umum, bukan pendapat hukum untuk kasus tertentu. (Republik Indonesia, 2022).

UU PDP menyebut hak subjek data, antara lain hak memperoleh informasi, memperbaiki data, mengakses, menarik persetujuan dalam kondisi yang relevan, mengakhiri atau menghapus pemrosesan sesuai ketentuan, serta mengajukan keberatan terhadap keputusan yang hanya didasarkan pada pemrosesan otomatis dan berdampak signifikan. Penerapan hak bergantung pada kondisi dan pengecualian dalam undang-undang. Kampus perlu memiliki prosedur untuk menerima, memverifikasi, dan menjawab permintaan, bukan hanya mencantumkan daftar hak pada kebijakan.

Perguruan tinggi juga mematuhi aturan sektor, kontrak, dan kebijakan institusi lain yang berlaku. Bila layanan menyasar atau melibatkan anak, aturan pelindungan anak di ruang digital dapat relevan, termasuk PP Nomor 17 Tahun 2025. Penggunaan lintas negara dapat membawa kewajiban tambahan

sesuai lokasi subjek, penyedia, atau pemrosesan. Unit hukum dan pelindungan data perlu mengonfirmasi aturan terkini serta hubungan antarperaturan sebelum peluncuran sistem berskala besar.

16. Prinsip pemrosesan yang sah dan bertanggung jawab

Kampus merumuskan tujuan yang spesifik dan sah untuk setiap aktivitas pemrosesan. Informasi yang diminta harus relevan, tidak berlebihan, akurat, serta dijaga sesuai tingkat risikonya. Data tidak digunakan untuk tujuan baru yang tidak selaras tanpa penilaian dasar dan pemberitahuan yang sesuai. Prinsip ini mendorong institusi menolak pengumpulan “untuk berjaga-jaga” karena data yang tidak digunakan tetap menambah risiko kebocoran, akses internal, dan inferensi.

Prinsip akuntabilitas berarti institusi mampu menunjukkan bagaimana kewajiban dipenuhi. Dokumentasi dapat mencakup inventaris pemrosesan, penilaian dampak, catatan keputusan, kebijakan akses, bukti pelatihan, dan kontrak vendor. Dokumen harus terkait praktik nyata. Kebijakan privasi yang menyatakan data dihapus dalam 30 hari tidak bermanfaat jika log tersimpan berbulan-bulan pada subprosesor tanpa mekanisme penghapusan.

Prinsip etis melengkapi kepatuhan hukum. Kegiatan dapat memenuhi syarat formal tetapi masih mengejutkan mahasiswa, menimbulkan ketimpangan, atau merusak kepercayaan. Kajian privasi mahasiswa dalam learning analytics menganjurkan perhatian yang melampaui solusi teknis dan mempertimbangkan konteks relasi pendidikan (Prinsloo, 2022; Pardo & Siemens, 2014). Institusi mempertimbangkan apakah pemrosesan itu pantas, perlu, dapat diterima, dan bermanfaat bagi mahasiswa.

17. Menentukan peran pengendali dan prosesor

Dalam banyak layanan kampus, perguruan tinggi menentukan alasan dan tujuan pengolahan data mahasiswa. Vendor dapat bertindak sebagai prosesor untuk menyediakan layanan sesuai instruksi, tetapi kedudukan bergantung pada fakta dan perjanjian. Beberapa penyedia dapat menentukan tujuan sendiri untuk keamanan, analitik produk, atau pelatihan model. Kampus harus memeriksa fungsi nyata, bukan menerima label kontrak tanpa evaluasi. Bila peran beberapa pihak tumpang tindih, tanggung jawab perlu disepakati dan dijelaskan.

Pengendali menetapkan proses untuk menghormati hak subjek data dan mengelola risiko. Prosesor menyediakan bantuan, keamanan, penghapusan, pemberitahuan insiden, dan dukungan audit sesuai perjanjian serta aturan yang berlaku. Subprosesor perlu diungkap dan dikendalikan. Kampus menyimpan daftar penyedia penting sehingga dapat mengetahui siapa yang menerima data ketika mahasiswa menggunakan suatu platform.

Penanggung jawab internal harus jelas pada tingkat institusi dan sistem. Kepala unit akademik memegang tujuan pedagogis; teknologi mengelola integrasi dan kontrol; fungsi privasi menilai kewajiban; pengadaan mengelola kontrak; pimpinan memutuskan risiko residual. Pembagian ini tidak mengurangi tanggung jawab institusi secara keseluruhan. Sebaliknya, ia menghindari situasi ketika semua pihak menganggap unit lain yang bertanggung jawab.

18. Dasar pemrosesan, persetujuan, dan pilihan yang nyata

Persetujuan merupakan salah satu dasar pemrosesan, tetapi bukan satu-satunya dasar yang dapat berlaku. Kampus menentukan dasar untuk tiap tujuan berdasarkan ketentuan hukum dan konteks; ia tidak mengandalkan persetujuan generik hanya karena cara itu paling mudah. Persetujuan harus

diberikan secara bebas, spesifik, diinformasikan, dan dapat ditarik sesuai hukum. Dalam hubungan pendidikan yang mengandung ketergantungan, institusi menilai apakah mahasiswa benar-benar dapat menolak tanpa kehilangan layanan esensial.

Untuk fitur opsional seperti analitik tambahan atau penggunaan percakapan bagi penelitian, pilihan sebaiknya terpisah dari persyaratan pendaftaran. Mahasiswa mengetahui manfaat, risiko, siapa yang menerima informasi, dan alternatif tanpa fitur. Tidak merespons tidak dianggap sebagai persetujuan untuk tujuan tambahan. Penarikan persetujuan memiliki mekanisme yang jelas dan tidak menghapus catatan akademik yang wajib dipertahankan berdasarkan dasar lain.

Persetujuan bukan pengganti keamanan dan pembatasan tujuan. Mahasiswa tidak dapat mengesahkan praktik yang melanggar kewajiban hukum atau memindahkan seluruh tanggung jawab ke pengguna. Kampus juga tidak meminta persetujuan untuk sesuatu yang tidak mampu dijelaskan, misalnya penggunaan prompt untuk melatih model tanpa rincian. Jika dasar pemrosesan tidak jelas, sistem tidak diluncurkan sampai penilaian yang tepat dilakukan.

19. Perlindungan mahasiswa di bawah umur

Sebagian mahasiswa pendidikan tinggi mungkin berusia di bawah 18 tahun, terutama pada program percepatan atau jalur tertentu. UU PDP menggolongkan data pribadi anak sebagai data spesifik dan mengatur pemrosesannya dengan persetujuan orang tua atau wali sesuai ketentuan. Kampus memeriksa usia dan konteks layanan tanpa mengumpulkan bukti identitas tambahan yang berlebihan. Persetujuan wali tidak menghapus kebutuhan menjelaskan penggunaan data kepada anak dalam bahasa yang sesuai.

Layanan digital yang dapat diakses oleh anak juga perlu memperhatikan PP Nomor 17 Tahun 2025 mengenai tata kelola penyelenggaraan sistem elektronik dalam pelindungan anak. Perguruan tinggi menilai kewajiban yang relevan menurut jenis layanan dan kelompok pengguna. Pengaturan usia bukan sekadar prosedur teknis; ia berhubungan dengan desain yang aman, pembatasan fitur berisiko, akses bantuan, dan pengolahan data yang sesuai. (Republik Indonesia, 2025).

Mahasiswa muda tetap memiliki martabat dan suara dalam keputusan tentang data mereka. Kampus menyediakan kanal untuk mengajukan pertanyaan, memperoleh bantuan, dan melaporkan masalah. Data anak dibatasi akses dan retensinya, serta tidak dipakai untuk pemasaran atau profil risiko yang tidak diperlukan. Ketika program memiliki mahasiswa dengan rentang usia beragam, kebijakan menjelaskan perbedaan prosedur secara adil.

20. Hak mahasiswa sebagai subjek data

Hak data menjadi operasional hanya jika mahasiswa tahu cara menggunakannya. Kampus menyediakan kanal permintaan yang mudah ditemukan, memberi nomor pelacakan, menjelaskan bukti identitas yang diperlukan, dan menetapkan proses respons. Permintaan dapat menyangkut akses, koreksi, penghapusan, keberatan, atau informasi tentang pemrosesan. Institusi melatih petugas untuk mengenali permintaan walau mahasiswa tidak menggunakan istilah hukum yang tepat.

Koreksi data penting ketika kesalahan administratif memengaruhi akses kelas, nilai, atau rekomendasi. Sistem perlu mengarahkan mahasiswa kepada unit pemilik data dan menjaga riwayat perubahan yang diperlukan untuk audit. Penghapusan dapat dibatasi oleh kewajiban arsip atau penyelesaian sengketa, tetapi kampus memberi alasan dan menjelaskan data mana yang dapat

dihapus, dibatasi, atau dianonimkan. Hak bukan sekadar formulir penolakan otomatis.

Mahasiswa juga berhak mengajukan keberatan pada proses pengambilan keputusan otomatis yang berdampak signifikan dalam cakupan UU. Kampus membuat prosedur peninjauan manusia yang benar-benar dapat mengubah hasil. Peninjau memahami dasar rekomendasi, bukti, dan konteks yang tidak tercatat. Statistik permintaan hak, waktu respons, dan jenis masalah ditinjau secara agregat untuk memperbaiki sistem.

21. Keputusan otomatis dan peninjauan manusia

Keputusan pendidikan berdampak besar dapat meliputi penerimaan, kelulusan, nilai, beasiswa, sanksi, kemajuan studi, atau akses akomodasi. AI dapat membantu meringkas berkas atau mengurutkan kasus, namun keputusan akhir perlu mengikuti hukum, kebijakan akademik, dan prosedur keadilan. Penggunaan skor sebagai penentu otomatis meningkatkan risiko kesalahan yang sulit diketahui mahasiswa. Institusi menilai konsekuensi, akurasi, penjelasan, dan jalur keberatan sebelum sistem digunakan.

Peninjauan manusia tidak bermakna bila petugas hanya mengesahkan rekomendasi algoritme. Peninjau memerlukan informasi, waktu, pelatihan, dan wewenang untuk menolak keluaran. Antarmuka sebaiknya tidak menonjolkan satu angka seolah sudah menjadi jawaban. Catatan keputusan menunjukkan bukti apa yang diperiksa dan alasan hasil ditetapkan. Mahasiswa mengetahui bahwa manusia dapat mempertimbangkan konteks dan menghubungi pihak yang tepat.

Otomatisasi juga dapat memengaruhi mahasiswa secara tidak langsung, misalnya ketika peringatan menentukan siapa yang dihubungi lebih dulu. Walau bukan keputusan akhir, prioritas tersebut dapat mengubah akses bantuan. Kampus mengaudit distribusi intervensi dan memastikan mahasiswa

yang tidak terdeteksi tetap memiliki cara meminta dukungan. Penilaian dampak mempertimbangkan sistem dan proses yang dibangunnya, bukan hanya label “keputusan otomatis”.

22. Transparansi, pemberitahuan, dan keterjelasan

Pemberitahuan privasi menjelaskan data yang dikumpulkan, tujuan, dasar pemrosesan, masa retensi, penerima, kemungkinan transfer, dan cara menggunakan hak. Dalam sistem AI, penjelasan juga menyebut kapan data dikirim ke model, apakah prompt disimpan, apakah keluaran dipakai untuk keputusan, serta keterbatasan sistem. Informasi disajikan pada saat relevan, bukan hanya pada halaman umum yang jarang dibuka mahasiswa.

Keterjelasan keputusan berbeda dari menjelaskan seluruh parameter model. Mahasiswa memerlukan alasan yang bermakna untuk tindakan yang memengaruhi mereka: data apa yang berkontribusi, tujuan yang dinilai, tingkat ketidakpastian, dan pilihan koreksi. Dosen dan staf juga membutuhkan panduan agar tidak menganggap prediksi sebagai bukti yang pasti. Sistem menyediakan dokumentasi yang sesuai tingkat pengguna.

Transparansi mencakup perubahan. Jika vendor mengubah model, data, atau retensi, institusi menilai ulang dan memperbarui pemberitahuan. Mahasiswa berhak mengetahui ketika perubahan memengaruhi cara data mereka diproses. Menampilkan ikon AI saja tidak menjawab pertanyaan tentang aliran data atau keputusan. Komunikasi yang baik singkat di muka dan terperinci bila pengguna ingin mendalami.

23. Pembatasan tujuan dan minimisasi data

Minimisasi data berarti mengumpulkan serta memproses hanya informasi yang diperlukan untuk tujuan yang telah ditetapkan. Untuk memberi latihan tambahan, dosen mungkin membutuhkan hasil kuis, bukan data lokasi atau

aktivitas di luar kursus. Untuk menjadwalkan bimbingan, kampus mungkin memerlukan ketersediaan, bukan rekaman konsultasi. Tim mendokumentasikan keputusan pengurangan data dan menguji apakah layanan tetap berjalan dengan atribut yang lebih sedikit.

Pembatasan tujuan mencegah data yang dikumpulkan untuk pembelajaran dialihkan diam-diam ke penilaian perilaku atau pemasaran. Tujuan baru memerlukan pemeriksaan dasar hukum, kompatibilitas, pemberitahuan, keamanan, dan dampak. Kampus membatasi akses berdasarkan fungsi, bukan karena semua data “milik kampus”. Fungsi baru harus menunjukkan kebutuhan dan manfaat yang sepadan.

Minimisasi dapat diterapkan pada desain prompt, log, analitik, dan dashboard. Sistem dapat menghapus nama sebelum mengirim pertanyaan ke model, mengirim bagian dokumen yang diperlukan saja, atau menggunakan statistik agregat. Pengajar dilatih untuk tidak mengunggah daftar nilai atau catatan mahasiswa ke alat publik. Pilihan tersebut mengurangi paparan sejak awal sehingga tidak seluruh beban perlindungan bergantung pada enkripsi setelah data terkumpul.

24. Retensi, arsip, dan penghapusan

Masa simpan data ditetapkan menurut tujuan dan aturan arsip, bukan kebiasaan platform. Log tutor yang dipakai untuk menyelesaikan sesi mungkin hanya diperlukan singkat; nilai resmi dan transkrip dapat memiliki retensi lebih panjang. Jadwal menjelaskan kategori, lama simpan, pemilik, lokasi salinan, dan metode penghapusan. Catatan sistem mencatat penghapusan tanpa mempertahankan isi pribadi yang tidak diperlukan.

Cadangan dan replikasi membuat penghapusan lebih kompleks. Kontrak vendor menyatakan kapan data dihapus dari sistem aktif dan cadangan, bagaimana penghapusan diverifikasi, serta apa yang terjadi setelah kontrak

berakhir. Jika penghapusan tertunda secara teknis, data dibatasi dan tidak dapat digunakan untuk tujuan lain. Institusi melakukan uji berkala terhadap prosedur agar penghapusan tidak hanya menjadi janji kontraktual.

Pengarsipan untuk kepentingan akreditasi, audit, atau penelitian harus mempunyai dasar dan akses yang jelas. Data yang disimpan untuk arsip tidak serta-merta boleh digunakan untuk analitik baru. Kampus dapat memisahkan salinan arsip, menghilangkan pengenal, atau membatasi akses. Mahasiswa diberi penjelasan tentang batas penghapusan dan hak yang berlaku menurut konteks.

25. Transfer lintas batas dan layanan komputasi awan

Penyedia AI dapat mengolah data di beberapa negara. UU PDP mengatur transfer data pribadi ke luar wilayah Indonesia dengan syarat tertentu yang perlu dipenuhi. Kampus memetakan lokasi pemrosesan dan menilai mekanisme perlindungan sebelum memilih layanan. Pernyataan bahwa perusahaan memiliki pusat data lokal belum menjawab apakah dukungan, log, atau subprosesor mengakses data dari luar negeri.

Transfer lintas batas mencakup lebih dari berkas utama. Telemetri, prompt, pencadangan, tiket dukungan, dan data diagnostik dapat ikut berpindah. Kontrak menentukan kategori data, lokasi, akses, keamanan, subprosesor, pemberitahuan insiden, serta bantuan memenuhi hak mahasiswa. Institusi meminta bukti dan hak audit yang memadai, bukan hanya sertifikat umum yang tidak menjelaskan cakupan layanan.

Kampus dapat mengurangi transfer dengan memakai data sintetis untuk uji coba, menyamarkan pengenal, menonaktifkan log, atau memilih konfigurasi lokal ketika memang layak. Pilihan lokasi harus dievaluasi bersama keamanan dan keberlangsungan layanan, bukan menjadi simbol kedaulatan data semata. Keputusan mencatat risiko residual dan pihak yang menyetujuinya.

26. Kontrak vendor dan pembagian risiko

Kontrak pendidikan dengan vendor perlu mengatur tujuan pemrosesan, larangan penggunaan sekunder, kerahasiaan, keamanan, subprosesor, retensi, penghapusan, transfer, audit, insiden, portabilitas, dan penghentian. Syarat layanan konsumen umum sering tidak cukup bagi data akademik. Tim pengadaan melibatkan fungsi hukum, teknologi, keamanan, privasi, akademik, serta aksesibilitas. Pengajar tidak diminta menerima persyaratan individual yang tidak dapat dinegosiasikan tanpa jalur institusi.

Vendor menjelaskan apakah data atau prompt digunakan untuk pelatihan model, apakah ada opt-out, bagaimana keluaran dipantau, dan bagaimana versi berubah. Kampus menilai apakah kontrol tersebut konsisten dengan tujuan serta dasar pemrosesan. Jika vendor dapat mengubah model secara sepihak, institusi meminta notifikasi dan hak menguji ulang. Ketersediaan ekspor data dan mekanisme keluar mengurangi ketergantungan jangka panjang.

Pembagian risiko tidak menghapus kewajiban institusi kepada mahasiswa. Kontrak dapat memberi ganti rugi antara perusahaan dan kampus, tetapi mahasiswa membutuhkan proses yang jelas ketika terjadi pelanggaran. Institusi menunjuk kontak dan prosedur penanganan yang konsisten. Vendor yang tidak memberi informasi cukup atau menolak kontrol penting mungkin tidak sesuai untuk data sensitif.

27. Keamanan siber dan kerahasiaan akademik

Keamanan melindungi kerahasiaan, integritas, dan ketersediaan data. Ancaman dapat berasal dari kredensial yang dicuri, perangkat hilang, salah konfigurasi penyimpanan, serangan ransomware, orang dalam, phishing, atau integrasi yang rentan. Kontrol meliputi autentikasi multifaktor, hak akses minimum, enkripsi saat penyimpanan dan pengiriman, pencatatan,

pemantauan, pencadangan, pembaruan, dan pelatihan. Setiap kontrol disesuaikan dengan sensitivitas serta dampak kebocoran.

Akses internal perlu ditinjau berkala. Dosen tidak memerlukan seluruh data layanan konseling; vendor dukungan tidak perlu melihat nilai; peneliti tidak semestinya memperoleh identitas tanpa kebutuhan. Prinsip least privilege dan pemisahan tugas membatasi kerusakan bila akun disalahgunakan. Sistem menghapus akses setelah staf pindah peran dan meninjau akun layanan yang jarang digunakan.

Keamanan AI mencakup risiko khusus seperti prompt injection, kebocoran data melalui keluaran, ekstraksi prompt, dan serangan terhadap integrasi. Pengguna dapat menempelkan informasi sensitif ke layanan yang tidak disetujui. Kampus menetapkan konfigurasi aman, filter masukan, batas output, dan proses redaksi. Panduan sederhana yang menjelaskan contoh data terlarang sering lebih efektif daripada kebijakan teknis yang sulit diterapkan.

28. Respons insiden dan pemberitahuan kebocoran

Insiden privasi dapat berupa akses tidak sah, kehilangan perangkat, publikasi berkas, salah kirim, penyimpanan berlebihan, atau penggunaan di luar tujuan. Rencana respons menetapkan siapa yang menerima laporan, cara mengamankan bukti, bagaimana menghentikan paparan, kapan melibatkan vendor, dan siapa yang berwenang menilai kewajiban pemberitahuan. Simulasi meja membantu unit akademik memahami perannya sebelum insiden nyata terjadi.

UU PDP mewajibkan pengendali memberikan pemberitahuan tertulis dalam jangka waktu yang ditentukan ketika terjadi kegagalan pelindungan data pribadi, dengan rincian yang relevan mengenai data, waktu, dan langkah penanganan. Institusi memeriksa ketentuan dan prosedur hukum yang berlaku secara cermat. Menunggu sampai semua fakta sempurna dapat

bertentangan dengan tenggat; karena itu, proses investigasi dan komunikasi disusun untuk bergerak paralel.

Komunikasi kepada mahasiswa menjelaskan apa yang terjadi, data yang terdampak, tindakan perlindungan yang dapat dilakukan, kontak bantuan, dan pembaruan. Pesan menghindari menyalahkan pengguna dan tidak menutupi ketidakpastian. Setelah insiden, tim mencari sebab sistemik: desain akses, kontrak, pelatihan, atau praktik penyimpanan. Pembelajaran dan tindakan korektif dilaporkan kepada pimpinan serta komunitas sesuai kebutuhan.

29. Privasi sejak tahap desain

Privacy by design memasukkan pelindungan data ke dalam tujuan, arsitektur, antarmuka, dan operasi layanan sejak awal. Tim memilih atribut minimum, memisahkan identitas dari konten bila mungkin, membatasi retensi, menyediakan kontrol akses, dan menyiapkan jalur hak. Jika privasi baru dibahas setelah sistem jadi, pilihan desain yang aman mungkin lebih mahal atau tidak tersedia. Gerbang peninjauan privasi menjadi bagian dari proses pengembangan dan pengadaan.

Privacy by default mengatur sistem pada konfigurasi yang paling melindungi tanpa meminta mahasiswa menonaktifkan pelacakan satu per satu. Berbagi log, personalisasi lintas kursus, dan penyimpanan panjang tidak diaktifkan otomatis bila tidak dibutuhkan. Mahasiswa dapat memilih fitur tambahan setelah memahami manfaat dan dampak. Pengaturan bawaan penting karena banyak pengguna tetap menggunakan opsi awal.

Desain berorientasi pengguna memeriksa apakah mahasiswa memahami indikator, melihat data yang disimpan, dan dapat memperbaiki kesalahan. Prototipe diuji dengan kelompok beragam sebelum skala luas. Kegagalan usability dapat menjadi masalah privasi jika pengguna tanpa sengaja

mengirim informasi atau tidak dapat menemukan pilihan. Tim desain mendokumentasikan kompromi dan meninjau ulang setelah kondisi berubah.

30. Penilaian dampak pelindungan data

Penilaian dampak diperlukan ketika pemrosesan berpotensi menimbulkan risiko tinggi terhadap hak dan kebebasan, serta digunakan untuk mengidentifikasi dan mengurangi risiko sebelum sistem berjalan. Untuk AI akademik, pemicu dapat mencakup pemrosesan skala besar, data spesifik, pemantauan sistematis, profiling, atau keputusan yang berdampak signifikan. Penilaian disesuaikan dengan kewajiban UU PDP dan aturan pelaksana. Ia tidak berhenti pada daftar risiko umum.

Penilaian memetakan tujuan, subjek data, kategori, alur, dasar, vendor, penerima, durasi, ancaman, kemungkinan dampak, dan pengamanan. Tim menguji skenario seperti salah identifikasi, kebocoran, inferensi sensitif, keberatan yang tidak terlayani, dan dampak tidak proporsional pada kelompok tertentu. Alternatif yang lebih ringan dibandingkan secara nyata. Mahasiswa dan dosen dilibatkan untuk menemukan dampak yang tidak terlihat oleh tim teknis.

Hasil penilaian menentukan mitigasi, pemilik tindakan, tenggat, dan risiko residual yang diterima. Jika risiko tinggi tidak dapat dikurangi dengan memadai, kampus mengubah atau tidak menjalankan pemrosesan sampai konsultasi yang disyaratkan dilakukan. Penilaian diperbarui saat tujuan, model, data, atau vendor berubah. Dokumen ini menjadi dasar keputusan dan pembelajaran institusi, bukan arsip administratif.

31. Teknik peningkatan privasi dan batasnya

Pseudonimisasi mengganti pengenal langsung dengan kode dan menyimpan kunci secara terpisah. Enkripsi menjaga data agar tidak terbaca tanpa kunci

yang sesuai. Agregasi mengurangi keterlihatan individu, sedangkan kontrol akses membatasi siapa yang dapat melihat data. Teknik tersebut mengurangi risiko tetapi tidak selalu menghilangkan kemungkinan identifikasi atau penyalahgunaan. Institusi memilih kontrol berdasarkan model ancaman dan menguji efektivitasnya.

Differential privacy dapat membatasi apa yang dapat dipelajari tentang individu dari statistik agregat dengan menambahkan noise terukur. Federated learning melatih model lintas perangkat atau institusi tanpa memusatkan seluruh data mentah, meskipun gradien dan model tetap dapat membawa risiko kebocoran. Secure multiparty computation dan trusted execution environments dapat membantu dalam skenario tertentu, tetapi membawa biaya dan kompleksitas.

Teknik perlindungan bukan alasan untuk mengumpulkan lebih banyak data. Privasi perlu dimulai dari pengurangan tujuan dan data, lalu menerapkan pengamanan yang sesuai. Klaim “anonim” atau “federated” perlu diuji menurut serangan yang relevan. Kampus memastikan staf memahami bahwa perlindungan teknis melengkapi transparansi, hak, dan akuntabilitas; satu teknik tidak menyelesaikan pertanyaan etis tentang penggunaan.

32. Data penelitian, etik, dan persetujuan akademik

Penelitian pendidikan dapat menggunakan data platform untuk mengevaluasi efektivitas, memahami partisipasi, atau mengembangkan model. Data yang tersedia dari kegiatan rutin tidak otomatis boleh digunakan untuk riset. Peneliti menilai tujuan baru, dasar pemrosesan, kebutuhan persetujuan, risiko identifikasi, dan persetujuan komite etik sesuai standar institusi. Mahasiswa perlu tahu apakah keputusan berpartisipasi memengaruhi nilai atau akses kelas; dosen yang meneliti kelasnya perlu mengelola konflik peran.

Pemisahan peran dapat mengurangi tekanan. Pengumpulan persetujuan dapat dilakukan pihak independen, dan dosen tidak melihat siapa yang menolak sampai penilaian selesai. Peneliti melaporkan batas dataset dan tidak mencoba mengidentifikasi peserta dari data yang telah dipseudonimkan. Kutipan, contoh prompt, dan tangkapan layar diperiksa untuk menghapus identitas langsung maupun konteks yang dapat dikenali.

Penggunaan ulang dataset memerlukan penilaian ulang jika pertanyaan, penerima, atau teknologi berubah. Persetujuan untuk satu penelitian tidak menjadi izin tanpa batas untuk pengembangan produk. Prinsip open science dan replikasi dapat didukung melalui data terkontrol, kode, metadata, atau dataset sintetis. Publikasi temuan harus menghindari membuka pola yang membuat mahasiswa tertentu mudah diketahui.

33. Privasi dalam penelitian dan pengembangan model

Model dapat dilatih atau diuji memakai tulisan mahasiswa, rekaman kuliah, forum, atau karya proyek. Karya tersebut memiliki nilai pendidikan dan hak cipta, serta mungkin memuat data pribadi. Kampus menetapkan apakah penggunaannya diperlukan, siapa yang memiliki hak, apakah data benar-benar dianonimkan, dan bagaimana mahasiswa menolak. Penggunaan sebagai bahan pelatihan komersial memerlukan pemeriksaan terpisah dari pemrosesan untuk memberikan layanan.

Model yang dilatih pada korpus kampus dapat menghafal bagian dokumen atau mereproduksi jawaban mahasiswa. Uji ekstraksi, redaksi, penghapusan data, dan dokumentasi sumber perlu dilakukan. Model dapat menunjukkan bias terhadap kelompok yang kurang terwakili. Pengembang membuat prosedur untuk menangani permintaan koreksi dan menghindari keluaran yang membeberkan catatan individual.

Mahasiswa dapat menjadi mitra penelitian dan desain, bukan hanya sumber data pasif. Keterlibatan mereka membantu menilai apakah manfaat yang dijanjikan selaras dengan pengalaman. Kampus menjelaskan kompensasi, hak atas hasil, dan batas penggunaan karya. Partisipasi yang bermakna membangun kepercayaan dan meningkatkan mutu pertanyaan penelitian.

34. Pengawasan proktor, kehadiran, dan aktivitas

Sistem pengawasan ujian dan kehadiran dapat mengumpulkan video, lokasi, suara, gerakan, atau perilaku perangkat. Sistem kehadiran otomatis mungkin salah mengenali wajah atau menganggap mahasiswa absen karena jaringan. Penilaian privasi memperhitungkan intensitas, keterpaksaan, kesalahan, retensi, dan kesempatan banding. Kampus membandingkan dengan daftar hadir manual, desain ujian terbuka, dan penilaian autentik sebelum memutuskan perlu atau tidaknya biometrik.

Pemantauan layar dan aktivitas dapat menyatukan tujuan yang berbeda: memastikan kehadiran, mendeteksi kecurangan, menilai keterlibatan, dan mengukur penggunaan. Penggunaan silang ini berisiko melampaui harapan mahasiswa. Sistem mendefinisikan satu tujuan, membatasi pemrosesan pada durasi relevan, dan melarang penggunaan log untuk evaluasi perilaku lain tanpa penilaian baru.

Mahasiswa yang membutuhkan akomodasi atau menghadapi kondisi ruang tidak ideal memerlukan alternatif yang setara. Prosedur banding menyediakan pemeriksaan manusia dan tidak menuntut mahasiswa membuktikan bahwa algoritme salah melalui proses yang rumit. Rekaman dikunci dan dihapus berdasarkan jadwal. Hasil peringatan tidak dibagikan di luar pihak yang menilai ujian.

35. Layanan konseling, kesehatan, dan dukungan mahasiswa

Layanan konseling, kesehatan, dan disabilitas menangani data yang sangat sensitif. Integrasi dengan LMS atau analitik akademik perlu dibatasi secara tegas. Dosen mungkin perlu tahu bahwa akomodasi tertentu berlaku, tetapi tidak perlu menerima diagnosis atau catatan konsultasi. Petugas layanan menetapkan informasi minimum yang perlu dibagikan, dasar pemrosesan, dan kanal aman. AI chatbot untuk dukungan emosional harus memberi tahu keterbatasan dan mengarahkan pada petugas saat diperlukan.

Sistem peringatan dini yang menggabungkan nilai dengan informasi kesehatan atau konseling dapat menghasilkan profil yang invasif. Mahasiswa berhak mengetahui bagaimana data dipakai dan apa dampak keputusan. Intervensi tidak boleh memaksa pengungkapan pribadi sebagai syarat memperoleh bantuan akademik. Dukungan dapat ditawarkan dengan pilihan dan penjelasan yang tidak menstigma.

Kampus memisahkan akses teknis dan substantif. Administrator dapat mengelola sistem tanpa membaca isi catatan klinis; analitik menggunakan agregat bila memungkinkan. Log akses membantu mendeteksi rasa ingin tahu yang tidak berwenang. Insiden layanan sensitif ditangani dengan kehati-hatian khusus dan komunikasi langsung yang sesuai.

36. Penerimaan mahasiswa, beasiswa, dan keputusan administratif

Data penerimaan dan beasiswa mencakup nilai, pendapatan, identitas, latar keluarga, esai, rekomendasi, dan kadang informasi kesehatan. AI dapat membantu mengurutkan berkas atau mendeteksi kelengkapan, tetapi otomatisasi berpotensi menyamarkan bias historis. Institusi menetapkan kriteria yang transparan, membatasi data pada kebutuhan, dan menguji hasil menurut kelompok. Keputusan akhir mempunyai alasan yang dapat dijelaskan serta mekanisme keberatan.

Esai dan surat rekomendasi dapat diunggah ke model generatif untuk ringkasan. Dokumen tersebut memuat informasi tentang pelamar dan pemberi rekomendasi. Kampus mencegah pengunggahan ke layanan yang tidak disetujui dan meminta vendor tidak menyimpan atau menggunakan materi untuk tujuan sekunder. Ringkasan otomatis diverifikasi terhadap berkas asli sebelum memengaruhi evaluasi.

Sistem administratif sering bertahan lama dan menyimpan data lintas tahun. Jadwal retensi dan hak akses disesuaikan untuk arsip serta proses banding. Penggunaan data penerimaan untuk pemasaran, prediksi donasi, atau tujuan lain membutuhkan penilaian baru. Kampus menjelaskan kepada pelamar informasi apa yang dipakai dan bagaimana meminta koreksi.

37. Pengelolaan identitas digital dan kredensial

Akun tunggal memudahkan akses namun menghubungkan banyak layanan melalui satu identitas. Jika akun kompromi, paparan dapat meluas. Kampus menerapkan autentikasi kuat, pembatasan sesi, pengelolaan peran, dan proses pemulihan akun yang aman. Untuk layanan eksternal, penggunaan identitas tersamar atau token terbatas dapat mengurangi pengaitan lintas konteks.

Kredensial digital dan portofolio dapat membantu mahasiswa membuktikan kompetensi. Informasi yang dibagikan keluar kampus harus berada dalam kendali mahasiswa sejauh sistem memungkinkan. Berbagi transkrip lengkap untuk tujuan yang hanya memerlukan satu sertifikat tidak proporsional. Kampus menyediakan format selektif dan menjelaskan metadata yang ikut terbawa.

Identitas digital juga mencakup nama pilihan, foto, status, dan informasi disabilitas yang tampil pada platform. Mahasiswa membutuhkan cara memperbarui atau membatasi informasi sesuai kebijakan. Sistem menghindari

publikasi daftar kelas, nilai, atau kehadiran yang tidak perlu. Desain identitas mengakui bahwa privasi mencakup bagaimana seseorang terlihat dalam komunitas akademik.

38. Bias, keadilan, dan dampak kelompok

Data historis mencerminkan keputusan dan ketimpangan terdahulu. Jika model belajar dari pola itu, rekomendasi dapat memberi dukungan berbeda berdasarkan proksi seperti sekolah asal, alamat, bahasa, atau aktivitas. Audit keadilan meninjau kualitas data, tujuan, kesalahan, intervensi, dan konsekuensi menurut kelompok yang relevan. Perbedaan skor tidak otomatis membuktikan bias, tetapi menjadi tanda untuk pemeriksaan lebih dalam.

Mahasiswa dari latar berbeda mungkin memiliki pola penggunaan yang tidak sama karena jadwal kerja, koneksi, budaya bertanya, atau desain aksesibilitas. Sistem yang menilai satu gaya sebagai keterlibatan ideal dapat mengklasifikasi kelompok lain secara tidak tepat. Tim melibatkan mahasiswa terdampak dan dosen lokal untuk menafsirkan hasil. Pengumpulan kategori sensitif untuk audit juga harus memiliki dasar dan pelindungan yang sesuai.

Keadilan menuntut perhatian pada manfaat yang tersebar, bukan sekadar akurasi rata-rata. Apakah bantuan sampai kepada mahasiswa yang membutuhkan? Apakah mahasiswa dengan prediksi risiko rendah tetap dapat meminta bantuan? Apakah sistem memindahkan beban pembuktian kepada kelompok yang dirugikan? Kebijakan memberi kesempatan koreksi dan meninjau kembali penggunaan ketika disparitas tidak dapat diterima.

39. Efek gentar dan kebebasan akademik

Mahasiswa dapat membatasi pertanyaan atau eksperimen ketika mereka mengira setiap interaksi dipantau untuk penilaian. Efek gentar ini dapat melemahkan diskusi, pencarian bantuan, penelitian, dan kebebasan untuk

mempertanyakan pandangan dominan. Pengawasan yang tidak transparan sangat merusak kepercayaan karena pengguna tidak mengetahui kapan perilaku mereka dinilai. Kampus membuat batas penggunaan data yang eksplisit dan melarang akses untuk tujuan disiplin yang tidak diumumkan.

Forum akademik membahas gagasan yang tidak populer, identitas, politik, agama, dan isu sensitif. Platform tidak seharusnya menyaring atau mengklasifikasi mahasiswa secara otomatis berdasarkan posisi atau minat, kecuali terdapat kebutuhan yang sah dan proporsional. Akses ke materi serta catatan pencarian dijaga. Peneliti dan mahasiswa tahu bahwa aktivitas akademik mereka tidak dipakai sebagai profil politik atau perilaku komersial.

Kepercayaan dapat pulih melalui transparansi, kontrol akses yang dapat diaudit, dan penjelasan insiden secara jujur. Dewan akademik meninjau kebijakan pemantauan dan mendengar pengalaman pengguna. Jika suatu alat menyebabkan mahasiswa menghindari layanan atau membatasi pertanyaan, indikator itu menjadi bukti dampak buruk yang perlu ditindaklanjuti.

40. Literasi privasi bagi mahasiswa dan dosen

Literasi privasi membantu mahasiswa mengenali data yang dibagikan, memahami pengaturan, menilai risiko, dan menggunakan hak. Pelatihan dapat memakai skenario: mengunggah tugas yang memuat wawancara, meminta AI menganalisis kondisi kesehatan, atau membagikan nilai teman. Contoh konkret lebih mudah diterapkan daripada definisi abstrak. Panduan menyebut kanal bantuan kampus dan layanan yang boleh dipakai.

Dosen membutuhkan pelatihan tentang pemrosesan prompt, pengelolaan daftar nilai, penggunaan model untuk umpan balik, kerahasiaan penelitian, serta alternatif tugas. Seringkali dosen menggunakan alat konsumen untuk mengatasi tekanan kerja tanpa mengetahui kebijakan data. Institusi

menyediakan lingkungan yang disetujui, lisensi, dukungan, serta waktu pelatihan agar pilihan aman juga praktis.

Literasi tidak memindahkan kewajiban perlindungan kepada pengguna. Mahasiswa boleh salah memahami layanan; desain harus mencegah kesalahan yang dapat diperkirakan. Pelatihan melengkapi kebijakan, konfigurasi sistem, kontrak, dan pengawasan. Kampus menilai pemahaman melalui kemampuan menggunakan prosedur dan mengidentifikasi masalah, bukan hanya kehadiran di webinar.

41. Partisipasi mahasiswa dalam tata kelola

Mahasiswa terlibat dalam penyusunan kebijakan, penilaian dampak, pemilihan alat, dan audit setelah penggunaan. Keterlibatan dapat melalui dewan perwakilan, lokakarya, survei berbayar, uji aksesibilitas, atau forum terbuka. Institusi memberi informasi yang cukup agar partisipasi tidak hanya menjadi legitimasi simbolis. Saran mahasiswa didokumentasikan bersama respons dan alasan keputusan.

Kelompok pengguna berbeda pengalaman dan kebutuhan. Kampus mengundang mahasiswa disabilitas, mahasiswa internasional, mahasiswa pekerja, dan kelompok yang jarang terwakili dengan cara yang aman. Tidak ada satu perwakilan yang dapat berbicara atas semua orang. Metode partisipasi menjaga kerahasiaan dan tidak meminta peserta menceritakan informasi sensitif secara terbuka.

Keterlibatan berlanjut setelah peluncuran. Mahasiswa melaporkan keluaran keliru, kesulitan menggunakan hak, dan dampak pada kebiasaan belajar. Institusi memberi umpan balik mengenai perubahan yang dilakukan. Dengan cara ini, pengalaman pengguna menjadi bagian dari akuntabilitas dan peningkatan sistem.

42. Tata kelola institusi dan pejabat pelindungan data

Kampus membentuk struktur tata kelola yang jelas untuk sistem AI dan data mahasiswa. Fungsi privasi, keamanan, akademik, hukum, pengadaan, aksesibilitas, dan perwakilan mahasiswa berkoordinasi. Pejabat atau fungsi pelindungan data yang ditunjuk sesuai kewajiban membantu memantau kepatuhan, memberi nasihat, dan menjadi kontak. Independensi, akses ke pimpinan, keahlian, dan sumber daya menentukan apakah fungsi tersebut efektif.

Komite peninjau menetapkan kategori risiko dan proses persetujuan. Penggunaan berisiko rendah dapat mengikuti prosedur sederhana; sistem yang memproses data sensitif, membuat prediksi, atau memengaruhi keputusan penting memerlukan evaluasi lebih dalam. Persetujuan bukan tanda bahwa risiko hilang. Pemilik sistem tetap memantau kinerja, keluhan, kontrak, dan perubahan versi.

Tata kelola juga menentukan bagaimana informasi disimpan, siapa mengaudit, kapan hasil diumumkan, dan bagaimana insiden dilaporkan ke pihak berwenang. Kebijakan institusi selaras dengan UU PDP dan regulasi relevan yang berlaku. Tinjauan berkala mencegah struktur menjadi formalitas tanpa pengaruh terhadap praktik.

43. Pengadaan AI secara bertanggung jawab

Pengadaan dimulai dari kebutuhan pendidikan atau administrasi yang terdefinisi. Tim membandingkan opsi AI dengan proses manual, desain ulang layanan, sumber terbuka, dan tambahan dukungan manusia. Analisis biaya mencakup lisensi, integrasi, keamanan, pemeliharaan, pelatihan, dan biaya keluar. Produk dengan fitur terbanyak tidak selalu paling tepat jika memerlukan data lebih banyak atau sulit diaudit.

Vendor diminta menunjukkan akurasi pada konteks yang relevan, aksesibilitas, performa bahasa Indonesia, keamanan, lokasi data, subprosesor, retensi, penggunaan untuk pelatihan, dan prosedur banding. Uji demonstrasi menggunakan data sintetis, bukan berkas mahasiswa nyata. Klaim pemasaran diverifikasi melalui bukti independen dan pilot terbatas.

Kontrak mengatur perubahan model, hak audit, pemberitahuan insiden, portabilitas, penghapusan, kepatuhan subprosesor, dan penghentian. Perguruan tinggi memastikan materi dan data dapat diekspor dalam format terbuka. Bila penyedia tidak dapat menjelaskan alur data, sistem tidak digunakan untuk informasi berisiko tinggi. Pengadaan menjadi instrumen tata kelola, bukan sekadar transaksi harga.

44. Audit algoritmik dan pemantauan berkelanjutan

Audit menilai apakah sistem melakukan tujuan yang disetujui, menggunakan data yang tepat, dan menghasilkan dampak yang dapat diterima. Pemeriksaan meliputi validasi teknis, distribusi kesalahan, akses, keterjelasan, keamanan, dan pengalaman mahasiswa. Audit independen dapat menambah kredibilitas ketika sistem memengaruhi keputusan penting. Hasilnya disampaikan kepada pimpinan dan pengguna dengan menghindari pengungkapan data pribadi.

Kinerja dapat berubah karena model diperbarui, populasi berbeda, atau pola pembelajaran berubah. Kampus mencatat versi, data evaluasi, konfigurasi, dan perubahan. Indikator pemantauan mencakup kesalahan, banding, keluhan, penggunaan yang tidak direncanakan, dan ketimpangan manfaat. Nilai agregat tidak cukup tanpa pembacaan kualitatif.

Jika audit menemukan dampak yang tidak dapat diterima, sistem dibatasi, diperbaiki, atau dihentikan. Kampus menyediakan prosedur penghentian dan layanan alternatif agar mahasiswa tidak kehilangan akses. Pemilik sistem

mendokumentasikan mitigasi dan menjelaskan keputusan. Tanggung jawab tidak berakhir setelah pilot dinyatakan berhasil.

45. Metrik manfaat dan kerugian privasi

Evaluasi manfaat dapat mengukur ketepatan bantuan, mutu umpan balik, waktu respons, hasil belajar, serta pemerataan akses. Namun, manfaat tersebut harus dibandingkan dengan praktik yang menjadi alternatif. Kerugian mencakup intrusi, rasa diawasi, kesalahan profil, beban koreksi, risiko kebocoran, dampak reputasi, dan ketergantungan vendor. Penilaian dampak meninjau probabilitas sekaligus tingkat konsekuensi.

Kampus dapat mengukur pengetahuan mahasiswa tentang penggunaan data, kepercayaan, kemampuan menarik pilihan, waktu penyelesaian permintaan, dan jumlah insiden. Survei perlu menjaga anonimitas dan tidak menanyakan hal yang tidak relevan. Wawancara dan kelompok diskusi mengungkap pengalaman yang tidak tertangkap metrik. Hasil dinilai menurut subkelompok secara hati-hati.

Keputusan melanjutkan teknologi bergantung pada manfaat bersih dan distribusinya. Jika manfaat kecil, sementara intrusi dan risiko tinggi, institusi memilih pendekatan lain. Bila sistem bermanfaat tetapi hanya dapat berjalan melalui pengumpulan yang tidak proporsional, desain diubah. Akuntabilitas meliputi kemampuan mengatakan tidak pada sistem yang tidak cocok.

46. Model kematangan privasi data mahasiswa

Kematangan awal ditandai oleh inventaris data yang tidak lengkap, kebijakan tersebar, dan penggunaan alat tanpa pemeriksaan. Tahap berikutnya menetapkan pemilik sistem, tujuan, dasar pemrosesan, kontrak, dan hak akses. Tingkat yang lebih matang mengintegrasikan penilaian dampak, desain privasi, partisipasi mahasiswa, audit algoritmik, dan evaluasi manfaat. Model

kematangan membantu institusi melihat jalur perbaikan, bukan hanya membuat daftar ketidakpatuhan.

Setiap tahap memerlukan bukti praktik. Contohnya, apakah masa retensi diuji; apakah staf menyelesaikan pelatihan; apakah permintaan hak direspons tepat waktu; apakah vendor mencatat subprosesor; dan apakah keluaran model diperiksa menurut kelompok. Skor kematangan tidak boleh menjadi pemeringkatan publik yang mendorong institusi menyembunyikan masalah. Tujuan utamanya ialah menetapkan prioritas investasi.

Kampus kecil dapat memulai dari dasar penting: pemetaan layanan, aturan unggah data, daftar alat yang disetujui, dan prosedur insiden. Kemudian memperluas kapasitas melalui kerja sama antarperguruan tinggi dan layanan bersama. Kematangan bukan ditentukan anggaran semata, tetapi kejelasan tanggung jawab, disiplin pembatasan data, dan keterbukaan untuk memperbaiki proses.

47. Peta jalan penerapan pada tingkat perguruan tinggi

Tahap pertama ialah pemetaan data dan penggunaan AI yang telah berjalan, termasuk praktik informal dosen dan mahasiswa. Tahap kedua menetapkan prinsip, kategori risiko, dan daftar penggunaan prioritas. Tahap ketiga membangun layanan pendukung seperti pelatihan, sistem pengaduan, lingkungan AI yang disetujui, serta kontrak standar. Tahap keempat menjalankan pilot dengan tujuan, kelompok, jangka waktu, dan ukuran keberhasilan yang jelas.

Pilot melibatkan dosen, mahasiswa, unit hukum, teknologi, keamanan, dan aksesibilitas sejak awal. Data sintetis digunakan saat menguji integrasi. Tim menguji kondisi ekstrem, bahasa campuran, akses perangkat, keluaran salah, serta jalur peninjauan manusia. Hasil negatif dilaporkan. Perluasan baru dilakukan jika manfaat terukur dan risiko dapat dikelola.

Peta jalan menetapkan evaluasi berkala, pemilik sistem, anggaran, dan kriteria penghentian. Kebijakan ditinjau ketika model atau regulasi berubah. Kampus menyiapkan portabilitas dan rencana keluar dari vendor. Komunikasi rutin membuat mahasiswa memahami perkembangan. Proses bertahap menghindari adopsi simbolik dan memberi waktu untuk membangun kepercayaan.

48. Skenario: tutor AI pada kelas pengantar statistik

Program studi ingin menggunakan tutor AI untuk mahasiswa yang kesulitan menafsirkan distribusi dan probabilitas. Tim terlebih dahulu menetapkan bahwa tujuan layanan adalah memberi latihan dan petunjuk, bukan mengukur ketekunan. Tutor memakai bahan yang disetujui dosen; identitas mahasiswa tidak dikirim bila tidak diperlukan; log percakapan disimpan singkat untuk dukungan teknis. Mahasiswa diberi informasi, pengaturan privasi, dan alternatif latihan dengan sumber non-AI.

Selama pilot, dosen meninjau agregat kesalahan konsep tanpa membaca setiap percakapan pribadi. Mahasiswa secara sukarela melaporkan contoh tutor yang keliru. Tim menguji apakah akurasi dan akses berbeda untuk bahasa Indonesia formal, bahasa campuran, dan pembaca layar. Setiap rekomendasi tentang mahasiswa tertentu tetap dapat ditolak dan tidak memengaruhi nilai akhir.

Evaluasi mencakup pemahaman pada tugas transfer, persepsi kendali, beban mahasiswa, kebutuhan bantuan manusia, serta insiden data. Bila tutor membantu tetapi menyimpan terlalu banyak informasi, tim menyesuaikan konfigurasi. Bila performa bahasa atau aksesibilitas tidak memadai, penggunaan dibatasi. Skenario menunjukkan bahwa privasi dan hasil belajar dapat dinilai dalam keputusan yang sama.

49. Skenario: sistem peringatan dini dan bantuan akademik

Kampus ingin menemukan mahasiswa yang mungkin memerlukan bimbingan sebelum nilai akhir. Model menganalisis pendaftaran dan hasil tugas. Sebelum menjalankan, tim menilai dasar pemrosesan, akurasi, indikator yang dipakai, data yang tidak relevan, dan dampak label. Peringatan tidak digunakan untuk sanksi atau pencabutan beasiswa; tujuannya mengundang mahasiswa secara sukarela ke layanan akademik.

Penasihat menerima alasan ringkas dan tingkat ketidakpastian, bukan hanya skor risiko. Mahasiswa diberi tahu bahwa model membantu menentukan tawaran dukungan dan dapat memperbaiki informasi. Sistem menyediakan jalur meminta bimbingan tanpa menunggu prediksi. Evaluasi menguji apakah dukungan benar-benar diterima dan membantu, serta siapa yang tidak terjangkau.

Jika kelompok tertentu lebih sering dilabeli karena pola penggunaan platform, kampus menilai apakah sistem mengukur akses, bukan kemampuan. Model dapat diubah atau dihentikan. Dukungan langsung seperti konsultasi terbuka tetap tersedia. Contoh ini menghubungkan manfaat intervensi dengan hak untuk tidak dikunci oleh prediksi.

50. Skenario: AI generatif untuk tugas dan umpan balik

Dosen mendorong mahasiswa menggunakan AI untuk mendapatkan pertanyaan awal tentang struktur tulisan. Sistem tidak menerima nama, nilai, atau informasi pribadi; mahasiswa menggunakan akun dan konfigurasi yang disetujui. Aturan mata kuliah menjelaskan penggunaan yang diperbolehkan, kewajiban memeriksa komentar, dan larangan mengunggah hasil wawancara yang dapat mengidentifikasi peserta. Mahasiswa tetap bertanggung jawab atas tugas akhir.

Kampus memeriksa apakah penyedia menyimpan prompt, menggunakannya untuk pelatihan, dan melibatkan subprosesor. Bila data tidak dapat dilindungi, dosen menyediakan alternatif seperti konsultasi teman sebaya atau rubrik mandiri. Draf mahasiswa tidak otomatis digunakan untuk penelitian. Jika pengajar ingin menganalisisnya, tujuan dan dasar ditinjau terpisah.

Penilaian menekankan proses revisi dan kemampuan mempertahankan argumen, bukan deteksi otomatis AI. Mahasiswa dapat melaporkan masukan yang salah; dosen mengevaluasi pola dan memperbarui panduan. Penggunaan teknologi menjadi bagian dari literasi akademik dengan tata kelola yang jelas.

51. Pelajaran untuk perguruan tinggi di Indonesia

Kampus Indonesia memiliki keragaman kapasitas, bahasa, ukuran kelas, dan infrastruktur. Kebijakan yang mengasumsikan jaringan stabil, perangkat pribadi, dan akses ke layanan berbayar dapat menyingkirkan mahasiswa tertentu. Pelindungan data perlu dirancang untuk konteks nyata: perangkat bersama, penggunaan ponsel, koneksi terbatas, bahasa campuran, dan dukungan staf yang tidak selalu cukup. Solusi lokal dapat meningkatkan kesesuaian jika dikembangkan dengan standar keamanan dan tata kelola yang kuat.

UU PDP menjadi dasar untuk memperkuat peran pengendali dan prosesor, prosedur hak, penilaian dampak, transfer lintas batas, dan keamanan. Perguruan tinggi menyelaraskan kebijakan dengan hukum yang berlaku serta mengikuti perkembangan aturan teknis dan kelembagaan. Panduan sektoral yang jelas dapat membantu kampus kecil membangun dokumen standar dan proses pengadaan tanpa mengurangi kewajiban masing-masing.

Kerja sama antarperguruan tinggi memungkinkan pertukaran materi, protokol audit, pelatihan, dan sistem bersama. Namun, berbagi data antarkampus

memerlukan tujuan, peran, dasar, keamanan, dan pembatasan yang jelas. Pengembangan kapasitas kolektif lebih baik daripada setiap kampus membeli produk tanpa kemampuan menilai. Kepentingan mahasiswa menjadi ukuran bersama bagi inovasi yang beragam.

52. Agenda riset tentang privasi dan AI akademik

Penelitian perlu memahami bagaimana mahasiswa di Indonesia menilai privasi, risiko, kontrol, dan manfaat AI dalam pendidikan tinggi. Studi lintas kampus dapat membandingkan pengalaman menurut lokasi, program, usia, bahasa, akses, dan jenis layanan. Instrumen survei perlu diuji dalam bahasa dan konteks lokal; wawancara dapat mengungkap alasan di balik pilihan. Hasil tidak boleh menganggap satu kampus mewakili semua mahasiswa Indonesia.

Agenda berikutnya menguji bagaimana kebijakan dan desain memengaruhi perilaku. Apakah pemberitahuan berlapis meningkatkan pemahaman? Apakah opsi opt-out yang nyata mengubah kepercayaan? Apakah pengurangan log memengaruhi mutu bimbingan? Penelitian dapat menggabungkan audit teknis, eksperimen desain, dan studi kasus tata kelola. Bukti membantu membedakan kontrol yang efektif dari simbol perlindungan.

Peneliti juga menilai dampak jangka panjang profil akademik, sistem peringatan, dan pemrosesan multimodal pada kebebasan mahasiswa. Studi tersebut memerlukan kolaborasi hukum, pendidikan, ilmu komputer, psikologi, dan sosiologi. Publikasi melindungi partisipan dan membuka metode serta batas penelitian. Temuan negatif perlu dibagikan agar pengambil kebijakan tidak hanya melihat cerita keberhasilan produk.

53. Masa depan: privasi sebagai syarat kepercayaan akademik

AI akan terus memperluas kemampuan menghubungkan data, memahami teks, dan memberikan respons kontekstual. Kemampuan ini dapat

memperbaiki akses dukungan dan mengurangi pekerjaan rutin. Pada saat yang sama, inferensi semakin sulit diprediksi dan data dapat berpindah melalui rantai layanan yang kompleks. Institusi perlu merancang privasi untuk sistem yang berubah, bukan hanya untuk satu model saat ini. Tujuan, data, penerima, serta kontrol harus dapat ditinjau kembali.

Kampus yang dipercaya menjelaskan batasnya, membatasi data, merespons permintaan, dan mengakui kesalahan. Kepercayaan bukan hasil dari slogan "AI aman", melainkan hubungan yang dibuktikan melalui tindakan. Mahasiswa dapat menolak penggunaan yang tidak perlu, memahami keputusan, memperbaiki data, dan memperoleh bantuan tanpa takut dicap. Prinsip ini menjaga ruang belajar sebagai tempat untuk berpikir dan mencoba.

Privasi tidak menghambat pemanfaatan data yang bertanggung jawab. Justru pembatasan yang jelas mendorong desain lebih fokus, data lebih bermutu, dan tujuan pendidikan lebih terukur. Perguruan tinggi mengembangkan kecerdasan kelembagaan untuk menentukan apa yang seharusnya diketahui sistem dan apa yang sebaiknya tetap berada dalam hubungan manusia. Keputusan ini membedakan dukungan akademik dari pengawasan yang tidak perlu.

54. Kesimpulan: melindungi mahasiswa sambil memajukan pendidikan

Ekosistem AI akademik bergantung pada data mahasiswa, tetapi akses teknis terhadap data tidak memberi institusi hak tanpa batas untuk mengumpulkan, menggabungkan, atau menyimpulkannya. Setiap pemrosesan membutuhkan tujuan yang jelas, dasar yang tepat, data minimum, keamanan, retensi terbatas, transparansi, dan proses hak. UU PDP memberi kerangka hukum Indonesia; pelaksanaan yang efektif memerlukan pembagian tanggung jawab, kontrak vendor, desain sistem, dan kebiasaan kerja yang sesuai.

Risiko meningkat ketika sistem membuat profil, memakai biometrik, mengawasi ujian, memproses informasi sensitif, atau memengaruhi keputusan penting. Kampus membandingkan alternatif, menguji kesalahan dan bias, melibatkan mahasiswa, menyediakan peninjauan manusia, serta menghentikan penggunaan yang tidak dapat dipertanggungjawabkan. Penilaian dampak dan audit dilakukan sepanjang siklus hidup, bukan hanya sebelum peluncuran.

Perguruan tinggi dapat menggunakan AI untuk membantu belajar tanpa mengorbankan martabat dan kendali mahasiswa. Ukuran keberhasilan ialah apakah dukungan menjadi lebih berguna, keputusan lebih adil, data lebih terlindungi, dan kepercayaan akademik tetap terjaga. Tata kelola privasi yang kuat memberi ruang bagi inovasi karena mahasiswa dan dosen mengetahui batas, pilihan, dan tanggung jawab. Pendidikan tinggi yang cerdas adalah pendidikan yang tahu kapan data membantu dan kapan privasi manusia harus didahulukan.

55. Privasi sebagai amanah institusi pendidikan

Perguruan tinggi dapat dipahami sebagai pemegang amanah informasi karena mahasiswa mempercayakan data untuk memperoleh pendidikan dan layanan. Gagasan ini tidak menggantikan status hukum pengendali atau prosesor, tetapi memberi lensa etis: institusi menggunakan data untuk kepentingan pendidikan yang dapat dijelaskan, menghindari konflik kepentingan, dan menjaga kepentingan mahasiswa saat menentukan praktik. Kepercayaan bukan sumber data tanpa batas; ia menuntut kewajiban untuk merawat informasi secara bertanggung jawab.

Amanah data mencakup tindakan aktif, seperti menjelaskan aliran informasi, membatasi akses, menghapus salinan yang tidak diperlukan, serta menyediakan jalur pertanyaan. Institusi memberi tahu mahasiswa bila sistem berubah dan tidak menyembunyikan penggunaan sekunder di dalam bahasa kontrak yang sulit dibaca. Tindakan tersebut menunjukkan bahwa nilai pendidikan menjadi pertimbangan utama.

Pendekatan amanah dapat memperkaya kepatuhan hukum dengan menanyakan apakah penggunaan patut, bermanfaat, dan dapat diterima dalam relasi akademik. Mahasiswa tidak harus membuktikan kerugian sebelum kampus memperbaiki desain yang terlalu mengawasi. Hak dan tanggung jawab tetap ditafsirkan menurut hukum, sementara etika membantu institusi mengambil keputusan yang bijaksana ketika aturan belum menjawab setiap situasi.

56. Menafsirkan aturan dalam operasi sehari-hari

UU PDP mengubah pelindungan data menjadi tanggung jawab operasional: institusi harus mengetahui data apa yang diproses, untuk tujuan apa, oleh siapa, dan dengan perlindungan apa. Perguruan tinggi menerjemahkan norma tersebut ke dalam formulir, konfigurasi, kontrak, prosedur permintaan

hak, evaluasi dampak, serta tanggapan insiden. Tanpa langkah operasional, kebijakan dapat terdengar lengkap tetapi tidak mengubah penggunaan sehari-hari.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga relevan bagi kewajiban penyelenggara sistem elektronik, berdampingan dengan UU PDP dan aturan sektoral. PP Nomor 17 Tahun 2025 berfokus pada tata kelola sistem elektronik dalam pelindungan anak dan menjadi relevan bila layanan kampus melibatkan pengguna anak. Tim hukum mengonfirmasi cakupan serta aturan pelaksana terbaru untuk konteks tertentu. (Republik Indonesia, 2019).

Pemetaan hukum dilakukan per tujuan, bukan sekadar per aplikasi. Satu platform dapat dipakai untuk layanan pembelajaran, riset, dan pemasaran, yang masing-masing memiliki kebutuhan dan dasar berbeda. Institusi menyimpan alasan penggunaan dan meninjau kembali saat fungsi baru diaktifkan. Dengan cara ini, kepatuhan terikat pada alur nyata dan tidak berhenti pada nama vendor.

57. Inventaris dan kamus data mahasiswa

Kamus data menjelaskan nama atribut, sumber, format, pemilik, tujuan, klasifikasi, akurasi, retensi, dan penerima. Contohnya, “kehadiran” dapat berasal dari presensi kelas, log LMS, atau rekaman proktor, dan masing-masing memiliki tingkat akurasi serta konsekuensi berbeda. Definisi yang jelas mencegah staf menganggap semua data dengan label sama dapat dipertukarkan. Kamus data juga membantu menemukan atribut yang tidak lagi diperlukan.

Inventaris mencatat relasi antarsistem dan cara data mengalir, termasuk ekspor manual dan akun pihak ketiga. Setiap aliran memiliki pengendali, prosesor, dasar pemrosesan, ukuran kelompok, dan titik penghapusan.

Diagram dapat dibuat sesederhana yang diperlukan, asalkan tim dapat menggunakannya untuk menjawab permintaan hak atau menelusuri insiden. Inventaris diperbarui saat integrasi dan fitur baru diluncurkan.

Kualitas data merupakan bagian dari privasi karena informasi yang salah dapat menghasilkan tindakan yang merugikan. Institusi menunjukkan tanggal pembaruan, sumber, dan proses koreksi. Data yang tidak akurat dibatasi penggunaannya sampai diperbaiki. Kamus yang transparan juga menolong mahasiswa memahami istilah seperti “aktivitas”, “keterlibatan”, atau “risiko”, yang dapat memiliki makna berbeda bagi sistem dan pengguna.

58. Tata kelola identitas, pseudonim, dan pengaitan akun

Akun tunggal memudahkan akses ke beragam sistem, tetapi juga memungkinkan penyatuan riwayat lintas mata kuliah. Kampus membedakan autentikasi dari analitik: sistem dapat memverifikasi bahwa seseorang berhak masuk tanpa mengirim nomor identitas ke setiap alat pembelajaran. Token sementara atau pseudonim mengurangi penyebaran pengenal langsung. Jika pengaitan diperlukan untuk dukungan, tujuan dan durasinya harus jelas.

Pseudonim bukan anonimitas. Unit tertentu mungkin dapat menghubungkan kode dengan nama, sehingga hak akses terhadap tabel penghubung dibatasi. Peneliti menerima data yang lebih minim dan tidak menerima kunci tanpa alasan. Penyedia eksternal hanya memperoleh atribut yang diperlukan untuk menjalankan layanan. Catatan audit merekam akses istimewa dan peninjauan berkala memeriksa apakah akses masih sesuai peran.

Mahasiswa perlu cara memisahkan identitas profesional, sosial, dan akademik bila layanan menghubungkan beberapa akun. Penggunaan akun pribadi untuk layanan kampus dapat menyatukan konteks secara tidak diharapkan. Institusi menawarkan identitas akademik terkelola dan menjelaskan

konsekuensi akun tunggal. Tata kelola identitas menjaga kenyamanan tanpa membuat setiap aktivitas mudah dipetakan ke satu profil menyeluruh.

59. Aplikasi pihak ketiga dan praktik penggunaan informal

Dosen dan mahasiswa sering mencoba aplikasi gratis untuk meringkas, menerjemahkan, membuat soal, atau menganalisis data. Aplikasi informal dapat mengumpulkan lebih banyak informasi daripada layanan resmi dan mungkin menyimpan data di luar kendali kampus. Larangan tanpa alternatif yang praktis mendorong penggunaan tersembunyi. Institusi memelihara daftar alat yang telah diperiksa dan memberi jalur cepat untuk menilai layanan baru.

Praktik bring-your-own-tool perlu dipandu oleh contoh data yang boleh dan tidak boleh dimasukkan. Tugas kelompok tidak mengunggah daftar anggota, umpan balik dosen, atau hasil wawancara ke alat publik. Dosen yang memilih sistem untuk kursus memeriksa persyaratan lisensi dan fitur retensi. Mahasiswa dapat melaporkan alat yang digunakan secara transparan tanpa langsung dicurigai melanggar integritas.

Pemantauan lalu lintas jaringan untuk menemukan layanan tidak disetujui sendiri dapat menimbulkan masalah privasi tambahan. Kampus menggunakan langkah yang proporsional, memusatkan komunikasi dan edukasi, dan hanya melakukan pemantauan khusus dengan dasar serta pemberitahuan yang tepat. Tujuan pengendalian adalah mengurangi paparan data, bukan memperluas pengawasan mahasiswa.

60. Perangkat pribadi, jaringan kampus, dan BYOD

Mahasiswa mengakses layanan lewat ponsel, komputer pribadi, perangkat pinjaman, dan jaringan publik. Perangkat bersama dapat menyimpan kata sandi, cache, atau dokumen lokal yang mudah dilihat orang lain. Panduan

keamanan menjelaskan cara keluar dari akun, menghapus berkas sementara, menggunakan autentikasi, dan mengenali tautan palsu. Langkah ini disampaikan tanpa menyalahkan mahasiswa yang tidak memiliki perangkat pribadi.

Kebijakan bring-your-own-device mempertimbangkan batas kendali kampus atas perangkat pribadi. Pengelolaan jarak jauh yang dapat menghapus seluruh isi perangkat tidak proporsional untuk aktivitas kuliah biasa. Jika aplikasi harus mengakses kamera, lokasi, kontak, atau mikrofon, alasan dan durasinya dijelaskan. Fitur yang tidak diperlukan dinonaktifkan secara default.

Jaringan kampus dan Wi-Fi tamu menghasilkan log yang dapat menunjukkan lokasi atau pola kunjungan. Retensi log dibatasi untuk keamanan jaringan dan tidak dipakai untuk menilai kehadiran atau keterlibatan tanpa tujuan serta pemberitahuan baru. Akses terhadap log dipisahkan dari fungsi akademik. Transparansi membantu mahasiswa membedakan pemantauan keamanan teknis dari evaluasi pendidikan.

61. Sensor kampus dan ruang belajar cerdas

Kampus dapat menggunakan kartu akses, sensor hunian, kamera keamanan, beacon, atau perangkat Internet of Things untuk mengelola gedung. Jika data tersebut dihubungkan dengan identitas mahasiswa, informasi tentang rutinitas, tempat belajar, dan interaksi dapat terbentuk. Institusi tidak menggabungkan data fasilitas dengan rekam akademik hanya karena integrasi tersedia. Penggunaan untuk keselamatan, energi, dan pembelajaran dinilai secara terpisah.

Sensor sebaiknya mengumpulkan data agregat bila tujuan dapat tercapai tanpa identifikasi. Misalnya, penghitungan jumlah orang di ruang belajar dapat menggunakan sensor yang tidak menyimpan wajah atau identitas kartu. Papan informasi menjelaskan kamera atau sensor aktif, tujuan, retensi, dan

kontak. Area konseling, kesehatan, dan layanan sensitif memiliki perlindungan yang lebih kuat.

Data fasilitas tidak menjadi bukti bahwa mahasiswa hadir belajar atau berperilaku tertentu. Kartu yang digunakan orang lain, pintu yang terbuka, dan perangkat yang berbagi dapat membuat catatan keliru. Data sensor digunakan sesuai tujuan teknis dan dikoreksi ketika berdampak pada individu. Keterbatasan pengukuran disampaikan agar log tidak berubah menjadi narasi pasti tentang mahasiswa.

62. Privasi dalam kelas daring dan rekaman perkuliahan

Kelas daring dapat menghasilkan rekaman suara dan gambar dosen, mahasiswa, percakapan, nama pengguna, serta isi ruang pribadi. Sebelum merekam, pengajar menjelaskan tujuan, penerima, lama simpan, dan apakah kamera mahasiswa perlu aktif. Alternatif seperti pertanyaan tertulis, nama tampilan, atau rekaman tanpa peserta dapat mengurangi pengumpulan. Materi rekaman disimpan pada layanan yang telah dinilai.

Rekaman kuliah dapat membantu mahasiswa yang tidak hadir atau memerlukan akses ulang, tetapi tidak otomatis boleh digunakan untuk pelatihan model atau publikasi. Hak cipta materi dan persetujuan peserta dipertimbangkan terpisah. Bagian diskusi pribadi dapat dipotong atau tidak direkam. Pengajar memberi tahu jika transkripsi otomatis aktif dan apakah teks transkrip disimpan.

Mahasiswa yang berbicara tentang pengalaman sensitif perlu mengetahui bahwa komentar mereka dapat ditonton ulang. Institusi menyediakan kanal yang memungkinkan partisipasi tanpa tampil pada rekaman bila capaian tidak mensyaratkannya. Penghapusan rekaman mengikuti jadwal dan menghindari penyimpanan permanen “untuk berjaga-jaga”. Praktik ini menjaga akses belajar tanpa menjadikan ruang privat peserta sebagai arsip kampus.

63. Sistem manajemen pembelajaran dan telemetri

LMS mencatat akses materi, waktu, unggahan, nilai, pesan, forum, dan aktivitas kelompok. Sebagian telemetri dibutuhkan untuk menjalankan sistem atau melihat gangguan, sebagian lain digunakan untuk analitik. Pemberitahuan menjelaskan perbedaan fungsi tersebut. Kampus mengaktifkan hanya fitur yang diperlukan dan meninjau pengaturan bawaan vendor yang mungkin mengumpulkan data tambahan.

Pengajar sering menerima dashboard yang merangkum aktivitas, tetapi indikator harus dibaca sesuai definisi. “Tidak aktif” dapat berarti mahasiswa membaca materi luring, mengunduh berkas sekali, atau menggunakan aplikasi lain. Interpretasi terburu-buru dapat merusak kepercayaan. Dosen menghubungi mahasiswa dengan bahasa terbuka dan menyediakan cara untuk mengoreksi log yang tidak tepat.

Data dari LMS dipisahkan menurut kursus dan periode jika tidak ada kebutuhan untuk menggabungkannya. Akses staf berakhir ketika tugas mengajar selesai, kecuali kewajiban penilaian atau audit berlaku. Akun vendor dibatasi. Institusi memeriksa ekspor dan cadangan agar penutupan kursus tidak meninggalkan data berlebihan.

64. Sistem pengawasan ujian dan alternatif yang lebih ringan

Pengawasan ujian jarak jauh sering dibenarkan untuk menjaga integritas, tetapi perekaman luas membawa risiko dan beban. Sistem dapat salah menandai gerakan, suara, atau perubahan layar sebagai kecurangan. Kampus terlebih dahulu meninjau apakah penilaian dapat dirancang ulang melalui pertanyaan terbuka, variasi kasus, presentasi, portofolio, atau ujian lisan. Alternatif tersebut dapat mengukur penalaran lebih baik dengan data yang lebih sedikit.

Jika proctoring dipakai, persyaratan perangkat, aksesibilitas, lingkungan rumah, dan privasi anggota keluarga dipertimbangkan. Mahasiswa diberi pilihan yang setara ketika ruangnya tidak dapat direkam. Data video dan flag otomatis dilindungi, diperiksa manusia, dan dihapus setelah proses banding selesai. Perusahaan tidak boleh menggunakan rekaman untuk tujuan sekunder yang tidak dinyatakan.

Institusi mengevaluasi keadilan dan akurasi di kondisi yang beragam, termasuk koneksi lambat dan penggunaan perangkat lama. Prosedur sanggahan tidak membebankan biaya pada mahasiswa. Temuan salah identifikasi, stres, atau gangguan teknis dilaporkan. Integritas akademik dan hak privasi diperlakukan sebagai tujuan yang harus diseimbangkan melalui rancangan, bukan dipilih salah satunya secara mutlak.

65. Catatan kelas, forum, dan komunikasi informal

Forum diskusi dan grup percakapan dapat memuat pandangan pribadi, konflik, identitas, dan gagasan yang belum matang. Pengarsipan seluruh interaksi mungkin tampak berguna untuk analitik, tetapi mahasiswa dapat berhenti berdiskusi secara terbuka. Kursus menjelaskan apakah forum hanya untuk komunitas kelas, berapa lama pesan tersedia, dan apakah model AI akan merangkum atau menilai kontribusi.

Chatbot yang merangkum diskusi perlu menghindari atribusi keliru kepada mahasiswa. Ringkasan dapat membagikan kembali komentar di luar konteks atau menghapus nuansa. Pengajar meninjau sebelum menyebarkan hasil. Mahasiswa dapat meminta komentar pribadi tidak ditampilkan pada publikasi kelas, sesuai tujuan dan aturan yang berlaku.

Grup belajar di luar platform kampus tidak otomatis berada di bawah kendali institusi. Namun, dosen yang mewajibkan aplikasi tertentu harus menilai syarat penggunaan, pemrosesan nomor telepon, dan visibilitas akun. Pilihan

kanal resmi yang lebih aman disediakan. Aturan komunikasi tidak boleh mengharuskan mahasiswa menyerahkan data kontak pribadi kepada seluruh kelas.

66. Privasi dalam pembelajaran terbuka dan MOOC

Kursus terbuka dapat melibatkan ribuan peserta lintas negara, layanan analitik, forum publik, dan vendor global. Keterbukaan memperluas akses tetapi meningkatkan kemungkinan profil perilaku dapat dicari atau disalin. Institusi menyampaikan apakah nama pengguna tampil ke publik, cara menghapus unggahan, dan batas kendali atas salinan pihak lain. Penggunaan data global dievaluasi menurut hukum yang mungkin berlaku bagi peserta.

Data pendaftaran terbuka tidak berarti peserta setuju untuk segala penelitian atau monetisasi. Persetujuan dan pemberitahuan membedakan penyelenggaraan kursus, evaluasi program, riset, serta pemasaran. Peneliti mempertimbangkan bahwa akun publik tetap dapat mengidentifikasi orang melalui kutipan yang dapat dicari. Hasil dipublikasikan dengan pengamanan kontekstual.

Sistem rekomendasi untuk kursus terbuka perlu mempertimbangkan bahwa peserta mungkin hanya belajar sebagian materi atau memakai akun bersama. Prediksi penyelesaian tidak digunakan sebagai diagnosis komitmen. Pengajar memilih indikator yang bermakna dan menyediakan materi unduhan. Evaluasi privasi mencakup jangkauan lintas yurisdiksi dan subprosesor yang berubah.

67. Keputusan berbasis data dalam layanan beasiswa

Pemrosesan data beasiswa menggabungkan nilai, kondisi ekonomi, data keluarga, dan dokumen pendukung. Data tersebut berisiko tinggi karena kesalahan dapat memengaruhi akses studi. Kampus mengumpulkan hanya bukti yang diperlukan untuk kriteria bantuan, membatasi akses pada petugas

berwenang, dan tidak menggunakan dokumen untuk analitik lain tanpa penilaian. Informasi tentang anggota keluarga juga ditangani secara hati-hati.

AI dapat membantu memeriksa kelengkapan atau menandai duplikasi, tetapi skor kebutuhan tidak berdiri sendiri. Petugas meninjau keadaan khusus dan dapat meminta klarifikasi secara aman. Keputusan menyebutkan kriteria, proses banding, dan kontak. Catatan model dan versi disimpan untuk audit, sementara dokumen pendukung dihapus sesuai jadwal.

Penerima bantuan mungkin enggan mengajukan karena khawatir informasi diketahui teman atau dosen. Kampus memisahkan informasi keuangan dari sistem kelas dan tidak menampilkan status beasiswa pada dashboard akademik. Data agregat untuk perencanaan anggaran tidak mengungkap individu. Privasi menjadi bagian dari akses setara terhadap dukungan.

68. Data karier, magang, dan kemitraan industri

Layanan karier mengumpulkan CV, minat pekerjaan, hasil asesmen, riwayat magang, dan umpan balik perusahaan. AI dapat merekomendasikan lowongan atau memperbaiki resume, tetapi data karier dapat memengaruhi reputasi dan peluang. Mahasiswa mengetahui apakah informasi dibagikan kepada perusahaan, berapa lama disimpan, dan apakah rekomendasi berasal dari profil otomatis.

Kemitraan industri tidak memberi perusahaan akses otomatis ke data mahasiswa. Kampus menetapkan kategori data, tujuan, penerima, masa simpan, dan dasar berbagi. Mahasiswa dapat memilih apakah profil mereka ditampilkan dan mengoreksi informasi. Data asesmen psikometrik tidak dipakai sebagai skor seleksi tanpa validasi dan pemberitahuan yang tepat.

Peringkat kandidat otomatis dapat memperkuat bias berdasarkan nama, lokasi, sekolah asal, atau gaya penulisan. Institusi mengaudit rekomendasi dan memberi jalur tinjauan manusia. Perusahaan menerima hanya informasi yang

relevan dengan kesempatan yang dipilih mahasiswa. Pelayanan karier bertujuan memperluas pilihan, bukan membangun profil permanen yang membatasi mobilitas.

69. Tanggung jawab etik komite penelitian

Komite etik penelitian menilai risiko terhadap partisipan, tetapi proyek analitik rutin dan pengembangan produk mungkin berada di wilayah yang tidak jelas. Institusi menetapkan kriteria kapan penilaian etik diperlukan dan bagaimana koordinasinya dengan fungsi privasi. Pengecualian dari telaah etik tidak otomatis menghilangkan kewajiban pelindungan data. Peneliti menyimpan alasan penetapan ruang lingkup.

Komite melihat relasi kuasa, kemampuan menolak, penggunaan ulang, penggabungan data, dampak kelompok, dan transparansi. Penggunaan log kursus oleh dosen yang sekaligus peneliti memerlukan pengamanan terhadap tekanan. Protokol menjelaskan cara mencegah dosen mengetahui pilihan partisipasi sebelum penilaian selesai.

Peninjauan berlanjut ketika metode atau tujuan berubah. Menambahkan model yang membuat prediksi baru dapat mengubah risiko awal. Komite meminta protokol diperbarui bila data sensitif muncul atau vendor berubah. Pendekatan ini menjaga penelitian inovatif tetap berada dalam tanggung jawab terhadap mahasiswa.

70. Privasi, inklusi, dan mahasiswa yang kurang terwakili

Kebijakan privasi kadang menganggap semua mahasiswa memiliki kemampuan membaca dokumen, perangkat, waktu, dan bahasa yang sama. Pemberitahuan dan kontrol harus aksesibel, kompatibel dengan pembaca layar, dan dapat digunakan melalui perangkat umum. Kampus juga mempertimbangkan mahasiswa yang berbagi perangkat, tinggal di asrama,

bekerja, atau memakai koneksi terbatas. Kegagalan akses dapat memaksa pengungkapan data atau penggunaan akun orang lain.

Audit kelompok perlu menjaga agar kategori analisis tidak mengekspos individu dalam kelompok kecil. Data sensitif untuk menguji keadilan dikumpulkan hanya dengan dasar, tujuan, dan perlindungan yang memadai. Jika kampus tidak dapat mengukur dampak kelompok secara aman, ia menggunakan metode kualitatif partisipatif dan melaporkan keterbatasan. Tidak mengukur bukan alasan menyatakan sistem adil.

Pilihan non-digital yang setara penting saat sistem AI menjadi syarat layanan. Mahasiswa dapat mengakses bantuan manusia, bahan cetak, atau metode penilaian lain. Alternatif tidak dibuat lebih sulit atau menurunkan nilai. Inklusi memastikan pelindungan privasi tidak hanya tersedia bagi pengguna yang mahir teknologi.

71. Pemberitahuan privasi yang efektif

Pemberitahuan efektif menjawab pertanyaan yang muncul pada titik penggunaan: apa yang dikumpulkan, mengapa, siapa melihat, berapa lama, apa dampaknya, serta bagaimana meminta bantuan. Ringkasan singkat dapat menggunakan diagram alur; rincian hukum tersedia untuk pembaca yang memerlukannya. Kampus menguji apakah mahasiswa benar-benar memahami, bukan sekadar membuka tautan.

Notifikasi kontekstual memberi penjelasan khusus saat mahasiswa mengunggah tugas ke AI, menyalakan kamera ujian, atau menyetujui berbagi portofolio. Pengulangan pemberitahuan perlu seimbang agar pengguna tidak mengalami fatigue. Pesan menonjolkan informasi yang berbeda dari ekspektasi wajar dan menjelaskan pilihan yang tersedia.

Pemberitahuan diperbarui ketika vendor, tujuan, atau masa retensi berubah. Riwayat versi disimpan dan pengguna diberi tahu jika perubahan material.

Penjelasan yang tepat waktu membuat keputusan lebih bermakna dibanding dokumen umum yang diterima saat pertama kali mendaftar.

72. Pengelolaan permintaan akses dan koreksi

Kampus menetapkan satu kanal untuk permintaan hak dan mengarahkan permintaan ke unit yang menguasai data. Identitas pemohon diverifikasi secukupnya agar tidak membuat mahasiswa menyerahkan data tambahan. Petugas mengumpulkan data dari sistem terkait, mencatat pengecualian, dan menjelaskan hasil dengan bahasa yang mudah dipahami. Waktu respons mengikuti batas hukum yang berlaku.

Koreksi nilai resmi mengikuti prosedur akademik, sedangkan koreksi log teknis mungkin dilakukan unit TI. Data yang dipakai sistem rekomendasi perlu dikoreksi di sumber dan kemudian diperbarui pada profil turunan. Mahasiswa diberi tahu bila sebuah inferensi tidak dapat “dihapus” dari model seketika, serta langkah mitigasi sementara.

Permintaan hak dapat menunjukkan pola masalah sistemik. Jika banyak mahasiswa meminta menghapus data yang tidak mereka ketahui, transparansi perlu diperbaiki. Jika koreksi berulang terjadi pada satu integrasi, validasi data diperiksa. Statistik permintaan menjadi salah satu indikator kualitas tata kelola.

73. Pembagian data antarfakultas dan unit layanan

Unit akademik sering meminta data dari bagian kemahasiswaan, perpustakaan, keuangan, dan TI untuk membuat profil menyeluruh. Berbagi data internal tetap merupakan pemrosesan dan memerlukan tujuan serta hak akses yang jelas. Kampus tidak menganggap label “internal” berarti tanpa risiko. Permintaan berbagi menjelaskan kebutuhan spesifik, atribut, penerima, masa, dan larangan penggunaan lanjutan.

Akses berdasarkan peran dan tujuan membatasi penyebaran. Penasihat mungkin melihat bahwa mahasiswa perlu menghubungi layanan beasiswa tanpa melihat jumlah utang keluarga. Dashboard dapat menampilkan saran tindakan tanpa membuka berkas sumber. Pemisahan ini mengurangi paparan sambil tetap memungkinkan dukungan yang relevan.

Perjanjian berbagi data mencakup keamanan, retensi, kontak insiden, dan verifikasi penghapusan. Audit memeriksa apakah penerima menggunakan data sesuai tujuan. Jika unit tidak lagi memerlukan informasi, akses dicabut. Tata kelola formal membantu kolaborasi tanpa menciptakan “data lake” yang dapat digunakan siapa pun.

74. Dokumentasi dan transparansi penggunaan sistem

Setiap sistem AI akademik memiliki dokumentasi tujuan, pemilik, data, model, vendor, pengguna, risiko, dan hasil uji. Dokumentasi mencatat versi serta pembaruan. Ringkasan publik menjelaskan fungsi dan batas sistem dengan tetap melindungi informasi keamanan. Catatan teknis yang memadai membantu kampus menjawab pertanyaan, menyelidiki keluhan, dan melakukan transisi ke sistem lain.

Transparansi institusi dapat berupa laporan tahunan jumlah sistem, kategori data, pemrosesan berisiko tinggi, insiden, permintaan hak, dan langkah perbaikan. Angka dilaporkan secara agregat agar tidak mengidentifikasi mahasiswa. Laporan juga menyebut penggunaan yang dihentikan dan alasan umum. Keterbukaan mengenai masalah memperkuat akuntabilitas.

Dokumentasi tidak berarti menyimpan seluruh data mahasiswa lebih lama. Institusi menyimpan catatan keputusan dan konfigurasi yang diperlukan, sementara konten pribadi mengikuti retensi tersendiri. Pemisahan ini menjaga auditabilitas tanpa menjadikan dokumentasi alasan retensi tanpa batas.

75. Prosedur tinjauan sebelum sistem dipakai

Sebelum peluncuran, pemilik sistem menjelaskan masalah yang ingin diatasi, kelompok terdampak, tujuan pemrosesan, alternatif, data yang diperlukan, dasar hukum, dan ukuran keberhasilan. Tim memeriksa vendor, integrasi, keamanan, aksesibilitas, transfer, retensi, dan pelatihan. Jika keputusan menyentuh nilai atau hak penting, tinjauan lebih mendalam dilakukan dan kewenangan manusia ditetapkan.

Prototipe menggunakan data sintetis dan diuji pada skenario normal serta kegagalan. Mahasiswa mencoba pemberitahuan, kontrol, dan mekanisme keberatan. Hasil uji ditinjau untuk akurasi, distribusi kesalahan, kemudahan pakai, dan konsekuensi. Risiko yang belum terselesaikan memiliki pemilik dan batas waktu; beberapa risiko menjadi alasan menunda.

Keputusan meluncurkan, membatasi, atau menolak ditandatangani pejabat berwenang. Rencana menetapkan cara memantau, melaporkan insiden, mengubah konfigurasi, dan menghentikan sistem. Dokumen ini menghubungkan tanggung jawab tata kelola dengan orang yang benar-benar dapat bertindak.

76. Menghentikan sistem dan menjaga portabilitas

Sistem AI dapat dihentikan karena biaya, kinerja, pelanggaran kontrak, bias, atau perubahan kebutuhan. Kampus merencanakan penghentian sejak pengadaan: format ekspor, pemindahan materi, penghapusan akun, pengembalian data, dan dukungan transisi. Tanpa rencana, mahasiswa dapat kehilangan riwayat belajar atau institusi terjebak pada vendor yang tidak lagi sesuai.

Penghentian juga mengatur inferensi dan profil yang telah dibuat. Institusi menentukan apakah data disimpan untuk arsip, dihapus, atau perlu diberi tanda bahwa rekomendasi tidak lagi berlaku. Staf diberi instruksi agar tidak

terus menggunakan label lama dalam proses manual. Mahasiswa mengetahui cara meminta salinan data yang berhak mereka peroleh.

Vendor mengeluarkan konfirmasi penghapusan dan mengidentifikasi pengecualian hukum yang masih berlaku. Kampus menguji hasilnya dan mematikan kunci atau integrasi. Evaluasi pascapenghentian menilai apakah risiko benar-benar berkurang dan pelajaran apa yang perlu diterapkan pada kontrak berikutnya.

77. Kesiapan kampus kecil dan kerja sama kapasitas

Perguruan tinggi dengan sumber daya terbatas dapat memulai dari inventaris sederhana, daftar alat yang disetujui, format pemberitahuan, dan prosedur insiden. Tidak setiap kampus harus membangun pusat AI atau sistem keamanan sendiri. Kerja sama asosiasi, layanan bersama, dan panduan nasional dapat menyediakan keahlian hukum serta teknis yang sulit diperoleh sendiri.

Paket model dokumen harus mudah disesuaikan dan tidak diperlakukan sebagai sertifikat kepatuhan otomatis. Kampus tetap menilai tujuan, data, vendor, dan karakter mahasiswa. Pelatihan lintas kampus mempercepat pembelajaran tentang insiden dan praktik yang berhasil tanpa membuka informasi pribadi.

Investasi prioritas dapat dimulai dari sistem berisiko paling tinggi, seperti rekaman ujian, data kesehatan, profil risiko, dan integrasi lintas platform. Pengendalian dasar pada area ini lebih penting daripada mempercantik dashboard. Pendekatan bertahap membuat peningkatan pelindungan dapat dijalankan secara realistis.

78. Nilai akademik dari batas privasi

Batas privasi membantu menciptakan ruang untuk bereksperimen, bertanya, dan gagal tanpa setiap tindakan menjadi catatan permanen. Ruang tersebut penting bagi pembelajaran karena mahasiswa membangun pemahaman melalui revisi dan perbedaan pendapat. Institusi yang mengurangi pemantauan yang tidak perlu dapat memperoleh diskusi yang lebih jujur dan hubungan bimbingan yang lebih kuat.

Keterbatasan data juga mendorong dosen merancang penilaian yang lebih bermakna. Alih-alih mengandalkan klik, kampus dapat meminta mahasiswa menjelaskan konsep, membuat proyek, atau berdialog tentang strategi. Bukti pembelajaran yang kaya tidak selalu memerlukan jejak digital yang lebih banyak. Nilai pendidikan menjadi lebih terlihat ketika kegiatan dirancang untuk tujuan yang jelas.

Privasi karena itu bukan biaya kepatuhan yang berdiri di luar misi akademik. Ia melindungi kondisi sosial yang memungkinkan kebebasan intelektual, kepercayaan, dan keterlibatan. AI dapat dipakai dalam batas yang ditentukan bersama komunitas akademik, dengan manfaat yang diuji dan tanggung jawab yang dapat dimintai penjelasan.

79. Mengukur kepercayaan dan pengalaman mahasiswa

Kepercayaan diukur dari pemahaman dan pengalaman, bukan hanya pernyataan bahwa kebijakan tersedia. Kampus dapat bertanya apakah mahasiswa tahu sistem apa yang memproses datanya, dapat menemukan saluran bantuan, dan merasa aman mengajukan koreksi. Survei anonim dilengkapi wawancara dan analisis keluhan. Penelitian menunjukkan bahwa kekhawatiran privasi berkaitan dengan kontrol yang dirasakan, kepercayaan, dan perilaku berbagi informasi (Mutimukwe et al., 2022; Jones, 2019).

Hasil dibedakan menurut layanan dan konteks. Mahasiswa mungkin mempercayai LMS untuk nilai namun tidak nyaman ketika rekaman suara dianalisis. Kepercayaan tidak menjadi angka tunggal yang dapat menggantikan penilaian hukum. Perbedaan tersebut membantu kampus menyesuaikan pemberitahuan, kontrol, dan batas pemakaian.

Bila kepercayaan menurun, institusi bertanya apakah penyebabnya adalah insiden, kurangnya penjelasan, pengalaman bias, atau ketidakmampuan memilih. Langkah korektif dijelaskan dan kemudian dievaluasi ulang. Keterbukaan terhadap kritik menjadi bagian penting dari tata kelola.

80. Prinsip ringkas bagi pimpinan perguruan tinggi

Pimpinan dapat mengajukan tujuh pertanyaan sebelum menyetujui sistem: tujuan apa yang hendak dicapai; data apa yang benar-benar diperlukan; siapa yang mengendalikan dan memprosesnya; apa yang diketahui mahasiswa; apa dampak kesalahan; bagaimana hak dan keberatan ditangani; dan kapan sistem akan ditinjau atau dihentikan. Jawaban harus merujuk pada bukti, kontrak, desain, serta penanggung jawab, bukan asumsi umum.

Pertanyaan tambahan menyangkut distribusi manfaat: apakah sistem membantu kelompok yang memiliki hambatan, atau hanya membuat proses lebih murah bagi institusi? Apakah dukungan manusia tetap tersedia? Apakah sistem mengubah penilaian akademik atau hubungan dengan dosen? Jawaban menentukan apakah pemrosesan proporsional dan sesuai misi.

Pimpinan menetapkan satu pemilik yang dapat dimintai pertanggungjawaban serta sumber daya untuk mitigasi. Persetujuan tidak menjadi cek kosong untuk penggunaan baru. Tata kelola berulang memberi kesempatan menyesuaikan sistem ketika bukti berubah. Model ini menghubungkan inovasi, hak mahasiswa, dan kualitas pendidikan dalam satu keputusan.

81. Keadilan dalam inferensi dan klasifikasi mahasiswa

Sistem dapat menyimpulkan mahasiswa “aktif”, “berisiko”, “membutuhkan bantuan”, atau “siap maju” dari perilaku digital. Kategori ini memengaruhi perhatian dosen dan sumber daya. Definisi operasional perlu dibuka dan diuji: apakah partisipasi berarti jumlah komentar, ketepatan waktu, atau refleksi? Jika indikator hanya menangkap perilaku yang mudah dihitung, sistem mungkin memberi gambaran yang berat sebelah.

Kategori tidak boleh menyatukan mahasiswa ke dalam kelompok tetap. Kesulitan pada satu mata kuliah bukan prediksi kemampuan umum; kebutuhan dukungan semester ini tidak mendefinisikan potensi. Inferensi diberi tanggal kedaluwarsa dan ditinjau berdasarkan bukti baru. Mahasiswa diberi kesempatan menjelaskan faktor yang tidak terlihat pada sistem, seperti akses, jadwal kerja, atau pengalaman sebelumnya.

Keadilan juga berarti tidak hanya menilai kesalahan model, tetapi menilai bagaimana manusia menggunakan hasilnya. Jika dosen memperlakukan skor tertentu sebagai fakta, bias dapat masuk melalui keputusan walaupun akurasi teknis cukup tinggi. Pelatihan dan audit mencakup interaksi antara dashboard dan perilaku staf. Tujuan klasifikasi adalah membuka bantuan, bukan menutup kesempatan.

82. Lokalisasi data dan kedaulatan digital kampus

Lokasi pusat data penting, tetapi bukan satu-satunya unsur kedaulatan digital. Pengendalian juga ditentukan oleh siapa mengelola kunci, siapa dapat mengakses dukungan, di mana subprosesor berada, serta apakah kampus dapat memindahkan data. Klaim bahwa layanan “lokal” diuji melalui peta pemrosesan yang mencakup log, cadangan, dan dukungan teknis.

Perguruan tinggi dapat mempertimbangkan infrastruktur lokal atau layanan bersama untuk sistem tertentu, tetapi solusi lokal tetap memerlukan

keamanan, pemeliharaan, dan tata kelola. Tidak ada jaminan bahwa penyimpanan di dalam negeri otomatis aman atau sesuai tujuan. Keputusan mempertimbangkan kontrol operasional, kualitas layanan, ketahanan, biaya, dan kewajiban hukum.

Kampus membangun kemampuan untuk memilih dan berpindah layanan. Format terbuka, dokumentasi, keahlian staf, dan kontrak yang dapat diakhiri mengurangi ketergantungan. Kolaborasi antarperguruan tinggi memperkuat kapasitas tawar terhadap vendor dan membuka peluang pengembangan alat yang sesuai bahasa serta konteks Indonesia.

83. Data mahasiswa sebagai aset pendidikan, bukan komoditas

Penyedia dapat memperoleh nilai komersial dari penggunaan data, pengembangan produk, analitik, atau pelatihan model. Institusi memeriksa apakah nilai tersebut sejalan dengan manfaat mahasiswa dan ketentuan hukum. Akses ke platform tidak otomatis memberikan hak untuk mengeksploitasi karya, prompt, atau data aktivitas. Kebijakan pengadaan secara eksplisit membatasi pemasaran, penjualan, dan penggunaan sekunder.

Data akademik mengandung kerja dan pengalaman mahasiswa. Jika kampus atau vendor menggunakan karya untuk melatih model, mahasiswa perlu mengetahui tujuan, hak, retensi, kemungkinan keluaran yang meniru materi, serta pilihan yang tersedia. Penggunaan yang tidak diperlukan bagi layanan utama dipisahkan dan memperoleh penilaian baru. Kampus tidak menyamarkan komersialisasi sebagai peningkatan layanan tanpa bukti.

Tata kelola data melihat mahasiswa sebagai pemilik hak dan peserta pendidikan, bukan sekadar sumber bahan baku. Institusi dapat menetapkan pembagian nilai, atribusi, atau manfaat publik dalam kerja sama penelitian sesuai konteks. Paling tidak, kampus harus dapat menjelaskan siapa yang

memperoleh manfaat ekonomi dan mengapa penggunaan data dianggap pantas.

84. Simulasi insiden untuk menguji kesiapan kampus

Bayangkan seorang dosen mengunggah lembar nilai dan catatan konsultasi ke layanan AI publik untuk membuat ringkasan kelas. Simulasi dimulai dengan pertanyaan siapa harus diberi tahu, bagaimana menghentikan akses, apakah vendor menyimpan salinan, data siapa yang terdampak, dan siapa menilai kewajiban pemberitahuan. Tim akademik, teknologi, hukum, komunikasi, dan privasi bekerja bersama dalam batas waktu nyata.

Latihan mengungkap apakah daftar kontak tersedia, kontrak memuat jalur insiden, dan pengajar memahami cara melaporkan. Tim menyiapkan pesan kepada mahasiswa yang menjelaskan fakta yang diketahui, tindakan, dan kontak bantuan. Mereka juga meninjau apakah catatan keuangan atau kesehatan ikut terunggah dan apakah akses atau kata sandi perlu dicabut.

Setelah simulasi, kampus memperbarui panduan penggunaan AI, konfigurasi unggah, pelatihan, dan prosedur respons. Fokusnya bukan menyalahkan satu dosen, melainkan memperbaiki sistem yang membuat kesalahan mudah terjadi. Simulasi berkala memastikan aturan dapat dipakai ketika situasi mendesak, bukan hanya disimpan dalam dokumen.

85. Kesimpulan operasional untuk pimpinan perguruan tinggi

Perlindungan privasi mahasiswa dalam ekosistem AI perlu diperlakukan sebagai tanggung jawab tata kelola akademik. Pimpinan perguruan tinggi dapat memulai dengan menetapkan penanggung jawab data, menyusun inventaris sistem dan aliran data, serta memetakan tujuan dan dasar pemrosesan untuk setiap layanan. Pemetaan ini perlu mencakup sistem yang dibeli dari vendor, integrasi dengan platform pembelajaran, aplikasi yang

digunakan unit akademik, dan perangkat yang mengumpulkan data di ruang belajar.

Setelah pemetaan, setiap penggunaan baru perlu dinilai berdasarkan kebutuhan pendidikan yang jelas, dampak terhadap mahasiswa, pilihan yang tersedia, kualitas dan keterbatasan model, serta risiko kebocoran atau penggunaan sekunder. Penilaian harus melibatkan fungsi akademik, teknologi informasi, hukum, keamanan informasi, pengelola data, dosen, dan perwakilan mahasiswa. Hasilnya diterjemahkan menjadi pembatasan akses, jadwal penghapusan, prosedur keberatan dan koreksi, mekanisme peninjauan manusia, serta pengawasan kontrak dan subprosesor.

Perguruan tinggi juga perlu menyediakan penjelasan yang dapat dipahami mahasiswa mengenai data apa yang dikumpulkan, untuk tujuan apa, siapa yang dapat mengaksesnya, berapa lama data disimpan, dan bagaimana meminta akses atau menyampaikan keberatan. Penjelasan itu harus hadir pada saat keputusan yang relevan dibuat, bukan hanya tersembunyi dalam dokumen kebijakan panjang. Kanal pelaporan insiden dan pengaduan perlu mudah ditemukan, menjaga kerahasiaan pelapor, dan memberi kepastian tentang tindak lanjut.

Keberhasilan tidak diukur dari banyaknya perangkat AI yang dipasang atau jumlah prediksi yang dihasilkan. Ukurannya ialah apakah dukungan belajar menjadi lebih tepat tanpa mengurangi hak mahasiswa; apakah sistem dapat dijelaskan dan dikoreksi; apakah keputusan berdampak penting tetap melibatkan penilaian manusia; dan apakah manfaatnya dinikmati secara adil oleh mahasiswa dengan latar, kemampuan, serta kondisi akses yang berbeda. Evaluasi berkala, audit independen yang proporsional, dan partisipasi mahasiswa membuat perlindungan privasi menjadi praktik nyata yang dapat diperbaiki dari waktu ke waktu.

Glossarium

AI generatif. Sistem AI yang menghasilkan teks, gambar, audio, kode, atau keluaran lain dari masukan pengguna dan pola yang dipelajarinya.

Anonimisasi. Pengolahan untuk menghilangkan kemungkinan identifikasi seseorang secara wajar; kekuatannya bergantung pada data dan konteks pengaitan.

Data biometrik. Data pribadi yang dihasilkan dari pemrosesan teknis ciri fisik, fisiologis, atau perilaku yang dapat mengidentifikasi seseorang.

Data pribadi. Informasi tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, secara langsung maupun tidak langsung.

Data pribadi spesifik. Kategori data pribadi yang oleh UU PDP diberi perlindungan khusus, termasuk kesehatan, biometrik, data anak, dan kategori lain yang ditentukan undang-undang.

Dampak privasi. Konsekuensi terhadap martabat, otonomi, keamanan, kepercayaan, atau hak seseorang akibat pemrosesan data.

Differential privacy. Teknik statistik yang membatasi kontribusi data individu terhadap keluaran agregat melalui penambahan noise terukur.

Hak subjek data. Hak orang yang datanya diproses, termasuk hak memperoleh informasi, mengakses, memperbaiki, dan hak lain sesuai UU PDP.

Learning analytics. Pengukuran dan analisis data peserta didik serta konteksnya untuk memahami dan memperbaiki proses belajar.

Minimisasi data. Pembatasan pemrosesan pada data yang relevan dan diperlukan bagi tujuan spesifik.

Pengendali data pribadi. Pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi sesuai peraturan.

Pemroses data pribadi. Pihak yang memproses data pribadi atas nama pengendali sesuai instruksi dan ketentuan yang berlaku.

Pseudonimisasi. Penggantian pengenal langsung dengan kode sehingga pengaitan kembali memerlukan informasi tambahan yang dipisahkan.

Profiling. Pemrosesan otomatis data untuk menilai atau memperkirakan aspek pribadi seseorang.

Privacy by design. Pendekatan yang memasukkan pelindungan data ke dalam tujuan, arsitektur, dan operasi sistem sejak tahap desain.

Privacy by default. Konfigurasi awal yang membatasi pemrosesan pada tingkat yang diperlukan bagi tujuan yang telah ditetapkan.

Penilaian dampak pelindungan data. Analisis sebelum pemrosesan berisiko tinggi untuk mengidentifikasi dan mengurangi risiko terhadap hak dan kebebasan subjek data.

Retensi data. Jangka waktu penyimpanan data beserta aturan pengarsipan, pembatasan, dan penghapusannya.

Sistem keputusan otomatis. Sistem yang menghasilkan atau membantu keputusan melalui pemrosesan otomatis, dengan dampak yang bervariasi menurut konteks.

Transfer lintas batas. Pemindahan atau pemberian akses terhadap data pribadi ke pihak atau sistem di luar wilayah Indonesia, sesuai ketentuan hukum.

Vendor. Penyedia produk atau layanan yang dapat memproses, menyimpan, atau mengakses data kampus dan mahasiswa.

Daftar Pustaka

Alfredo, R., Echeverria, V., Jin, Y., Yan, L., Swiecki, Z., Gašević, D., & Martinez-Maldonado, R. (2024). Human-centred learning analytics and AI in education: A systematic literature review. *Computers and Education: Artificial Intelligence, 6*, Article 100215. https://doi.org/10.1016/j.caeai.2024.100215

Bond, M., Khosravi, H., De Laat, M., Bergdahl, N., Negrea, V., Oxley, E., Pham, P., Chong, S. W., & Siemens, G. (2024). A meta systematic review of artificial intelligence in higher education: A call for increased ethics, collaboration, and rigour. *International Journal of Educational Technology in Higher Education, 21*, Article 4. https://doi.org/10.1186/s41239-023-00436-z

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Hakimi, L., Eynon, R., & Murphy, V. A. (2021). The ethics of using digital trace data in education: A thematic review of the research landscape. *Review of Educational Research, 91(5)*, 671–717. https://doi.org/10.3102/00346543211020116

Jones, K. M. L. (2019). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education, 16*, Article 24. https://doi.org/10.1186/s41239-019-0155-0

Kizilcec, R. F. (2016). How much information? Effects of transparency on trust in an algorithmic interface. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2390*–2395. https://doi.org/10.1145/2858036.2858402

Mutimukwe, C., Viberg, O., Öberg, L.-M., & Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology, 53(4)*, 932–951. https://doi.org/10.1111/bjet.13234

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology, 45(3)*, 438–450. https://doi.org/10.1111/bjet.12152

Prinsloo, P. (2022). The answer is (not only) technological: Considering student data privacy in learning analytics. *British Journal of Educational Technology, 53(4)*, 876–893. https://doi.org/10.1111/bjet.13216

Prinsloo, P., & Slade, S. (2017). An elephant in the learning analytics room: The obligation to act. *Proceedings of the Seventh International Learning Analytics & Knowledge Conference, 46*–55. https://doi.org/10.1145/3027385.3027406

Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Republik Indonesia. (2025). Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak. https://peraturan.bpk.go.id/Details/316698/pp-no-17-tahun-2025

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist, 57(10)*, 1510–1529. https://doi.org/10.1177/0002764213479366

UNESCO. (2023). Guidance for generative AI in education and research. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386693

UNESCO. (2024a). AI competency framework for students. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000391105

UNESCO. (2024b). AI competency framework for teachers. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000391104

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education—Where are the educators? *International Journal of Educational Technology in Higher Education, 16*, Article 39. https://doi.org/10.1186/s41239-019-0171-0