
PELINDUNGAN DATA PRIBADI:
FONDASI KEPERCAYAAN TERHADAP AI
RudyCT Academic Series | IBM-ASMI
AI
1
TUJUAN YANG JELAS
Data dipakai untuk tujuan yang sah dan spesifik
2
MINIMISASI DATA
Kumpulkan hanya yang benar-benar diperlukan
3
TRANSPARANSI
Jelaskan penggunaan data dan dampak keputusan AI
4
KEAMANAN & PRIVASI
Lindungi data sepanjang siklus hidup AI
5
AKUNTABILITAS
Audit, koreksi, keberatan, dan pemulihan
SIKLUS TATA KELOLA AI
Tentukan tujuan
Petakan data
Nilai dampak
Uji dan awasi
Perbaiki atau hentikan
Kepercayaan tumbuh ketika AI dapat diperiksa, dijelaskan, dan dikoreksi.
Oleh: Prof Ir Rudy C Tarumingkeng, PhD
Guru Besar Manajemen dan AI Data Analyst
www.rudyct.com/cv.pdf | IBM-ASMI

Perlindungan Data Pribadi sebagai Fondasi Kepercayaan terhadap AI

Prof Ir Rudy C Tarumingkeng, PhD

www.rudyct.com/cv.pdf

Guru Besar Manajemen dan AI Data Analyst

IBM-ASMI | RudyCT Academic Series

Abstract

Artikel ini membahas perlindungan data pribadi sebagai prasyarat kepercayaan publik terhadap kecerdasan artifisial (AI), bukan semata-mata kewajiban kepatuhan. AI modern memperoleh kemampuan dari data, tetapi pengumpulan, penggabungan, inferensi, penggunaan ulang, dan penyimpanan data dapat menimbulkan risiko terhadap otonomi, keamanan, kesetaraan, serta martabat manusia. Dengan pendekatan konseptual dan analisis kebijakan, tulisan ini menghubungkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dengan siklus hidup AI, prinsip etika AI Indonesia, dan praktik tata kelola risiko internasional. Pembahasan mencakup dasar pemrosesan, pembatasan tujuan, minimisasi, transparansi, hak subjek data, keputusan otomatis, keamanan, transfer lintas batas, teknologi peningkat privasi, serta akuntabilitas organisasi. Artikel mengusulkan model tata kelola yang memadukan perlindungan sejak desain, penilaian dampak, pengawasan manusia yang bermakna, dokumentasi, audit, dan pemulihan bagi pihak terdampak. Kepercayaan tidak tumbuh dari klaim bahwa AI akurat atau canggih, melainkan dari bukti bahwa sistem bekerja secara sah, aman, dapat dipahami, dapat digugat, dan memperlakukan manusia secara adil.

Kata kunci: kecerdasan artifisial, data pribadi, privasi, kepercayaan digital, UU PDP, tata kelola AI, akuntabilitas, privacy by design

Pendahuluan

Kecerdasan artifisial semakin hadir dalam keputusan yang dahulu dilakukan melalui percakapan langsung antara manusia: bank menilai kelayakan kredit, perusahaan menyaring pelamar, platform memilih rekomendasi yang ditampilkan, rumah sakit mengurutkan risiko pasien, sekolah mengelola pembelajaran, dan instansi publik menyalurkan layanan. Di balik setiap prediksi terdapat rangkaian data, asumsi, dan keputusan desain. Sistem dapat menampilkan jawaban dalam hitungan detik, tetapi dampaknya terhadap seseorang dapat berlangsung lama: permohonan pinjaman ditolak, kesempatan kerja menyempit, harga yang ditawarkan berbeda, atau informasi sensitif tersingkap.

Pertanyaan utama karena itu bukan hanya apakah AI bekerja dengan baik, melainkan apakah data yang membuatnya bekerja diperoleh dan digunakan secara patut. Ketika orang memberikan data untuk satu layanan, mereka biasanya tidak membayangkan data itu akan digabungkan dengan catatan lain, dipakai untuk menaksir keadaan yang belum pernah mereka ungkapkan, atau dimasukkan ke dalam model yang digunakan oleh pihak berbeda. Kesenjangan antara harapan manusia dan operasi sistem menjadi sumber ketidakpercayaan. Perlindungan data pribadi membantu memperkecil kesenjangan tersebut dengan menetapkan batas mengenai siapa boleh memproses data, untuk tujuan apa, atas dasar apa, berapa lama, dengan pengamanan apa, dan bagaimana seseorang dapat meminta penjelasan atau koreksi.

Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menyediakan kerangka hak dan kewajiban yang menyentuh seluruh rangkaian pemrosesan. Undang-undang itu mencakup hak subjek data, dasar pemrosesan, kewajiban pengendali dan prosesor, transfer

data, sanksi, serta ketentuan pidana. UU PDP berlaku sejak diundangkan pada 17 Oktober 2022 dan menetapkan masa penyesuaian dua tahun (Republik Indonesia, 2022). Keberadaan kerangka hukum ini penting, tetapi tidak otomatis menjamin kepatuhan. Perusahaan tetap perlu mengubah proses bisnis, kontrak, arsitektur teknologi, kebijakan retensi, pelatihan, dan mekanisme penanganan pengaduan.

Konteks AI membuat tugas itu lebih rumit. Model dapat menyerap pola dari banyak data dan menghasilkan inferensi baru. Data yang tampak biasa, jika digabungkan, dapat menyimpulkan kondisi kesehatan, keyakinan, lokasi, tingkat pendapatan, atau kerentanan seseorang. Dalam sistem generatif, masukan pengguna dapat tersimpan pada log, dievaluasi untuk meningkatkan model, atau diteruskan ke penyedia layanan lain. Akibatnya, perlindungan data tidak bisa dibatasi pada halaman persetujuan atau kebijakan privasi. Perlindungan harus menjadi bagian dari pilihan tujuan, pemilihan data, desain model, evaluasi, pengoperasian, pemantauan, dan penghentian sistem.

Tesis tulisan ini adalah bahwa perlindungan data pribadi merupakan fondasi kepercayaan terhadap AI karena mengubah kepercayaan dari harapan abstrak menjadi tata kelola yang dapat diperiksa. Kepercayaan yang sehat bukan kepatuhan buta kepada sistem, melainkan kesediaan untuk mengandalkannya secara proporsional ketika hak, tanggung jawab, batas penggunaan, dan pemulihan telah dirancang dengan jelas. Artikel ini menguraikan alasan konseptual, kerangka hukum, risiko sepanjang siklus hidup, perangkat teknis dan organisasi, serta agenda penerapan bagi pemerintah, perusahaan, perguruan tinggi, dan masyarakat sipil.

1. Memahami hubungan antara data, AI, dan kepercayaan

AI bukan satu benda tunggal. Istilah ini mencakup sistem berbasis aturan, pembelajaran mesin, pengenalan pola, pemrosesan bahasa, sistem rekomendasi, dan model generatif. Sebagian sistem memberi rekomendasi

kepada operator; sebagian lain mengotomatiskan keputusan. Perbedaan ini penting karena risikonya bergantung pada tujuan, konteks, skala, kelompok terdampak, dan seberapa besar manusia masih dapat mengintervensi hasilnya. Sistem penyaring spam memiliki dampak berbeda dari sistem yang menilai risiko kriminal atau menentukan akses bantuan sosial.

Data pribadi adalah informasi tentang orang yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun melalui penggabungan informasi. Nama dan nomor identitas jelas bersifat personal, tetapi pengenal daring, pola lokasi, rekaman suara, citra wajah, identitas perangkat, atau kombinasi atribut dapat juga mengidentifikasi individu. UU PDP membedakan data pribadi yang bersifat umum dan spesifik. Kategori spesifik antara lain data kesehatan, biometrik, genetika, catatan kejahatan, data anak, dan data keuangan pribadi (Republik Indonesia, 2022). Kategori ini membantu organisasi mengenali tingkat sensitivitas, namun data yang tidak masuk kategori khusus pun dapat menimbulkan risiko besar bila dipakai untuk membuat keputusan yang berdampak.

Kepercayaan adalah penilaian relasional. Pengguna mempercayai bukan hanya model, melainkan organisasi yang mengumpulkan data, pemasok teknologi, operator, auditor, dan regulator yang membentuk lingkungan penggunaannya. Sistem dapat bekerja secara teknis tetapi tidak layak dipercaya apabila pemiliknya menyembunyikan tujuan, mengabaikan keberatan, atau tidak menyediakan jalan pemulihan. Sebaliknya, sistem yang memiliki keterbatasan tetapi mengungkapkannya, menguji dampaknya, dan menyediakan koreksi dapat dinilai lebih dapat dipercaya daripada sistem yang mengklaim objektivitas sempurna. Literatur tata kelola AI menekankan bahwa kepercayaan berkaitan dengan sifat sistem dan institusi yang menggunakannya, bukan sekadar persepsi terhadap mesin (Kerasidou, 2024).

Tiga gagasan perlu dibedakan. Privasi adalah ruang bagi seseorang untuk mengelola akses terhadap dirinya dan kehidupannya. Pelindungan data adalah perangkat hukum, teknis, dan organisasi untuk mengatur pemrosesan informasi personal. Keamanan informasi menjaga kerahasiaan, integritas, dan ketersediaan sistem serta data. Ketiganya beririsan, tetapi tidak sama. Enkripsi yang kuat tidak membuat pemrosesan menjadi sah jika tujuannya tidak patut. Sebaliknya, persetujuan yang sah tidak cukup bila data bocor karena pengamanan lemah. Kepercayaan membutuhkan semua unsur tersebut sekaligus.

2. Mengapa kepercayaan adalah modal sosial bagi AI

AI hanya dapat memberi manfaat secara berkelanjutan bila orang bersedia berinteraksi dengannya dan menyediakan data yang memang diperlukan. Pengguna yang memahami tujuan layanan, melihat manfaat yang proporsional, dan memiliki kendali yang nyata cenderung lebih siap menggunakan sistem. Namun, keterlibatan itu bukan cek kosong. Ketika organisasi mengumpulkan data berlebihan, mengubah tujuan diam-diam, atau memanfaatkan kerentanan pengguna, kepercayaan dapat runtuh dengan cepat. Dampaknya dapat meluas dari satu aplikasi ke layanan digital lain, bahkan menurunkan kesediaan warga untuk menggunakan layanan publik.

Perlindungan yang kuat juga memberi manfaat ekonomi. Perusahaan yang mengelola data dengan baik dapat mengurangi risiko insiden, sengketa, biaya pemulihan, dan gangguan operasional. Pelanggan bisnis dapat lebih mudah menilai vendor yang mendokumentasikan aliran data serta kontrol keamanan. Bagi usaha kecil dan menengah, pendekatan yang sederhana tetapi konsisten—inventaris data, pembatasan akses, retensi yang jelas, dan kontrak vendor yang masuk akal—dapat menjadi pembeda dalam persaingan. Kepercayaan mendorong penggunaan berulang dan kemitraan jangka

panjang, sedangkan pemrosesan oportunistik menghasilkan keuntungan jangka pendek dengan kewajiban tersembunyi yang besar.

Kepercayaan memiliki batas rasional. Pengguna tidak harus mempercayai semua algoritma, dan kehati-hatian bukan sikap anti-teknologi. Dalam layanan berisiko tinggi, ketidakpercayaan fungsional—meminta bukti, melakukan audit, membandingkan keluaran dengan sumber independen—membantu mencegah kesalahan dan penyalahgunaan. Kerasidou (2024) mengingatkan bahwa tata kelola AI yang layak membutuhkan pemahaman mengenai bagaimana kepercayaan diberikan dan bagaimana institusi membuktikan kelayakannya. Dalam praktiknya, organisasi harus memfasilitasi verifikasi, bukan menuntut keyakinan berdasarkan merek atau kecanggihan model.

Kepercayaan tidak dapat dibeli hanya dengan antarmuka yang ramah. Pemberitahuan yang mudah dibaca memang membantu, tetapi janji privasi harus sesuai dengan konfigurasi sistem, kontrak pemasok, serta perilaku nyata. Bila sebuah layanan mengatakan data tidak digunakan untuk pelatihan, tetapi pengaturan teknis mengirimkan log ke vendor yang memanfaatkannya untuk tujuan lain, janji tersebut tidak memiliki nilai. Oleh karena itu, tata kelola yang baik menghubungkan komunikasi eksternal dengan kontrol internal dan bukti audit.

3. Kerangka hukum Indonesia dan relevansinya terhadap AI

UU PDP menempatkan pelindungan data pribadi sebagai upaya untuk melindungi hak konstitusional subjek data dalam rangkaian pemrosesan. Kerangka tersebut relevan bagi AI sebab pemrosesan berlangsung jauh melampaui tahap pengumpulan. Data dapat dikurasi, diberi label, digabungkan, dipakai melatih atau menguji model, diubah menjadi skor, disimpan dalam log, lalu diakses oleh pihak lain. Pengendali harus mengetahui aliran itu agar dapat menjelaskan dasar hukum dan pertanggungjawaban yang melekat pada setiap tahap.

UU PDP mengenali sejumlah dasar pemrosesan, termasuk persetujuan yang sah, pemenuhan kontrak, kewajiban hukum, kepentingan vital, pelaksanaan tugas untuk kepentingan umum atau kewenangan, dan kepentingan yang sah dengan memperhatikan keseimbangan hak subjek data. Organisasi tidak seharusnya menganggap persetujuan sebagai dasar universal. Jika layanan inti hanya dapat diakses setelah seseorang menyetujui pemrosesan tambahan yang tidak diperlukan, persetujuan dapat kehilangan sifat bebas dan spesifik. Untuk pengembangan AI, organisasi perlu mengidentifikasi secara terpisah tujuan layanan, analitik, pencegahan penipuan, pelatihan model, personalisasi, serta penggunaan sekunder lain. Satu kalimat umum yang mencakup semuanya bukan pengganti analisis dasar pemrosesan.

Prinsip tujuan tertentu dan transparansi menuntut organisasi menyampaikan penggunaan data secara jelas. Dalam konteks AI, kata-kata seperti "meningkatkan layanan" terlalu luas untuk menjelaskan apakah data dipakai membuat profil, melatih model, atau dipindahkan ke penyedia eksternal. Pemberitahuan perlu menerangkan kategori data, alasan pengumpulan, bentuk keputusan yang dibantu AI, penerima data, masa retensi, konsekuensi bagi individu, serta cara mengajukan keberatan atau koreksi. Transparansi yang bermakna tidak mengharuskan organisasi membuka kode sumber atau rahasia dagang; tetapi pengguna berhak memperoleh penjelasan yang cukup untuk memahami penggunaan data dan dampak keputusan.

Subjek data memiliki hak yang berhubungan langsung dengan desain layanan, termasuk hak memperoleh informasi, akses, koreksi, pengakhiran pemrosesan atau penghapusan sesuai syarat hukum, penarikan persetujuan, keberatan atas keputusan yang hanya didasarkan pada pemrosesan otomatis yang berdampak signifikan, dan hak lain menurut UU PDP. Hak tersebut menantang asumsi bahwa model adalah kotak hitam yang tidak dapat dipengaruhi. Organisasi perlu menyediakan saluran permintaan, verifikasi identitas yang proporsional, batas waktu, dan proses eskalasi. Jika penghapusan data dari model terlatih

secara teknis sulit, organisasi harus menjelaskan batasnya dan merancang kebijakan pelatihan serta retensi sejak awal, bukan menjadikan kompleksitas model sebagai alasan untuk meniadakan hak.

UU PDP mengatur kewajiban pengendali dan prosesor. Pengendali menentukan tujuan dan kendali atas pemrosesan; prosesor memproses atas nama pengendali. Dalam AI modern, rantai peran sering rumit: penyedia cloud, penyedia model dasar, integrator, pengembang aplikasi, dan organisasi pengguna dapat mempunyai fungsi yang berbeda. Label dalam kontrak tidak otomatis menentukan peran sebenarnya. Setiap pihak harus memetakan siapa menentukan tujuan, siapa memilih data, siapa menggunakan kembali data, siapa menanggapi hak subjek, dan siapa mengelola insiden. Kontrak pemrosesan perlu menetapkan instruksi, subprosesor, lokasi penyimpanan, keamanan, audit, penghapusan, dan notifikasi insiden.

Undang-undang juga memberi perhatian pada penilaian dampak pelindungan data pribadi untuk pemrosesan berisiko tinggi, termasuk keputusan otomatis yang berdampak signifikan, pemrosesan data spesifik, pemantauan sistematis, dan penggunaan teknologi baru. Penilaian dampak bukan dokumen formal yang selesai sebelum peluncuran, melainkan alat untuk menemukan risiko, menguji alternatif, dan memutuskan apakah manfaat sistem dapat dicapai dengan cara yang kurang intrusif. Organisasi sebaiknya mengaitkan hasil penilaian tersebut dengan penilaian dampak AI, keselamatan, keamanan, dan hak asasi agar analisis tidak terpecah menjadi silo.

Transfer data lintas negara juga relevan karena layanan AI dapat memproses data melalui infrastruktur global. Organisasi wajib menilai ketentuan transfer menurut UU PDP, memastikan perlindungan yang memadai atau mekanisme yang diwajibkan, dan mengetahui lokasi pemrosesan aktual. Ketergantungan pada layanan internasional tidak menghapus kewajiban pengendali Indonesia untuk memahami tujuan, akses, penyimpanan, serta subprosesor. Data yang

dipindahkan ke pusat data regional dapat tetap diproses oleh tim dukungan atau layanan analitik di yurisdiksi lain.

Komdigi menerbitkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Pedoman ini memuat nilai inklusivitas, kemanusiaan, keamanan, transparansi, kredibilitas dan akuntabilitas, pelindungan data pribadi, pembangunan berkelanjutan, serta penghormatan terhadap kekayaan intelektual (Kementerian Komunikasi dan Informatika, 2023). Surat edaran tersebut menjadi rujukan etis dan administratif, sementara UU PDP merupakan undang-undang yang mengikat. Pada 2025, pemerintah juga membuka konsultasi publik atas buku putih peta jalan AI nasional dan konsep pedoman etika AI sebagai bahan kebijakan (Kementerian Komunikasi dan Digital, 2025). Organisasi perlu memeriksa status final setiap kebijakan sebelum menyebutnya sebagai kewajiban hukum yang telah berlaku.

4. Risiko privasi di sepanjang siklus hidup AI

Risiko AI mulai muncul pada tahap penentuan masalah. Organisasi bisa memilih pertanyaan yang keliru, misalnya menggunakan data perilaku konsumen untuk memprediksi "keandalan" calon pekerja tanpa bukti bahwa indikator tersebut berkaitan dengan kinerja. Tujuan yang kabur mendorong pengumpulan data luas dan penggunaan ulang tanpa batas. Tahap pertama yang bertanggung jawab adalah menguji kebutuhan: masalah apa yang ingin diselesaikan, apakah AI benar-benar diperlukan, siapa yang akan terpengaruh, dan apakah metode yang lebih sederhana akan memberi hasil yang memadai.

Pada tahap pengumpulan, data dapat diperoleh dari formulir, perangkat, sensor, kamera, transaksi, aktivitas media sosial, pihak ketiga, atau data publik. Ketersediaan teknis tidak berarti penggunaan otomatis patut. Data publik dapat dikumpulkan dalam konteks yang tidak mengantisipasi pemeringkatan atau pelatihan model komersial. Data yang diberikan untuk satu tujuan tidak

otomatis boleh dialihkan ke tujuan lain. Organisasi perlu menguji sumber, legalitas, kualitas, keterwakilan, ekspektasi individu, dan batas lisensi. Data anak, biometrik, kesehatan, serta keuangan membutuhkan kehati-hatian yang lebih tinggi.

Penggabungan data menciptakan risiko inferensi. Bahkan saat nama dan nomor identitas dihapus, kombinasi lokasi, waktu, pekerjaan, kebiasaan belanja, dan relasi sosial dapat mengidentifikasi seseorang kembali. Model dapat pula mengungkap atribut sensitif yang tidak pernah diserahkan langsung. Contohnya, pola pembelian dan pencarian dapat memberi petunjuk tentang kondisi kesehatan; data lokasi dapat mengungkap tempat ibadah atau keikutsertaan dalam kegiatan politik. Risiko ini berarti minimisasi perlu meliputi bukan hanya jumlah kolom, tetapi juga kedalaman, granuralitas, masa cakupan, hubungan antar-sumber, dan kemampuan model untuk menebak atribut.

Dalam pelatihan, model bisa menghafal fragmen data, mereproduksi teks atau gambar, atau menyimpan pola yang memungkinkan serangan inferensi keanggotaan dan ekstraksi data. Liu et al. (2021) meninjau interaksi privasi dan pembelajaran mesin, termasuk serangan yang mengeksploitasi informasi yang terpelajari. Menghapus data dari tabel sumber tidak selalu menghapus pengaruhnya dari parameter model. Karena itu, tim harus mengevaluasi risiko kebocoran dari model, menerapkan kontrol akses dan pemisahan lingkungan, membatasi logging, serta menguji keluaran dengan skenario adversarial.

Pada tahap penggunaan, skor prediktif dapat berubah menjadi perlakuan nyata. Risiko muncul ketika sistem menilai individu berdasarkan proksi yang bias, memberi harga berbeda, menyaring pelamar, atau mengurutkan warga berdasarkan kemungkinan melakukan pelanggaran. Sistem dapat secara tidak langsung mengidentifikasi kelompok berdasarkan atribut yang dilarang, meski atribut itu tidak digunakan secara eksplisit. Data lama atau tidak akurat juga dapat menciptakan kesalahan yang berulang. Penggunaan AI sebagai

dukungan keputusan harus disertai pemantauan atas hasil dan kemampuan operator untuk menantang keluaran model.

Layanan generatif menambah bentuk risiko baru. Pengguna mungkin memasukkan kontrak, catatan medis, kode sumber, atau data pelanggan ke dalam prompt. Jika batas retensi, penggunaan data, dan akses vendor tidak jelas, masukan dapat tersimpan atau digunakan untuk tujuan lain. Keluaran sistem pun dapat membeberkan informasi yang pernah masuk pada pelatihan atau memuat detail personal yang keliru. Organisasi perlu mengatur penggunaan AI generatif melalui klasifikasi data, daftar layanan yang disetujui, pengaturan retensi, pemisahan akun, serta panduan bagi pegawai mengenai apa yang tidak boleh ditempelkan ke sistem.

Pada tahap penyimpanan dan penghapusan, risiko berupa akses berlebihan, kebocoran, salinan cadangan yang tidak terkelola, dan jejak data pada log. Retensi tanpa batas meningkatkan dampak insiden dan memperbesar peluang data dipakai kembali di luar konteks asal. Organisasi perlu mendefinisikan jadwal retensi per tujuan dan tipe data, termasuk data turunan dan dataset pelatihan. Bila data sudah tidak dibutuhkan, sistem harus menghapusnya atau membuatnya tidak dapat diidentifikasi sesuai ketentuan, serta menyimpan bukti penghapusan yang dapat diaudit.

Siklus hidup tidak berakhir ketika model diluncurkan. Perubahan populasi, pola perilaku, sumber data, konfigurasi vendor, atau tujuan bisnis dapat membuat sistem melenceng dari asumsi awal. Model yang dulu hanya memberi rekomendasi dapat kemudian dipakai untuk keputusan otomatis; data baru dapat membawa informasi sensitif; model vendor bisa diperbarui tanpa pemberitahuan yang memadai. Pemantauan berkala, pencatatan versi, pembatasan perubahan, dan prosedur penghentian merupakan unsur perlindungan, bukan beban tambahan setelah inovasi selesai.

5. Persetujuan, pemberitahuan, dan kendali nyata

Persetujuan sering diperlakukan sebagai tombol "Saya setuju", seolah-olah setiap risiko telah dipahami dan diterima. Dalam praktik, kebijakan privasi panjang, pilihan yang tidak seimbang, dan pola desain manipulatif membuat persetujuan formal tidak selalu mencerminkan pilihan bebas. Untuk pemrosesan berisiko rendah, persetujuan dapat menjadi dasar yang tepat bila informasi jelas dan pilihan mudah ditolak. Namun, persetujuan bukan alasan untuk mengumpulkan semua data yang mungkin berguna di masa depan. Pengendali harus menjelaskan kebutuhan dan dasar pemrosesan secara spesifik, serta menghormati penarikan persetujuan sesuai hukum.

Pemberitahuan yang baik memakai lapisan informasi. Ringkasan awal menyebut tujuan utama, kategori data, pihak yang menerima, keputusan yang mungkin dibantu AI, dan tautan ke penjelasan rinci. Pengguna dapat membaca informasi lebih lengkap tanpa harus menelusuri dokumen hukum yang padat. Untuk sistem yang memengaruhi hak atau akses penting, pemberitahuan perlu menjelaskan jenis faktor yang dipertimbangkan, kemungkinan konsekuensi, jalur pengaduan, dan cara meminta peninjauan manusia. Organisasi tidak harus mengungkapkan rahasia dagang, tetapi ketidakjelasan tidak boleh menjadi strategi perlindungan bisnis.

Kendali nyata juga berarti menyediakan pengaturan yang dapat digunakan. Pengguna perlu dapat mengubah preferensi personalisasi, memperbaiki data, menolak pemrosesan opsional, dan memahami konsekuensi pilihan mereka. Antarmuka tidak boleh membuat tombol menolak lebih sulit ditemukan daripada tombol menerima. Untuk kelompok dengan literasi digital terbatas, dukungan melalui petugas, bahasa sederhana, dan kanal non-digital tetap penting. Kepercayaan tumbuh ketika hak dapat dijalankan tanpa biaya dan hambatan yang tidak masuk akal.

6. Keputusan otomatis, penjelasan, dan pengawasan manusia

Keputusan otomatis dapat meningkatkan kecepatan dan konsistensi, tetapi juga mengalihkan kekuasaan ke sistem yang sulit dipahami. UU PDP mengakui hak untuk mengajukan keberatan terhadap keputusan yang hanya didasarkan pada pemrosesan otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau dampak signifikan. Dalam penerapan, organisasi harus lebih dulu mengidentifikasi keputusan mana yang termasuk berdampak besar, bukan menunggu keluhan. Contohnya dapat mencakup keputusan tentang kredit, pekerjaan, layanan esensial, pendidikan, asuransi, dan akses bantuan.

Peninjauan manusia harus bersifat bermakna. Menambahkan tombol persetujuan bagi operator yang tidak memahami sistem atau tidak berwenang mengubah hasil hanya menghasilkan pengawasan semu. Petugas perlu memiliki informasi yang relevan, pelatihan, waktu, akses kepada konteks tambahan, dan kewenangan untuk menolak rekomendasi. Catatan keputusan harus menunjukkan apa yang dipertimbangkan manusia, bukan hanya bahwa seseorang "mengeklik setuju". Organisasi perlu menguji apakah operator terlalu bergantung pada skor algoritmik atau, sebaliknya, mengabaikannya dengan cara yang tidak konsisten.

Penjelasan tidak harus berupa paparan matematis yang sulit dipahami. Bagi orang yang terdampak, penjelasan perlu menjawab: data apa yang digunakan, faktor utama apa yang memengaruhi hasil, apa yang bisa diperbaiki, bagaimana meminta koreksi atau peninjauan, dan apa tenggat responsnya. Penjelasan teknis bagi auditor dapat lebih rinci, mencakup validasi, batas model, metrik kesalahan per kelompok, versi data dan model, serta hasil pengujian. Tingkat penjelasan disesuaikan dengan audiens, tetapi semuanya harus konsisten dengan sistem nyata.

7. Privacy by design sebagai strategi rekayasa dan manajemen

Privacy by design berarti mempertimbangkan perlindungan data sejak masalah dan arsitektur sistem ditentukan, bukan menambahkannya setelah produk selesai. Prinsip ini mencakup pencegahan, perlindungan sebagai pengaturan bawaan, integrasi ke desain, keamanan sepanjang siklus, transparansi, dan penghormatan terhadap kepentingan individu. Meurisch dan Mühlhäuser (2021/2022) menunjukkan bahwa perlindungan layanan AI perlu menggabungkan pendekatan manajemen, sistem, dan tingkat AI. Tidak ada satu teknik yang menyelesaikan seluruh masalah.

Langkah awalnya adalah inventaris data dan diagram aliran. Organisasi perlu mencatat jenis data, sumber, tujuan, pemilik, sistem yang memproses, lokasi, penerima, masa simpan, serta model yang menggunakannya. Peta ini harus memuat aliran yang tidak terlihat di antarmuka, misalnya telemetri, log dukungan, pemantauan kualitas, dan subprosesor cloud. Tanpa peta yang andal, pengendali tidak dapat memenuhi hak individu atau menjawab di mana data tersimpan ketika terjadi insiden.

Selanjutnya, tetapkan minimisasi sebagai syarat produk. Tim menentukan fitur minimum untuk memenuhi tujuan, mengurangi presisi lokasi atau durasi data bila ketepatan lebih rendah sudah cukup, dan menghindari atribut sensitif kecuali benar-benar diperlukan serta memiliki dasar yang sah. Dataset sintetis atau data agregat dapat membantu eksperimen awal, meskipun kualitas dan risiko reidentifikasinya harus diuji. Data sintetis bukan jaminan privasi: model pembangkitnya mungkin menghafal data asli atau sampel sintetis dapat terlalu mirip dengan individu nyata.

Privacy engineering memasukkan kontrol konkret ke dalam arsitektur. Ini termasuk pemisahan identitas dari data analitik, kontrol akses berdasarkan peran, enkripsi saat transit dan tersimpan, pencatatan akses, manajemen kunci, lingkungan pengembangan terpisah, masking, pembatasan ekspor, dan

pengujian keamanan. Teknik harus disesuaikan dengan ancaman. Enkripsi dapat mengurangi risiko akses tidak sah, tetapi tidak mencegah pengguna sah yang memiliki hak terlalu luas. Pseudonimisasi mengurangi keterkaitan langsung, tetapi bukan anonimisasi jika kunci atau data penghubung masih tersedia.

Organisasi juga perlu membangun privacy gate di alur pengembangan model. Dataset baru tidak langsung masuk ke pelatihan sebelum pemeriksaan sumber, hak pemanfaatan, kualitas, representasi, dan risiko. Setiap eksperimen mencatat versi data, konfigurasi, tujuan, akses, hasil evaluasi, serta keputusan persetujuan. Perubahan tujuan atau penggunaan dataset untuk domain risiko lebih tinggi memerlukan penilaian ulang. Dengan cara ini, kepatuhan menjadi langkah kerja yang terukur, bukan dokumen yang diperiksa hanya menjelang audit.

8. Teknologi peningkat privasi dan batasnya

Teknologi peningkat privasi (privacy-enhancing technologies/PETs) menawarkan cara untuk memperoleh manfaat analitik sambil mengurangi paparan data. Namun, teknologi ini bukan pengganti dasar hukum, tata kelola, dan akuntabilitas. Pilihannya bergantung pada jenis ancaman, jumlah pihak, kebutuhan akurasi, skala, biaya komputasi, dan kemampuan organisasi. Evaluasi harus menyatakan apa yang dilindungi, dari siapa, dan dalam kondisi apa.

Differential privacy menambahkan gangguan matematis yang terukur pada hasil agar kontribusi satu individu tidak mudah disimpulkan. Teknik ini berguna ketika organisasi merilis statistik atau melatih model dari banyak orang, tetapi membutuhkan pengelolaan anggaran privasi. Jika terlalu banyak kueri dilakukan atau parameter dipilih tanpa pemahaman, perlindungan dapat melemah atau hasil menjadi tidak berguna. Diferensial privasi juga tidak

memperbaiki data yang bias, tujuan yang tidak sah, atau keputusan yang diskriminatif.

Federated learning memungkinkan model dilatih di perangkat atau institusi lokal tanpa mengumpulkan seluruh data mentah ke satu pusat. Meski demikian, pembaruan gradien atau parameter masih dapat membawa informasi, sehingga agregasi aman, differential privacy, dan perlindungan terhadap serangan perlu dipertimbangkan. Federated learning juga memiliki tantangan heterogenitas perangkat, kualitas jaringan, dan tata kelola peserta. Menyebut data "tidak pernah meninggalkan perangkat" tidak cukup bila metadata atau pembaruan model masih dapat mengungkap pola pengguna.

Secure multiparty computation, homomorphic encryption, dan trusted execution environments memungkinkan bentuk komputasi dilakukan tanpa membuka data mentah kepada semua pihak. Teknik ini dapat memfasilitasi kolaborasi antarorganisasi untuk deteksi penipuan atau riset kesehatan. Biaya dan kompleksitasnya harus dibandingkan dengan manfaatnya; pada banyak kasus, pengurangan data, pemisahan peran, atau agregasi yang baik mungkin sudah memadai. Pilihan tepat dimulai dari model ancaman dan kebutuhan layanan, bukan dari tren teknologi.

Anonimisasi juga sering disalahpahami. Menghapus nama atau nomor telepon menghasilkan pseudonimisasi bila hubungan kembali masih mungkin dilakukan. Anonimisasi adalah hasil yang menuntut penilaian terhadap kemungkinan identifikasi ulang berdasarkan data tambahan dan kemampuan pihak yang mungkin mengaksesnya. Data berjumlah besar dan bergranular tinggi lebih mudah dikaitkan kembali. Karena itu, organisasi perlu menilai risiko reidentifikasi secara berkala, terutama ketika sumber data baru tersedia atau informasi yang sebelumnya langka menjadi umum.

9. Keadilan, bias, dan pelindungan kelompok rentan

Privasi dan keadilan saling terkait. Pengumpulan data berlebihan meningkatkan pengawasan, tetapi pengurangan data secara sederhana kadang membuat organisasi kehilangan kemampuan untuk mengukur diskriminasi. Misalnya, jika atribut demografis tidak pernah dikumpulkan atau dianalisis secara aman, organisasi dapat kesulitan mengetahui bahwa model menolak kelompok tertentu dengan frekuensi yang tidak proporsional. Solusinya bukan mengumpulkan data sensitif tanpa batas, melainkan menetapkan dasar, pembatasan akses, tujuan audit yang sempit, teknik agregasi, dan penghapusan setelah evaluasi selesai.

Bias dapat masuk melalui data historis yang mencerminkan ketimpangan, label yang tidak akurat, fitur proksi, desain tujuan, atau cara hasil dipakai. Model yang dilatih pada keputusan masa lalu dapat menyalin pola diskriminatif dan memberi kesan objektif karena hasilnya berupa angka. Pengujian harus meliputi metrik yang relevan bagi tujuan, analisis error per kelompok, penilaian dampak pada individu, serta tinjauan kualitatif atas konteks sosial. Angka keadilan tunggal tidak cocok untuk semua situasi; pilihan metrik harus dijelaskan dan konsekuensi trade-off didokumentasikan.

Anak, orang lanjut usia, penyandang disabilitas, masyarakat yang kurang terlayani, dan kelompok dengan daya tawar rendah memerlukan perlindungan tambahan. Mereka mungkin tidak memahami pengumpulan data, sulit menolak layanan esensial, atau menghadapi kerugian yang tidak dapat dipulihkan. Antarmuka aksesibel, bahasa lokal, pendampingan, pengujian dengan komunitas terdampak, dan larangan praktik eksploitatif harus menjadi bagian dari desain. Penilaian risiko sebaiknya menanyakan siapa yang tidak hadir dalam tim desain dan siapa yang akan menanggung kesalahan sistem.

10. Keamanan siber dan respons insiden

Kebocoran data bukan hanya persoalan kerahasiaan; ia dapat menyebabkan penipuan, pemerasan, pencurian identitas, diskriminasi, dan rasa tidak aman yang berkepanjangan. Sistem AI membuka permukaan serangan baru: manipulasi data pelatihan, pencurian model, prompt injection, ekstraksi informasi melalui keluaran, penyalahgunaan akun layanan, dan eksploitasi antarmuka pihak ketiga. Tim keamanan perlu memahami ancaman terhadap model dan data secara bersamaan, serta memperlakukan dataset pelatihan dan log sebagai aset sensitif.

Program keamanan meliputi autentikasi kuat, prinsip hak minimum, segmentasi jaringan, pengelolaan rahasia, pencadangan, pemantauan, patching, uji penetrasi, dan rencana respons insiden. Untuk sistem AI, kontrol tambahan mencakup validasi input, rate limiting, pengamanan endpoint, pengujian prompt, deteksi keluaran yang membocorkan data, pembatasan penggunaan eksternal, dan evaluasi ketahanan model. Kontrol teknis harus disertai pemilik tanggung jawab yang jelas dan latihan insiden berkala.

Ketika terjadi kegagalan, organisasi perlu mengetahui siapa yang memutuskan pemberitahuan, bagaimana dampak dinilai, kapan regulator dan subjek data diberi tahu, serta bentuk dukungan yang disediakan. UU PDP menetapkan kewajiban pemberitahuan tertulis atas kegagalan pelindungan data pribadi dalam jangka waktu tertentu, termasuk kepada subjek data dan lembaga yang berwenang sesuai ketentuan. Organisasi perlu memiliki prosedur yang dapat dijalankan di luar jam kerja, daftar kontak, dan format komunikasi yang menjelaskan fakta, risiko, langkah mitigasi, serta saluran bantuan tanpa mengecilkan dampak.

11. Akuntabilitas organisasi dan tata kelola vendor

Akuntabilitas berarti organisasi mampu menunjukkan, bukan hanya menyatakan, bahwa pemrosesan telah dipertimbangkan dan dikendalikan.

Dewan atau pimpinan perlu menyetujui toleransi risiko, menetapkan sponsor, dan menerima pelaporan berkala. Unit legal, privasi, keamanan, data, produk, SDM, pengadaan, dan layanan pelanggan memiliki peran berbeda. Menyerahkan seluruh tanggung jawab kepada petugas perlindungan data atau tim TI tidak memadai bila keputusan strategis tetap dibuat tanpa analisis hak dan risiko.

Model tata kelola yang praktis menggabungkan tiga lapis. Lapis pertama adalah pemilik bisnis dan tim produk yang merancang tujuan serta menerapkan kontrol sehari-hari. Lapis kedua adalah fungsi privasi, hukum, keamanan, dan manajemen risiko yang menetapkan kebijakan, menantang asumsi, dan memberi panduan. Lapis ketiga adalah audit internal atau penilai independen yang menguji desain dan bukti pelaksanaan. Garis tanggung jawab ini membantu menghindari keadaan ketika pengembang menilai sendiri kualitas dan kepatuhan sistem yang mereka buat.

Vendor AI perlu dipilih berdasarkan bukti dan kesesuaian, bukan hanya harga atau demo yang mengesankan. Uji tuntas mencakup lokasi dan arus data, subprosesor, penggunaan data untuk pelatihan, kontrol retensi, penghapusan, insiden, audit, hak penggunaan keluaran, dukungan terhadap permintaan subjek data, dan mekanisme perubahan model. Organisasi harus menguji layanan dalam konfigurasi aktual, sebab janji di materi pemasaran tidak selalu cocok dengan pengaturan akun atau kontrak. Bila penyedia tidak dapat memberikan informasi minimum, risiko residual harus dicatat dan keputusan penggunaan dibatasi.

Klausul kontrak hendaknya melarang penggunaan data pelanggan untuk tujuan yang tidak diinstruksikan, mewajibkan pengamanan dan pemberitahuan insiden, mengatur subprosesor, mendukung hak subjek, serta mengatur penghapusan dan pengembalian data. Pihak yang menggunakan model eksternal tetap bertanggung jawab atas keputusan apakah layanan tersebut

sesuai. Ketika vendor memperbarui model, mengubah lokasi pemrosesan, atau menambah fitur, perubahan tersebut harus melewati proses perubahan terkendali, termasuk penilaian dampak bila risiko berubah.

12. Penerapan pada sektor-sektor utama Indonesia

Di sektor keuangan, pemodelan risiko dapat memperluas akses kredit bagi orang yang tidak memiliki riwayat formal. Data transaksi alternatif berpotensi membantu usaha mikro dan pekerja informal, tetapi dapat pula menghasilkan keputusan opak yang sulit dikoreksi. Bank, fintech, dan penyedia skor perlu menjelaskan kategori data, membatasi penggunaan data yang tidak relevan, mengecek kualitas serta representasi, dan menyediakan proses banding yang melibatkan manusia. Data keuangan pribadi termasuk data spesifik menurut UU PDP, sehingga pengelolaannya membutuhkan pengamanan dan dasar pemrosesan yang jelas.

Dalam kesehatan, AI dapat membantu membaca citra, memprioritaskan kasus, dan mengidentifikasi risiko populasi. Data kesehatan sangat sensitif dan sering melibatkan informasi keluarga, genetika, serta kondisi psikologis. Persetujuan pasien perlu dibedakan menurut layanan klinis, riset, dan pengembangan produk. Penggunaan ulang rekam medis memerlukan dasar, pembatasan, dan pengawasan etik. Sistem harus divalidasi pada populasi Indonesia, termasuk variasi bahasa, usia, gender, akses fasilitas, dan prevalensi penyakit. Kesalahan prediksi bukan sekadar kekurangan statistik; ia dapat menunda perawatan atau meningkatkan stigma.

Dalam ketenagakerjaan, AI dipakai untuk mengurutkan CV, merekam wawancara, menilai produktivitas, dan memprediksi pengunduran diri. Data wajah, suara, gerakan, dan pola ketikan dapat mengungkap lebih banyak daripada yang diperlukan untuk pekerjaan. Pekerja berada dalam relasi kuasa yang tidak seimbang sehingga pilihan untuk menolak pemrosesan mungkin terbatas. Pemberi kerja perlu membatasi data pada kebutuhan yang relevan,

menguji apakah alat benar-benar meningkatkan keputusan, memberi informasi kepada kandidat, serta memastikan manusia meninjau hasil yang berdampak terhadap kesempatan kerja. Penilaian kepribadian dari ekspresi atau suara sebaiknya tidak diadopsi hanya karena vendor mengklaim akurasi tinggi.

Pemerintah menggunakan data untuk administrasi, bantuan sosial, identitas, pendidikan, kesehatan, dan penegakan hukum. Penggunaan AI dapat membantu alokasi sumber daya tetapi juga mengonsolidasikan informasi yang sangat luas dan menciptakan konsekuensi terhadap hak warga. Sistem pemerintah harus memiliki dasar kewenangan yang jelas, tujuan terbatas, audit independen, standar akses, mekanisme koreksi, dan pencatatan keputusan. Jika suatu keputusan berdampak pada hak, warga harus dapat memperoleh penjelasan dan meminta peninjauan. Pengadaan sistem harus transparan dalam spesifikasi risiko, bukan hanya harga, kapasitas, dan jadwal implementasi.

Platform digital menggunakan rekomendasi, moderasi konten, deteksi penipuan, iklan bertarget, dan personalisasi. Penggabungan aktivitas lintas layanan menciptakan profil rinci mengenai individu. Platform perlu menyediakan pengaturan yang mudah dipahami, mengurangi penggunaan data sensitif untuk iklan, memberi penjelasan atas moderasi yang merugikan, dan menilai dampak sistem rekomendasi terhadap anak serta kelompok rentan. Tanggung jawab tidak berhenti pada penyedia model jika perusahaan penerapannya menentukan tujuan dan mengendalikan pengalaman pengguna.

Di pendidikan, analitik pembelajaran dapat mendeteksi siswa yang memerlukan dukungan. Namun, skor risiko dapat menjadi label permanen yang memengaruhi ekspektasi guru dan siswa. Data anak harus dilindungi dengan pembatasan akses dan retensi, serta hasil sistem harus dipakai untuk memberi dukungan, bukan menghukum. Sekolah perlu menjelaskan kepada orang tua dan siswa data apa yang dipakai, siapa yang dapat melihatnya, serta bagaimana

meminta koreksi. Keputusan penting tetap membutuhkan penilaian profesional yang mempertimbangkan konteks keluarga, bahasa, disabilitas, dan akses internet.

Bagi UMKM, kepatuhan tidak harus berarti membangun birokrasi mahal. Langkah dasar meliputi daftar data pelanggan dan pegawai, pemisahan data yang tidak relevan, penggunaan perangkat lunak terpercaya, autentikasi multifaktor, pembatasan staf yang memiliki akses, pengaturan cadangan dan penghapusan, serta pengecekan syarat layanan aplikasi AI. UMKM sebaiknya tidak mengunggah daftar pelanggan, dokumen identitas, informasi keuangan, atau rahasia dagang ke layanan publik tanpa memastikan pengaturan penggunaan data. Asosiasi bisnis dan pemerintah dapat membantu dengan panduan sederhana, kontrak contoh, layanan konsultasi bersama, dan pelatihan keamanan.

13. Tantangan khusus AI generatif

Model generatif mengubah batas antara pengguna dan pembuat data. Pengguna memberikan instruksi, dokumen, gambar, suara, atau kode; model menyusun keluaran berdasarkan pola yang dipelajari; layanan menyimpan log untuk keamanan atau evaluasi. Risiko muncul baik pada masukan maupun keluaran. Prompt bisa membawa data rahasia, sedangkan respons dapat mencampur informasi publik dan personal tanpa konteks yang benar. Karena keluaran terdengar yakin, pegawai dapat menyebarkannya tanpa menyadari bahwa informasi sensitif telah dimunculkan.

Organisasi perlu membuat kebijakan penggunaan yang membagi data ke dalam kelas: publik, internal, rahasia, dan sangat sensitif. Setiap kelas memiliki aturan alat yang boleh dipakai. Untuk layanan yang disetujui, konfigurasi retensi, pelatihan, wilayah penyimpanan, dan akses harus diperiksa. Pengguna diberi tahu bahwa keluaran AI perlu diverifikasi dan bahwa model dapat menghasilkan informasi salah atau mengungkapkan materi yang seharusnya

tidak disebarkan. Data pelanggan dan pegawai tidak dimasukkan ke model konsumen kecuali dasar dan perlindungannya telah dievaluasi.

Penggunaan model pihak ketiga untuk pencarian internal atau asisten perusahaan memerlukan retrieval-augmented generation (RAG) yang aman. RAG menghubungkan model dengan dokumen perusahaan, tetapi kontrol akses harus diterapkan pada dokumen sumber, bukan hanya antarmuka chatbot. Jika pegawai biasa tidak berhak membaca dokumen HR, model tidak boleh menjawab pertanyaan yang mengungkap isinya. Log prompt dan respons perlu memiliki retensi terbatas serta akses yang ketat. Perlu pula pengujian terhadap prompt injection yang berusaha membuat model mengambil atau mengungkapkan dokumen di luar kewenangan.

14. Mengukur kepercayaan dan kinerja pelindungan

Kepercayaan perlu diukur dengan kombinasi indikator proses, hasil, dan pengalaman. Indikator proses meliputi persentase proyek AI yang memiliki inventaris data, penilaian dampak, dokumentasi vendor, pengujian privasi, dan pemilik risiko. Indikator hasil dapat mencakup jumlah insiden, waktu respons permintaan hak, frekuensi penghapusan sesuai jadwal, tingkat temuan audit yang ditutup, serta error keputusan per kelompok. Indikator pengalaman menilai apakah orang memahami tujuan pengumpulan, mudah menemukan pengaturan, memperoleh jawaban atas keluhan, dan percaya bahwa koreksi mereka akan ditindaklanjuti.

Organisasi harus berhati-hati menafsirkan survei kepercayaan. Pengguna mungkin menyatakan puas karena sistem mudah digunakan, tetapi tidak memahami penggunaan data; atau sebaliknya, mereka dapat bersikap skeptis karena pengalaman buruk sebelumnya meskipun kontrol teknis telah membaik. Karena itu, survei harus dipadukan dengan wawancara, uji kegunaan pemberitahuan, analisis keluhan, pengujian perilaku sistem, dan audit

independen. Tujuan bukan menghasilkan satu angka kepercayaan yang mengesankan, melainkan menemukan bagian tata kelola yang belum bekerja.

Tolok ukur harus dikaitkan dengan tingkat risiko. Sistem rekomendasi musik tidak memerlukan proses yang sama dengan penilaian bantuan sosial. Namun, semua sistem perlu memiliki pemilik, tujuan, dasar pemrosesan, kontrol keamanan, dan jadwal peninjauan. Untuk penggunaan berdampak tinggi, organisasi memerlukan dokumentasi yang lebih rinci, pengujian independen, mekanisme banding, konsultasi kelompok terdampak, dan kesiapan menghentikan sistem. NIST AI RMF 1.0 menyediakan kerangka sukarela untuk memasukkan kepercayaan dan pengelolaan risiko ke dalam desain, pengembangan, penggunaan, dan evaluasi AI melalui fungsi Govern, Map, Measure, dan Manage (National Institute of Standards and Technology, 2023). Kerangka ini dapat dipakai sebagai referensi proses, bukan pengganti hukum Indonesia.

15. Rancangan model tata kelola terpadu

Model tata kelola terpadu dimulai dengan mandat pimpinan. Pimpinan menetapkan prinsip bahwa data hanya dikumpulkan untuk tujuan yang dapat dijelaskan dan AI tidak boleh diterapkan apabila risiko hak tidak dapat dikurangi secara memadai. Mandat itu diterjemahkan menjadi kebijakan, anggaran, toleransi risiko, dan mekanisme pelaporan. Tanpa dukungan pimpinan, tim privasi dan keamanan sering hanya diminta memeriksa setelah keputusan investasi dibuat.

Tahap kedua adalah inventaris dan klasifikasi. Setiap use case dicatat dengan tujuan, populasi terdampak, kategori data, sumber, penerima, dasar pemrosesan, model, dampak keputusan, vendor, lokasi, dan jadwal retensi. Klasifikasi risiko mengarahkan kedalaman pemeriksaan. Penggunaan yang menyangkut anak, kesehatan, biometrik, keuangan, pekerjaan, layanan publik, atau keputusan signifikan membutuhkan pemeriksaan lebih ketat.

Tahap ketiga adalah analisis kelayakan dan alternatif. Tim menguji apakah AI benar-benar dibutuhkan, apakah sistem sederhana bisa menyelesaikan masalah, dan apakah data dapat diminimalkan atau diganti dengan agregat. Penilaian dampak menggali skenario penyalahgunaan, kesalahan, kebocoran, bias, perubahan tujuan, dan kegagalan vendor. Kelompok terdampak diminta memberi masukan, terutama bila keputusan dapat memengaruhi akses terhadap hak atau layanan dasar.

Tahap keempat adalah desain kontrol. Organisasi menetapkan dasar hukum, pemberitahuan, pengaturan pengguna, jadwal retensi, kontrol akses, keamanan, batas model, pengawasan manusia, mekanisme koreksi, dan proses banding. Kontrak vendor menyelaraskan kewajiban eksternal dengan janji kepada pengguna. Pengujian dilakukan terhadap akurasi, privasi, keamanan, ketahanan, dan dampak distribusional sebelum peluncuran.

Tahap kelima adalah persetujuan peluncuran dan pemantauan. Pemilik risiko memutuskan apakah risiko residual dapat diterima dan siapa yang berwenang menghentikan layanan. Setelah berjalan, sistem diawasi atas perubahan data, performa, komplain, akses tidak sah, dan dampak yang tidak direncanakan. Model, tujuan, dan vendor yang berubah memicu tinjauan ulang. Catatan audit membantu organisasi menjelaskan apa yang dilakukan dan mengapa.

Tahap terakhir adalah pemulihan dan pembelajaran. Jika sistem merugikan seseorang, tersedia jalur koreksi, banding, kompensasi atau pemulihan lain sesuai konteks hukum. Insiden dan keluhan dianalisis untuk mencegah pengulangan, bukan sekadar menghindari sanksi. Temuan dibagikan secara proporsional kepada pimpinan, regulator, dan masyarakat yang terdampak. Sistem dapat ditangguhkan atau dihentikan bila manfaatnya tidak lagi sebanding dengan risikonya.

16. Agenda implementasi bagi Indonesia

Pertama, organisasi harus memulai dengan peta penggunaan AI dan data yang nyata. Banyak institusi mengetahui proyek resmi, tetapi tidak mengetahui penggunaan alat generatif oleh pegawai, integrasi vendor, atau pemrosesan yang berjalan pada aplikasi tambahan. Pemetaan yang jujur membantu menetapkan prioritas. Untuk setiap penggunaan, organisasi menuliskan tujuan, pemilik, jenis data, penerima, risiko, serta keputusan yang dipengaruhi. Pemetaan ini diperbarui ketika sistem dan kontrak berubah.

Kedua, peningkatan kapasitas harus berlangsung lintas disiplin. Insinyur perlu memahami hak subjek data dan risiko reidentifikasi; pimpinan bisnis perlu memahami konsekuensi keputusan otomatis; petugas privasi perlu memahami arsitektur model; pengadaan perlu mampu menilai klausul vendor; dan layanan pelanggan perlu menerima serta mengeskalasi permintaan. Perguruan tinggi dapat memasukkan etika data, keamanan, dan hukum ke kurikulum AI, dengan studi kasus lokal dan latihan penilaian dampak.

Ketiga, dibutuhkan panduan sektoral yang jelas dan dapat dipraktikkan. Prinsip umum perlu diterjemahkan menjadi standar bagi layanan keuangan, kesehatan, pendidikan, ketenagakerjaan, dan administrasi publik. Panduan sebaiknya memuat contoh dasar pemrosesan, format penilaian dampak, kewajiban dokumentasi vendor, cara menjalankan hak, dan pola pelaporan insiden. Panduan teknis yang terbuka akan membantu inovator kecil yang tidak memiliki tim legal besar.

Keempat, koordinasi antarotoritas dan mekanisme pengawasan perlu dibangun dengan kompetensi teknis, independensi, dan transparansi. AI menyentuh perlindungan data, persaingan, konsumen, keamanan siber, ketenagakerjaan, kesehatan, pendidikan, dan hak asasi. Pengawasan yang terfragmentasi dapat menciptakan celah atau kewajiban yang saling bertentangan. Kerja sama harus menghormati mandat tiap lembaga, dengan

saluran rujukan kasus, pertukaran keahlian, dan kejelasan siapa yang menangani pengaduan.

Kelima, kebijakan publik harus menyediakan ruang inovasi yang bertanggung jawab. Sandbox dapat digunakan untuk menguji teknologi pada ruang lingkup terbatas dengan peserta yang diberi informasi, kontrol pengamanan, indikator keberhasilan, batas waktu, dan rencana penghentian. Sandbox bukan pengecualian permanen dari hukum. Tujuannya adalah pembelajaran dan validasi risiko, serta publikasi hasil agregat yang tidak membocorkan data peserta.

Keenam, literasi masyarakat tidak boleh dibebankan sebagai satu-satunya solusi. Pengguna perlu memahami risiko, tetapi tanggung jawab utama tetap berada pada organisasi yang menentukan tujuan dan mengendalikan sistem. Edukasi publik harus membahas cara mengenali layanan AI, memeriksa pengaturan privasi, mengenali penipuan, dan mengajukan pengaduan, tanpa menormalisasi pengumpulan berlebihan atau menyalahkan korban kebocoran.

17. Prinsip keputusan bagi pemimpin

Sebelum menyetujui investasi AI, pimpinan dapat mengajukan sejumlah pertanyaan: Masalah apa yang hendak diselesaikan? Mengapa AI diperlukan? Apakah data yang dipakai relevan dan diperoleh secara sah? Siapa yang paling mungkin dirugikan oleh kesalahan? Dapatkah orang memahami dan menggugat hasil? Apakah ada pilihan yang lebih sederhana dan kurang intrusif? Siapa bertanggung jawab ketika vendor atau model berubah? Bagaimana keputusan akan dihentikan jika dampak buruk melampaui manfaat?

Pertanyaan tersebut bukan hambatan inovasi; ia membantu memastikan bahwa inovasi memecahkan masalah yang tepat. Organisasi yang menetapkan tujuan secara jelas dapat menghindari pengumpulan data untuk berjaga-jaga, memperkecil biaya penyimpanan, mengurangi risiko kebocoran, dan lebih mudah menguji keberhasilan. Tata kelola yang terintegrasi juga mempercepat

pengadaan karena kriteria vendor dan perlindungan sudah disiapkan, bukan dibuat setelah negosiasi selesai.

Pemimpin perlu menerima bahwa tidak semua risiko dapat dihilangkan. Tugas tata kelola adalah mengidentifikasi risiko, memilih mitigasi, menjelaskan risiko residual, dan memutuskan apakah penggunaan layak diteruskan. Risiko yang menyangkut kerugian berat atau pelanggaran hak mungkin tidak dapat diterima meskipun manfaat bisnis tinggi. Keputusan seperti ini membutuhkan bukti dan dokumentasi, serta tidak boleh diserahkan secara otomatis kepada tim teknis atau vendor.

18. Kesimpulan

Perlindungan data pribadi adalah fondasi kepercayaan terhadap AI karena AI memerlukan data dan dapat mengubahnya menjadi prediksi, profil, rekomendasi, serta keputusan yang memengaruhi kehidupan. Tanpa batas tujuan, minimisasi, transparansi, keamanan, hak koreksi, dan akuntabilitas, kecanggihan model dapat memperbesar ketimpangan informasi dan kekuasaan. Pengguna mungkin menerima manfaat dalam jangka pendek, tetapi sulit mempercayai sistem yang tidak menjelaskan bagaimana data dipakai atau bagaimana kesalahan dapat diperbaiki.

UU PDP memberikan dasar penting bagi Indonesia melalui hak subjek data dan kewajiban pengendali serta prosesor. Surat Edaran Etika AI 2023 menegaskan nilai keamanan, transparansi, akuntabilitas, inklusivitas, dan pelindungan data. Implementasi yang efektif bergantung pada kerja sehari-hari organisasi: pemetaan aliran data, dasar pemrosesan yang tepat, penilaian dampak, kontrol teknis, uji vendor, pengawasan manusia, respons insiden, dan pemulihan. Kerangka internasional seperti NIST AI RMF dapat membantu menyusun proses manajemen risiko, dengan tetap mengutamakan hukum Indonesia dan konteks lokal.

Kepercayaan yang layak terhadap AI bukan kepercayaan tanpa syarat. Ia adalah keyakinan yang dapat diperiksa, disertai hak untuk bertanya, memperbaiki, menolak, mengajukan keberatan, dan memperoleh pemulihan. Organisasi yang memperlakukan privasi sebagai kualitas sistem, bukan biaya kepatuhan, akan memiliki dasar lebih kuat untuk menggunakan AI secara produktif dan bertanggung jawab. Dengan demikian, perlindungan data bukan penghalang bagi inovasi; ia menentukan apakah inovasi itu memperoleh legitimasi sosial dan dapat bertahan.

Glossarium

Akuntabilitas: kewajiban organisasi untuk bertanggung jawab atas pemrosesan data serta mampu menunjukkan kepatuhan dan efektivitas kontrolnya.

Anonimisasi: proses yang menghilangkan keterkaitan data dengan individu sehingga identifikasi kembali tidak lagi mungkin secara wajar dalam konteks yang dinilai. Berbeda dari pseudonimisasi.

AI generatif: sistem AI yang menghasilkan teks, gambar, audio, video, kode, atau keluaran lain berdasarkan pola dalam data dan instruksi pengguna.

Dasar pemrosesan: landasan hukum yang membolehkan pengendali memproses data pribadi untuk tujuan tertentu, misalnya persetujuan, kontrak, kewajiban hukum, tugas kepentingan umum, atau kepentingan sah sesuai UU PDP.

Data pribadi: data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, secara langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik.

Differential privacy: teknik matematis yang membatasi seberapa jauh keluaran analisis dapat mengungkap kontribusi satu individu.

Federated learning: metode pelatihan model pada beberapa perangkat atau institusi tanpa harus mengumpulkan seluruh data mentah pada satu pusat, dengan tetap memerlukan pengamanan tambahan.

Hak subjek data: hak yang dimiliki individu atas pemrosesan data pribadinya, termasuk akses, koreksi, informasi, penghapusan atau penghentian sesuai ketentuan, dan keberatan atas keputusan otomatis berdampak signifikan.

Inferensi: kesimpulan yang dihasilkan dari analisis data, termasuk atribut yang tidak diberikan langsung oleh individu.

Pengendali data pribadi: pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi.

Pemroses data pribadi: pihak yang memproses data pribadi atas nama pengendali.

Penilaian dampak pelindungan data: evaluasi sistematis atas risiko pemrosesan terhadap hak subjek data dan langkah untuk mengurangi risiko tersebut.

Pseudonimisasi: penggantian pengenal langsung dengan kode atau atribut lain sehingga identitas tidak langsung tampak, tetapi masih dapat dipulihkan dengan informasi tambahan.

Privacy by design: pendekatan yang memasukkan perlindungan privasi ke dalam tujuan, desain, pengembangan, pengadaan, dan operasi sistem sejak awal.

Privacy-enhancing technologies (PETs): keluarga teknik dan arsitektur yang membantu membatasi paparan data saat disimpan, dibagikan, atau dianalisis.

Profiling: pemrosesan otomatis data untuk menilai atau memprediksi aspek pribadi seseorang, seperti perilaku, minat, keadaan ekonomi, kesehatan, atau preferensi.

Subjek data pribadi: orang perseorangan yang pada dirinya melekat data pribadi yang diproses.

Teknologi pengenal biometrik: teknologi yang memproses karakteristik fisik atau perilaku untuk mengidentifikasi atau memverifikasi individu, seperti wajah, sidik jari, atau suara.

Transfer lintas batas: pengiriman atau pemberian akses atas data pribadi kepada pihak atau sistem di luar wilayah hukum Indonesia.

Trustworthy AI: AI yang dapat diandalkan berdasarkan sifat sistem dan tata kelola, termasuk validitas, keamanan, privasi, keadilan, transparansi, dan akuntabilitas.

Daftar Pustaka

Budiman, R. (2023). The development of personal data protection law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. *Jurnal Smart Hukum, 2*(1), 24–36. https://doi.org/10.55299/jsh.v2i1.1352

De Cristofaro, E. (2021). A critical overview of privacy in machine learning. *IEEE Security & Privacy, 19*(4), 19–27. https://doi.org/10.1109/MSEC.2021.3076443

Lahusen, C., Maggetti, M., & Slavkovik, M. (2024). Trust, trustworthiness and AI governance. *Scientific Reports, 14*, Article 20752. https://doi.org/10.1038/s41598-024-71761-0

Kementerian Komunikasi dan Digital. (2025). *Konsultasi publik buku putih peta jalan kecerdasan artifisial nasional dan konsep pedoman etika kecerdasan artifisial*. https://portal.komdigi.go.id/kanal-publik/berita-kini/9531

Kementerian Komunikasi dan Informatika. (2023). *Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang etika kecerdasan artifisial*. https://jdih.komdigi.go.id/produk_hukum/view/id/883

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys, 54*(2), Article 31. https://doi.org/10.1145/3436755

Meurisch, C., & Mühlhäuser, M. (2021). Data protection in AI services: A survey. *ACM Computing Surveys, 54*(2), Article 40. https://doi.org/10.1145/3440754

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820. https://peraturan.bpk.go.id/Details/229798/u

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review, 14*(2), Article 4. https://doi.org/10.15742/ilrev.v14n2.4

Catatan Referensi

Naskah ini menggunakan sumber hukum primer dan karya ilmiah yang dapat diverifikasi. Peraturan, pedoman, dan rancangan kebijakan dapat berubah; pembaca disarankan memeriksa naskah resmi terbaru sebelum mengambil keputusan kepatuhan. DOI pada daftar pustaka dicantumkan untuk sumber akademik yang memilikinya; peraturan dan dokumen pemerintah umumnya tidak memiliki DOI.