JIPSI: Jurnal Ilmu Pendidikan dan Sains Islam Interdisipiner
Vol. 5, No. 4, November 2026, pp. 3709-3724
http://journal.amorfati.id/index.php/jipsi || ISSN 2962-9187

Interdisciplinary Scope of Science and Education, Islamic Education and Science, Integration of Science and Islam, Islamic Thought and Philosophy, Integration of Social Sciences, Humanities, and Islamic Studies, Islamic Economics and Business Studies, and Islamic Ethics in Science and Technology

Dampak Ganda Artificial Intelligence terhadap Keamanan Data Konsumen: Perspektif Hukum dan Etika Islam

Rika [a,1], Nabilla Ivana Nova [b,2], Sela Nabila [c,3,*], Parid Rehan Paiza [d,4], Norita Sinaga [e,5]

[a,b,c,d,e] Universitas Pamulang, Indonesia.

[1]rikaa7728@gmail.com; [2]nabillaivananova@gmail.com; [3]selanabila0311@gmail.com; [4]paridrehanpaiza17@gmail.com; [5]dosen03146@unpam.ac.id
*Correspondent Author: selanabila0311@gmail.com

ARTICLE INFO

Article history
Received:
17-08-2026
Revised:
21-09-2026
Accepted:
24-10-2026

Keywords
Artificial intelligence; Privasi konsumen; Tata kelola AI; Etika Islam; Perlindungan data

ABSTRAK

Adopsi artificial intelligence (AI) memperkuat deteksi anomali dan penipuan, tetapi juga memperluas risiko profiling, inferensi atribut sensitif, dan kebocoran melalui model. Kajian ini menganalisis dampak ganda tersebut serta merumuskan tata kelola perlindungan data konsumen yang memadukan kontrol teknis, kewajiban hukum Indonesia, dan etika Islam. Tinjauan literatur integratif menggunakan 24 artikel jurnal inti, enam buku teoretis, serta dokumen kebijakan; tiga kajian etika Islam ditambahkan sebagai lensa normatif. Artikel dipilih berdasarkan relevansi AI, privasi konsumen, dan keamanan data, kemudian disintesis secara tematik menurut siklus hidup data dan model. Sintesis menunjukkan bahwa manfaat deteksi adaptif dan privacy-enhancing technologies bergantung pada minimisasi data, pengujian kebocoran, pembatasan akses, dan pengawasan manusia. Sebaliknya, personalisasi tanpa kendali tujuan meningkatkan risiko intrusi dan menurunkan kepercayaan. Kebaruan kajian terletak pada enam gerbang tata kelola yang memetakan bukti literatur ke kontrol yang dapat diaudit, dengan prinsip amanah, keadilan, kemaslahatan, dan pencegahan mudarat sebagai landasan lintas tahap. Kerangka ini memberi pedoman praktis berupa inventaris data, penilaian risiko model, pengelolaan persetujuan dan hak konsumen, serta evaluasi insiden. Temuan bersifat konseptual dan masih memerlukan pengujian empiris.

Pendahuluan

Artificial intelligence (AI) telah bergerak dari teknologi eksperimental menjadi infrastruktur keputusan yang tertanam dalam perdagangan elektronik, layanan keuangan, telekomunikasi, kesehatan digital, transportasi, pemasaran, dan layanan pelanggan. Kemampuan AI untuk memproses data dalam volume besar, mengenali pola, serta menghasilkan prediksi secara real time membuat organisasi mampu menawarkan layanan yang lebih cepat dan lebih personal. Literatur pemasaran menunjukkan bahwa AI dapat memperkuat standardisasi, personalisasi, dan relasi

dengan konsumen melalui analisis data yang sebelumnya sulit dilakukan secara manual (Davenport et al., 2020; Huang & Rust, 2021). Dari sudut pengalaman konsumen, manfaat tersebut muncul dalam bentuk rekomendasi yang relevan, layanan otomatis, deteksi transaksi tidak wajar, hingga dukungan keputusan berbasis pola perilaku (Puntoni et al., 2021). Namun, keunggulan yang sama bergantung pada akumulasi dan pemrosesan data konsumen dalam skala yang jauh lebih intensif dibandingkan sistem konvensional.

Ketergantungan AI pada data menjadikan keamanan data konsumen bukan sekadar persoalan penyimpanan informasi, tetapi persoalan seluruh siklus hidup data dan model. Data dapat terekspos pada tahap pengumpulan, pembersihan, pelabelan, pelatihan, inferensi, integrasi dengan aplikasi lain, maupun ketika hasil model digunakan untuk mengambil keputusan. Perkembangan generative AI semakin memperluas permukaan risiko karena sistem dapat menerima masukan bebas dari pengguna, memanfaatkan data pelatihan yang sangat besar, dan menghasilkan keluaran yang berpotensi mengungkap informasi sensitif secara langsung maupun melalui inferensi. Martin dan Zimmermann (2024) menegaskan bahwa implikasi AI terhadap privasi perlu dibaca sebagai suatu ekosistem, sebab risiko tidak hanya muncul dari data yang sengaja diberikan, tetapi juga dari informasi yang dapat diturunkan dari kombinasi jejak digital. Ye et al. (2024) dan Liu et al. (2025) juga menunjukkan bahwa kompleksitas model generatif menantang pendekatan perlindungan data yang bertumpu semata pada persetujuan individual.

Persoalan tersebut membentuk paradoks. Semakin kaya data yang tersedia, semakin tinggi potensi AI untuk memperbaiki keamanan, misalnya melalui deteksi anomali, pemantauan fraud, klasifikasi risiko, dan respons insiden otomatis. Akan tetapi, semakin kaya data pula potensi penyalahgunaan, reidentifikasi, profiling, dan kebocoran meningkat. Pada konteks pemasaran berbasis AI, Alhitmi et al. (2024) mengidentifikasi kerahasiaan data, distribusi informasi, serangan siber, fraud, dan disinformasi sebagai risiko yang saling beririsan. Di sisi konsumen, kecanggihan AI bahkan dapat memunculkan persepsi hilangnya kendali atas data. Studi Shuqair et al. (2024) menunjukkan bahwa persepsi terhadap AI yang sangat kuat dapat meningkatkan kekhawatiran privasi ketika konsumen merasa kontrolnya atas informasi pribadi berkurang. Dengan demikian, efektivitas AI dan keamanan data tidak dapat dipisahkan sebagai dua agenda yang berdiri sendiri.

Kajian privasi konsumen sebelumnya banyak menjelaskan keputusan pengungkapan data melalui privacy calculus, yaitu pertukaran antara manfaat yang dirasakan, kepercayaan, dan persepsi risiko (Acquisti et al., 2015). Dalam ekosistem AI, kalkulus tersebut menjadi lebih rumit karena konsumen tidak selalu mengetahui jenis inferensi yang dapat dihasilkan dari data yang tampak tidak sensitif. Data lokasi, pola klik, riwayat pencarian, metadata perangkat, atau kombinasi perilaku dapat digunakan untuk memperkirakan preferensi, kondisi, atau karakteristik personal yang tidak pernah dinyatakan secara eksplisit. Brough (2026) menyebut kondisi ini sebagai perluasan risiko privasi

berbasis inferensi, yakni ketika 'brankas' data sensitif tidak perlu dibuka karena AI mampu menebak isinya dari sinyal lain. Situasi tersebut menggeser fokus pelindungan dari sekadar mencegah akses tanpa izin menuju pengendalian atas tujuan, konteks, dan konsekuensi pemrosesan data.

Bagi organisasi, keamanan data konsumen juga berkaitan langsung dengan kepercayaan dan legitimasi layanan digital. Pemenuhan ekspektasi privasi terbukti berkaitan dengan meningkatnya kepercayaan dan kepuasan, sedangkan pelanggaran batas privasi dapat menurunkan niat untuk melanjutkan hubungan dengan penyedia layanan (Swani et al., 2023). Pada personalisasi cerdas, kekhawatiran privasi dapat memicu resistensi konsumen, terutama ketika manfaat personalisasi tidak diimbangi dengan kontrol dan transparansi yang memadai (Cai & Mardani, 2023). Di tingkat organisasi, konsep corporate digital responsibility menempatkan tata kelola teknologi dan data sebagai bagian dari nilai serta norma perusahaan, bukan hanya kepatuhan teknis (Lobschat et al., 2021). Oleh karena itu, kebijakan keamanan yang hanya berfokus pada firewall, enkripsi, dan kontrol akses belum memadai apabila desain bisnis tetap mendorong pengumpulan data berlebihan atau penggunaan sekunder yang tidak dipahami konsumen.

Dalam konteks Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur hak subjek data, dasar pemrosesan, kewajiban pengendali dan prosesor, keamanan, transfer, serta sanksi. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial juga menempatkan keamanan, transparansi, akuntabilitas, dan pelindungan data pribadi sebagai prinsip penyelenggaraan AI. Meski demikian, tata kelola AI nasional masih berkembang. Hingga September 2026, pemerintah masih menyiapkan Peta Jalan AI Nasional dan regulasi etika AI yang lebih operasional. Kondisi ini menunjukkan bahwa organisasi perlu menerjemahkan prinsip hukum yang bersifat umum menjadi kontrol teknis dan manajerial di tingkat sistem, bahkan sebelum regulasi AI yang lebih spesifik berlaku penuh (Junaidi & Fadzil, 2024; Judijanto et al., 2024).

Kajian terdahulu cenderung mengulas kemampuan AI untuk pemasaran atau keamanan (Davenport et al., 2020; Alabdulatif, 2025), membahas risiko privasi konsumen (Martin & Zimmermann, 2024; Liu et al., 2025), atau mengkaji kepatuhan hukum secara terpisah (Junaidi & Fadzil, 2024; Judijanto et al., 2024). Hubungan antara inovasi AI, hak konsumen, dan kontrol yang dapat dibuktikan pada setiap tahap siklus data belum dirumuskan secara operasional melalui satu kerangka yang sekaligus mempertimbangkan etika Islam. Perspektif tersebut relevan bagi jurnal interdisipliner karena prinsip amanah dan keadilan memperluas evaluasi dari kepatuhan administratif ke pertanggungjawaban moral atas penggunaan data (Gorian & Osman, 2024; Habib, 2025). Atas kesenjangan itu, kajian ini memetakan manfaat dan ancaman AI, memperbandingkan keterbatasan pilihan teknis, serta menurunkan enam gerbang pengendalian yang terhubung dengan

UU PDP, hak konsumen, dan nilai kemaslahatan. Kontribusinya merupakan sintesis konseptual yang dapat diuji dan diaudit, bukan klaim bahwa semua kontrol telah terbukti efektif di setiap sektor.

Metode

Penelitian ini memakai tinjauan literatur integratif dengan sintesis tematik konseptual, sebagaimana pendekatan integratif yang menggabungkan temuan empiris, kajian teoretis, dan kebijakan untuk menghasilkan penjelasan baru (Whittemore & Knafl, 2005; Snyder, 2019). Unit analisis utama adalah 24 artikel jurnal yang tercantum dalam naskah awal, enam buku teoretis, dan dokumen hukum/kebijakan Indonesia. Tiga kajian tambahan tentang etika AI dan privasi dari perspektif Islam digunakan untuk menafsirkan aspek normatif (Gorian & Osman, 2024; Habib, 2025; Wicaksana et al., 2026), sedangkan dua artikel metodologi menjadi rujukan prosedur peninjauan. Pemisahan ini menjaga agar jumlah 24 artikel inti tidak keliru dipahami sebagai jumlah seluruh referensi.

Penelusuran dan pemeriksaan ulang literatur diarahkan pada laman jurnal/penerbit dan metadata DOI hingga 17 Oktober 2026, menggunakan padanan kata kunci artificial intelligence, consumer data security, data privacy, generative AI, privacy-preserving machine learning, profiling, AI governance, Islamic AI ethics, maqasid al-shariah, dan pelindungan data pribadi. Kriteria inklusi sumber inti meliputi: (1) membahas AI dan keamanan/privasi data atau hak konsumen secara langsung; (2) memberikan temuan, konsep, atau rekomendasi yang dapat dipetakan ke fase pengumpulan, pelatihan, inferensi, penggunaan, atau respons insiden; (3) berupa publikasi ilmiah yang identitas bibliografinya dapat diperiksa; serta (4) diutamakan terbit pada 2020–2026. Buku dan karya lebih lama dipertahankan khusus sebagai landasan teori. Sumber yang tidak relevan dengan fokus, duplikat, atau tidak jelas identitasnya tidak dimasukkan ke sintesis inti.

Analisis dilakukan melalui empat langkah: identifikasi fokus setiap publikasi, pencatatan potensi manfaat dan risiko AI, pengelompokan temuan menurut siklus data/model, lalu pemetaan kontrol dan nilai etis yang sesuai. Kesimpulan dipertemukan secara komparatif untuk menunjukkan kesepakatan, batasan teknis, serta konteks hukum Indonesia. Asal enam gerbang tata kelola ditelusuri melalui pasangan bukti–risiko–mitigasi pada Tabel 3. Perlu ditegaskan bahwa arsip pencarian awal, daftar hasil yang tidak terpilih, dan catatan deduplikasi tidak disertakan dalam naskah sumber; karena itu jumlah temuan sebelum penyaringan dan alur PRISMA tidak direkonstruksi secara spekulatif. Kajian ini merupakan integrative review, bukan systematic review atau meta-analisis, dan tidak menyimpulkan besaran efek kausal lintas industri.

Hasil dan Pembahasan

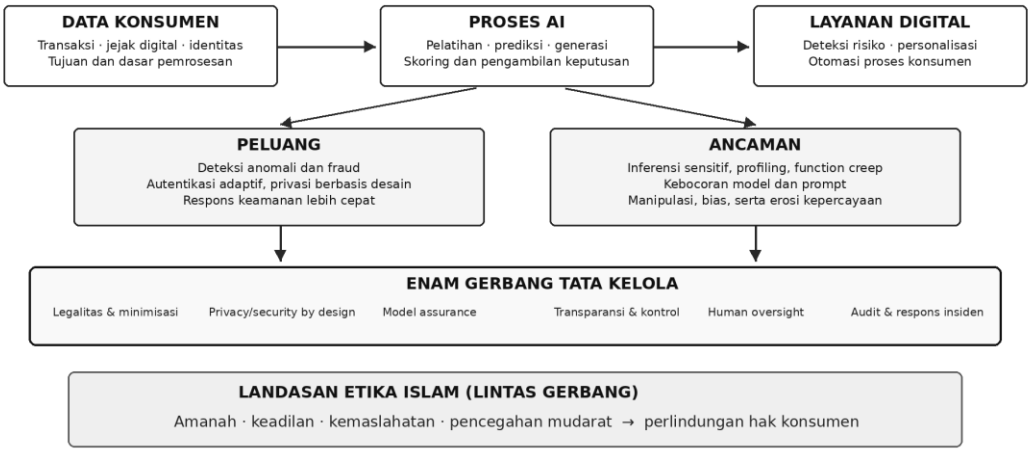
1. Arsitektur Dampak Ganda AI terhadap Keamanan Data Konsumen

Dampak ganda AI dapat dipahami dari sifat dasar teknologi ini yang mengubah data menjadi keputusan melalui pembelajaran pola. Pada jalur positif, kemampuan pengenalan pola meningkatkan

sensitivitas sistem terhadap anomali yang sulit diamati manusia. AI dapat membandingkan ribuan sinyal transaksi, perilaku login, perangkat, lokasi, dan pola jaringan untuk membentuk skor risiko dinamis. Pendekatan semacam ini relevan untuk mendeteksi fraud, account takeover, bot, aktivitas akses tidak wajar, dan indikasi serangan siber. Pada sistem terdistribusi, federated learning memungkinkan model belajar dari data lokal tanpa harus memindahkan seluruh data mentah ke satu pusat. Penelitian terkini menunjukkan bahwa kombinasi federated learning, differential privacy, secure aggregation, dan deteksi anomali dapat memperkuat perlindungan data sekaligus mempertahankan kemampuan deteksi (Alabdulatif, 2025; Bunko et al., 2026).

Pada jalur negatif, proses yang sama memperbesar kapasitas organisasi atau penyerang untuk menghubungkan titik-titik data yang sebelumnya terpisah. Model dapat menginferensi atribut sensitif, mengidentifikasi pola perilaku, dan membangun profil yang jauh lebih rinci daripada data input eksplisit. Risiko juga tidak berhenti pada database. Parameter model, embedding, log percakapan, output probabilitas, prompt, dan catatan telemetri dapat menjadi sumber kebocoran baru. Survei privasi pada generative AI menunjukkan bahwa model dapat menghadapi risiko kebocoran melalui data pelatihan, interaksi pengguna, serangan inferensi, maupun akses tidak sah terhadap infrastruktur model (Liu et al., 2025). Karena itu, keamanan data konsumen harus mencakup data at rest, data in transit, data in use, serta informasi yang direpresentasikan atau dapat diekstraksi dari model.

Gambar 1 menggambarkan mekanisme sebab-akibat yang disintesis. Data konsumen diproses AI dan dapat menghasilkan peningkatan keamanan ataupun ancaman baru. Enam gerbang tata kelola bertindak sebagai kontrol sepanjang siklus penggunaan, sedangkan nilai amanah, keadilan, kemaslahatan, dan pencegahan mudarat menjadi lensa evaluasi lintas gerbang. Model tersebut menggabungkan perlindungan teknis, hak konsumen, dan tanggung jawab etis; hubungan yang ditunjukkan merupakan proposisi konseptual, bukan hasil pengujian efektivitas.



Gambar 1. Kerangka integratif AI, keamanan data konsumen, hukum, dan etika Islam

Tabel 1. Peta dampak ganda AI pada siklus pengelolaan data konsumen

Tahap	Peluang	Ancaman	Kontrol prioritas
Akuisisi data	Deteksi identitas palsu, validasi sinyal, risk scoring awal	Over-collection, pengumpulan tanpa tujuan jelas, function creep	Purpose limitation, minimisasi, consent granular, inventaris data
Pemrosesan dan pelatihan	Analitik risiko, deteksi anomali, pembelajaran lintas sumber	Kebocoran data pelatihan, inferensi atribut, memorisasi, bias	Pseudonimisasi, federated learning, differential privacy, akses berbasis peran
Inferensi dan personalisasi	Layanan relevan, autentikasi adaptif, pencegahan fraud real time	Profiling invasif, keputusan opak, manipulasi, diskriminasi	Explainability proporsional, batas penggunaan profil, opt-out, uji fairness dan privasi
Interaksi generative AI	Otomasi dukungan pelanggan, edukasi keamanan, triase insiden	Prompt leakage, data sensitif masuk ke model, phishing/deepfake, prompt injection	DLP, redaksi otomatis, sandboxing, filter input-output, human review
Respons insiden	Prioritisasi alert, korelasi log, isolasi ancaman lebih cepat	False positive otomatis dan keputusan tanpa akuntabilitas	Human-in-the-loop, logging, mekanisme banding, post-incident audit

2. Peluang AI sebagai Penguat Keamanan dan Privasi

Peluang pertama berasal dari kemampuan AI untuk melakukan deteksi ancaman secara adaptif. Sistem keamanan tradisional cenderung mengandalkan aturan yang telah ditentukan, sedangkan model machine learning dapat mempelajari pola normal dan mengenali deviasi yang tidak sesuai dengan baseline. Dalam lingkungan transaksi konsumen, pendekatan ini memungkinkan identifikasi fraud dari kombinasi variabel yang sangat banyak tanpa menunggu satu indikator tunggal melewati ambang tertentu. Alabdulatif (2025) menunjukkan bahwa deteksi anomali berbasis federated learning dan differential privacy dapat mempertahankan utilitas model sambil mengurangi eksposur data mentah. Kajian Bunko et al. (2026) juga menegaskan bahwa federated learning relevan untuk intrusion detection, walaupun data locality saja tidak cukup dan perlu diperkuat dengan privacy-enhancing techniques lain.

Peluang kedua adalah pergeseran dari keamanan reaktif menuju keamanan prediktif. AI dapat menghubungkan event dari berbagai sumber, memberi skor risiko, memprioritaskan alert, dan membantu analis menentukan insiden yang paling kritis. Dalam skenario konsumen, manfaatnya dapat berupa pemblokiran transaksi abnormal, step-up authentication, peringatan login berisiko, serta deteksi perubahan pola penggunaan yang mengindikasikan pengambilalihan akun. Nilai utama bukan pada penggantian analis manusia, tetapi pada pengurangan beban pemantauan dan percepatan respons. Model yang digunakan tetap memerlukan validasi karena otomatisasi tanpa

kontrol dapat menghasilkan false positive, memblokir pengguna sah, atau memunculkan keputusan yang sulit dijelaskan.

Peluang ketiga terletak pada penggunaan AI bersama privacy-enhancing technologies. Federated learning memungkinkan pelatihan kolaboratif dengan mempertahankan data mentah pada sumbernya; differential privacy menambahkan mekanisme noise terkontrol untuk mengurangi peluang identifikasi individu; dan homomorphic encryption membuka kemungkinan komputasi atas data terenkripsi. Abdirahman et al. (2026) memperlihatkan perkembangan kerangka machine learning berbasis homomorphic encryption untuk inferensi cloud tanpa membuka data mentah kepada server. Bozorgpanah dan Torra (2024) menambahkan bahwa privasi dan explainability dapat dirancang bersama melalui pilihan teknik yang menyeimbangkan keterbacaan dan perlindungan data. Artinya, arsitektur AI tidak harus selalu mempertukarkan akurasi dengan privasi secara absolut; desain teknis dapat memindahkan titik keseimbangan menjadi lebih aman.

Masing-masing teknologi pelindung memiliki batas implementasi. Federated learning mengurangi sentralisasi data mentah, tetapi gradien atau pembaruan model tetap dapat mengungkap informasi tanpa secure aggregation atau differential privacy. Differential privacy mengurangi risiko inferensi statistik, namun penambahan noise berpotensi menurunkan utilitas, terutama bagi kelompok data kecil. Homomorphic encryption melindungi data selama komputasi, tetapi menambah latensi, kompleksitas, dan kebutuhan sumber daya. Bahkan explainable AI menimbulkan dilema: penjelasan meningkatkan kontrol pengguna, tetapi penjelasan yang terlalu rinci dapat membocorkan informasi (Bozorgpanah & Torra, 2024; Nguyen et al., 2025). Oleh sebab itu, pilihan mitigasi tidak dapat ditetapkan sebagai daftar teknologi universal; organisasi perlu menilai skenario ancaman, data sensitif, performa model, serta biaya kepatuhan secara proporsional.

Peluang keempat adalah otomasi kepatuhan dan kontrol data. AI dapat membantu menemukan data sensitif, mengklasifikasikan dokumen, memonitor retensi, mengidentifikasi akses tidak lazim, atau menandai data pribadi yang dimasukkan pengguna ke kanal yang tidak semestinya. Namun, penggunaan AI untuk fungsi kepatuhan perlu didesain sebagai alat bantu, bukan sebagai legitimasi pengumpulan data yang lebih luas. Prinsip data minimization tetap harus menjadi titik awal. Dalam kerangka corporate digital responsibility, teknologi yang kuat harus disertai nilai organisasi yang menentukan apa yang boleh dilakukan terhadap data, bukan hanya apa yang secara teknis mungkin dilakukan (Lobschat et al., 2021).

3. Ancaman: Ekspansi Data, Inferensi, Kebocoran Model, dan Profiling

Ancaman paling mendasar adalah ekspansi data. Model yang lebih kompleks sering mendorong organisasi menambah jumlah variabel, memperpanjang periode retensi, dan menggabungkan data lintas kanal dengan alasan meningkatkan akurasi. Praktik tersebut menciptakan function creep, yaitu pergeseran penggunaan data dari tujuan awal ke tujuan baru yang tidak dipahami konsumen.

Semakin banyak data disatukan, semakin besar dampak ketika terjadi breach. Selain itu, data yang pada awalnya tampak tidak sensitif dapat berubah menjadi sensitif setelah dikombinasikan dengan data lain. Kerangka contextual integrity dari Nissenbaum (2010) relevan di sini karena pelanggaran privasi tidak selalu ditentukan oleh kerahasiaan data, melainkan oleh ketidaksesuaian aliran informasi dengan konteks dan ekspektasi yang wajar.

Ancaman kedua adalah inferensi. AI dapat menghasilkan informasi baru tentang konsumen tanpa harus mengakses kategori data sensitif secara eksplisit. Pola transaksi, lokasi, jenis perangkat, waktu aktivitas, dan preferensi konten dapat digunakan untuk memprediksi kondisi ekonomi, kebiasaan, atau preferensi personal. Brough (2026) menekankan bahwa risiko privasi modern semakin bergeser dari pencurian data rahasia menuju kemampuan menyimpulkan data rahasia. Konsekuensinya, mekanisme persetujuan yang hanya menjelaskan daftar data yang dikumpulkan menjadi tidak cukup. Konsumen juga perlu memperoleh informasi mengenai tujuan profiling, kategori keputusan, konsekuensi penting, dan batas penggunaan inferensi.

Ancaman ketiga berkaitan dengan model leakage. Model dapat menyimpan representasi statistik dari data pelatihan dan, dalam kondisi tertentu, mengungkap pola atau informasi melalui keluaran, gradien, embedding, atau respons yang tidak semestinya. Liu et al. (2025) memetakan risiko privacy attack pada generative AI, termasuk kebocoran dari data pelatihan dan interaksi. Nguyen et al. (2025) menunjukkan bahwa bahkan mekanisme explainability dapat menjadi kanal kebocoran apabila penjelasan mengungkap terlalu banyak informasi tentang model atau data. Karena itu, audit privasi perlu mencakup model dan interface, bukan hanya database. Pengujian red-team, evaluasi prompt injection, pengendalian retrieval-augmented generation, pembatasan logging, serta kebijakan retensi prompt menjadi bagian dari keamanan operasional generative AI.

Ancaman keempat adalah peningkatan skala manipulasi dan rekayasa sosial. Generative AI dapat mempercepat pembuatan pesan phishing, impersonasi, deepfake, atau konten yang dipersonalisasi berdasarkan informasi publik maupun data bocor. Di sisi internal, data poisoning dan prompt injection dapat mengubah perilaku sistem sehingga memberikan jawaban atau tindakan yang merugikan. Risiko ini mengubah relasi antara keamanan model dan keamanan konsumen. Sistem yang memiliki akses ke akun, basis data, atau fungsi agentic tidak boleh diberi otoritas yang sama dengan chatbot informasi biasa. Semakin besar dampak keputusan, semakin tinggi kebutuhan terhadap pembatasan hak akses, konfirmasi manusia, logging yang dapat diaudit, dan mekanisme penghentian otomatis ketika anomali terdeteksi.

Ancaman kelima bersifat psikologis dan institusional, yakni erosi kepercayaan. Konsumen dapat menerima personalisasi ketika manfaat dan batas penggunaan data dipahami, tetapi resistensi meningkat ketika proses dianggap terlalu invasif atau tidak dapat dikendalikan. Cai dan Mardani (2023) menemukan hubungan antara privasi konsumen, personalisasi cerdas, dan resistensi

pembelian. Shuqair et al. (2024) menunjukkan bahwa persepsi AI yang sangat kuat dapat menimbulkan kekhawatiran privasi karena konsumen merasa kehilangan kontrol. Temuan ini konsisten dengan perspektif privacy calculus, tetapi AI menambah ketidakpastian baru karena pengguna sulit memperkirakan apa yang dapat disimpulkan model dari data yang mereka berikan. Transparansi karenanya harus lebih dari sekadar kebijakan privasi panjang; transparansi perlu berorientasi pada keputusan yang dapat dipahami dan tindakan yang dapat dipilih konsumen.

4. Konteks Indonesia: Dari Kepatuhan Hukum menuju Tata Kelola Sistem

UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menyediakan landasan penting melalui prinsip pemrosesan yang sah, hak subjek data, kewajiban pengendali dan prosesor, keamanan pemrosesan, serta tanggung jawab ketika terjadi kegagalan pelindungan. Dalam praktik AI, ketentuan tersebut perlu diterjemahkan ke pertanyaan teknis yang konkret: apakah setiap fitur yang digunakan model memiliki tujuan yang sah, apakah data yang tidak relevan dihapus, siapa yang dapat mengakses data pelatihan, berapa lama prompt atau log disimpan, bagaimana data lintas sistem digabungkan, dan bagaimana konsumen dapat menggunakan haknya. Putra et al. (2024) menunjukkan bahwa pemrosesan data konsumen pada e-commerce Indonesia masih menyisakan celah implementasi yang membutuhkan penguatan mekanisme kepatuhan dan akuntabilitas.

Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 memperluas orientasi tersebut dengan prinsip inklusivitas, kemanusiaan, keamanan, transparansi, kredibilitas dan akuntabilitas, serta pelindungan data pribadi. Dokumen ini penting sebagai rujukan etika, tetapi karakter surat edaran belum menggantikan kebutuhan kontrol sektoral dan standar teknis yang dapat diaudit. Junaidi dan Fadzil (2024) menyoroti urgensi pengaturan yang lebih operasional pada transaksi e-commerce berbasis AI, sedangkan Judijanto et al. (2024) menekankan tantangan AI terhadap persetujuan, transparansi, dan standar privasi dalam hukum siber Indonesia.

Per September 2026, pemerintah masih menyiapkan Peta Jalan AI Nasional dan regulasi etika AI yang lebih kuat. Arah kebijakan yang dikemukakan pemerintah menekankan pendekatan berbasis risiko, human-centric AI, human-in-the-loop, keamanan, serta keterkaitan tata kelola AI dengan pelindungan data pribadi. Bagi pelaku usaha, masa transisi regulasi bukan alasan untuk menunda mitigasi. Sebaliknya, organisasi dapat menggunakan UU PDP dan prinsip etika AI yang telah ada sebagai baseline untuk membangun governance-by-design. Pendekatan ini juga mengurangi biaya penyesuaian ketika standar AI nasional menjadi lebih spesifik, karena inventaris data, risk register, dokumentasi model, kontrol akses, dan audit trail sudah tersedia sejak awal.

Pada titik ini, perbedaan antara compliance dan governance menjadi penting. Compliance menanyakan apakah organisasi telah memenuhi ketentuan minimum; governance menanyakan siapa yang berwenang membuat keputusan, bagaimana risiko diukur, kontrol apa yang dipasang, bagaimana pengecualian disetujui, dan bagaimana bukti kepatuhan dipelihara. AI membutuhkan

keduanya. Regulasi tanpa arsitektur teknis sulit dioperasionalkan, sedangkan arsitektur teknis tanpa dasar etika dan hukum dapat mengoptimalkan tujuan bisnis dengan mengabaikan hak konsumen.

Dalam operasional UU PDP, pembatasan tujuan dan minimisasi memerlukan data inventory, klasifikasi atribut, serta jadwal retensi; hak akses, koreksi, dan penghapusan membutuhkan alur permohonan yang terhubung ke data pelatihan, log, dan pemasok model; kewajiban keamanan membutuhkan pembatasan akses, pengujian, dan pencatatan insiden. Akan tetapi, menghapus data dari basis operasional belum otomatis menghapus pengaruhnya dari parameter model. Di sinilah penilaian dampak, dokumentasi model, dan prosedur pemutakhiran atau penghentian sistem menjadi penghubung teknis terhadap pelaksanaan hak subjek data. Penjabaran tersebut merupakan implikasi analitis dari UU PDP, bukan pernyataan bahwa undang-undang secara eksplisit mewajibkan setiap teknologi yang disebutkan.

5. Etika Islam sebagai Lensa Evaluasi Keamanan Data Konsumen

Etika Islam memberi pijakan substantif untuk menilai dampak yang tidak selalu terlihat dari kepatuhan formal. Amanah menempatkan data konsumen sebagai titipan yang penggunaannya harus dapat dipertanggungjawabkan; keadilan menuntut agar keputusan otomatis tidak memindahkan risiko diskriminasi kepada kelompok rentan; prinsip kemaslahatan dan pencegahan mudarat mengharuskan manfaat personalisasi ditimbang terhadap kerugian privasi, penipuan, dan reputasi. Gorian dan Osman (2024) menunjukkan relevansi nilai privasi Islam terhadap kebijakan etika AI, sedangkan Habib (2025) menawarkan pembacaan maqasid al-shariah bagi risiko bias, data, dan akuntabilitas. Wicaksana et al. (2026) secara khusus menempatkan amanah, keadilan, dan pencegahan mudarat sebagai pelengkap normatif bagi UU Pelindungan Data Pribadi.

Secara operasional, prinsip tersebut diterjemahkan menjadi pertanyaan audit, bukan klaim bahwa semua perusahaan atau konsumen memiliki orientasi keagamaan yang sama. Pada tahap akuisisi, amanah menguji apakah data yang diminta benar-benar diperlukan; pada personalisasi, keadilan menguji keberpihakan dan akses terhadap mekanisme keberatan; pada generative AI, pencegahan mudarat menguji kemungkinan kebocoran, manipulasi, dan pengungkapan informasi yang merusak martabat. Nilai etis ini tidak menggantikan UU PDP atau standar keamanan teknis, tetapi memperjelas alasan moral mengapa kontrol tetap harus dilakukan ketika eksploitasi data memungkinkan secara teknis namun merugikan konsumen.

6. Kerangka Integratif Tata Kelola AI Berorientasi Hak Konsumen dan Etika Islam

Kerangka enam gerbang dihasilkan melalui pengelompokan bukti literatur berdasarkan tahapan proses data serta jenis kegagalan yang hendak dicegah. Bukti privasi konsumen mendasari gerbang legalitas/minimisasi; studi privasi komputasional mendasari privacy dan security by design; kajian kebocoran model mendasari model assurance; studi privacy calculus dan pengalaman pengguna mendasari transparansi serta kontrol; risiko keputusan otomatis menuntut human oversight;

sedangkan risiko insiden memerlukan audit yang dapat ditelusuri (Acquisti et al., 2015; Alabdulatif, 2025; Liu et al., 2025; Shuqair et al., 2024). Keenam gerbang bekerja secara berurutan namun iteratif: pengendalian pada saat desain harus diuji kembali setelah model digunakan. Prinsip amanah dan keadilan berfungsi sebagai penilaian etis lintas gerbang agar pemenuhan prosedur tidak berhenti pada formalitas.

Gerbang pertama ialah legalitas dan minimisasi yang mewajibkan tujuan, dasar pemrosesan, dan pembatasan atribut. Kedua, privacy/security by design menerapkan pemisahan data, kontrol akses, pengamanan aplikasi, dan PETs sesuai ancaman. Ketiga, model assurance menguji akurasi, bias, kebocoran, dan manipulasi. Keempat, transparansi dan kontrol konsumen memungkinkan penjelasan yang proporsional, koreksi, serta penolakan pemrosesan sesuai hak yang berlaku. Kelima, human oversight menyediakan peninjauan dan mekanisme keberatan atas keputusan berisiko tinggi. Keenam, audit dan respons insiden memastikan pembuktian tindakan, perbaikan, dan akuntabilitas. Bukti implementasi minimum dan penanggung jawab perlu diperiksa pada setiap fase, termasuk pengadaan model pihak ketiga.

Kerangka tersebut juga menyelesaikan kesalahpahaman bahwa privasi selalu menghambat inovasi. Justru, kontrol privasi yang jelas dapat meningkatkan kualitas data dan kepercayaan. Cloarec (2022) menunjukkan bahwa kontrol privasi dapat mengurangi perilaku konsumen memalsukan data sebagai respons atas rasa rentan. Swani et al. (2023) menunjukkan bahwa pemenuhan ekspektasi privasi mendukung kepercayaan dan keberlanjutan hubungan. Dari sisi desain AI, teknologi seperti differential privacy, federated learning, dan homomorphic encryption memperlihatkan bahwa perlindungan dapat dibangun ke dalam arsitektur, walaupun selalu terdapat trade-off yang harus diukur. Dengan kata lain, tujuan yang realistis bukan 'tanpa risiko', melainkan risiko yang dikenali, diminimalkan, diuji, dikomunikasikan, dan dapat dipertanggungjawabkan.

Hubungan bukti dengan rancangan gerbang diringkas dalam Tabel 3. Setiap kelompok artikel memiliki kontribusi berbeda: studi teknis menunjukkan kemampuan dan batas mitigasi, studi konsumen mengungkap dampak pada persepsi dan kontrol, sedangkan literatur hukum dan etika menilai legitimasi tujuan penggunaan data. Karena karakter sumber heterogen, kerangka tidak boleh dibaca sebagai peringkat bukti numerik ataupun pengujian hubungan kausal.

Tabel 2. Kerangka operasional tata kelola AI, hak konsumen, dan etika Islam

Gerbang tata kelola	Pertanyaan kontrol	Implementasi minimum	Bukti audit
Legalitas & minimisasi	Apakah data dan fitur benar-benar diperlukan untuk tujuan layanan	Data inventory, purpose mapping, batas retensi, consent/landasan pemrosesan; audit amanah	RoPA, data dictionary, catatan retensi

Gerbang tata kelola	Pertanyaan kontrol	Implementasi minimum	Bukti audit
Privacy & security by design	Apakah arsitektur mengurangi eksposur data sejak awal	Enkripsi, pseudonimisasi, RBAC, secure API, segmentasi, PETs; cegah mudarat	Architecture review, access log, hasil security testing
Model assurance	Apakah model aman terhadap kebocoran dan manipulasi	Privacy test, robustness test, red-team, prompt injection/data poisoning test; uji keadilan	Model card, test report, risk register
Transparansi & kontrol konsumen	Apakah pengguna memahami penggunaan AI dan memiliki pilihan bermakna	Notice ringkas, preference center, opt-out/limitation, correction channel; verifikasi hak	Versi notice, consent log, ticket hak subjek data
Human oversight	Apakah keputusan berdampak tinggi dapat ditinjau manusia	Escalation rule, approval gate, manual override; peninjauan adil	Decision log, approval record, appeal outcome
Audit & respons insiden	Apakah insiden dapat dideteksi, ditelusuri, dan dipulihkan	Monitoring, alerting, versioning, incident playbook, post-incident review; pemulihan hak	Audit trail, incident report, corrective action record

Tabel 3. Matriks sintesis bukti dan derivasi gerbang tata kelola

Klaster bukti	Temuan dan batas penting	Risiko/implikasi	Gerbang yang diturunkan
Deteksi keamanan; PETs	Alabdulatif (2025); Bunko et al. (2026); Abdirahman et al. (2026): deteksi dan komputasi lebih terlindungi, dengan biaya dan kompromi utilitas.	Paparan data dan keterbatasan mitigasi	Privacy/security by design; model assurance
Profiling, privasi dan pengalaman konsumen	Acquisti et al. (2015); Cai & Mardani (2023); Shuqair et al. (2024): manfaat personalisasi bergantung pada ekspektasi dan kontrol pengguna.	Penggunaan sekunder, resistensi, hilang kontrol	Legalitas/minimisasi; transparansi dan kontrol
Model generatif dan kebocoran	Liu et al. (2025); Ye et al. (2024); Nguyen et al. (2025): input, output, parameter, dan penjelasan dapat mengekspos data.	Inferensi dan prompt/model leakage	Model assurance; audit dan respons insiden
Akuntabilitas organisasi dan hukum	Lobschat et al. (2021); Putra et al. (2024); Judijanto et al. (2024): tata kelola perlu melampaui keamanan infrastruktur.	Kesenjangan hak pengguna dan tanggung jawab vendor	Human oversight; audit dan respons insiden
Norma Islam dan hak digital	Gorian & Osman (2024); Habib (2025); Wicaksana et al. (2026): amanah, keadilan, maslahat dan pencegahan mudarat menilai legitimasi praktik.	Dampak moral yang lolos dari kepatuhan formal	Lensa etika lintas keenam gerbang

7. Implikasi Praktis dan Hambatan Penerapan pada Layanan Digital

Bagi pengembang, implikasi utama adalah kebutuhan memisahkan data yang 'tersedia' dari data yang 'layak digunakan'. Ketersediaan teknis tidak otomatis menciptakan legitimasi pemrosesan. Feature engineering perlu disertai review terhadap sensitivitas, risiko inferensi, dan dampak jika fitur dikombinasikan dengan data lain. Dalam penggunaan model pihak ketiga, organisasi perlu memahami kebijakan penyimpanan input, penggunaan data untuk peningkatan model, lokasi

pemrosesan, subprosesor, serta opsi enterprise privacy. Input pengguna yang mengandung identitas, data keuangan, kesehatan, atau informasi rahasia sebaiknya diproteksi melalui redaction, tokenization, atau routing ke model yang memiliki kontrol privasi memadai.

Bagi penyelenggara layanan, prioritasnya adalah membangun tata kelola lintas fungsi. Keamanan data AI tidak dapat diserahkan hanya kepada tim IT karena keputusan tentang tujuan data, pengalaman pengguna, pemasaran, retensi, dan monetisasi berada di unit yang berbeda. Komite atau fungsi tata kelola AI sebaiknya menghubungkan pemilik bisnis, keamanan informasi, legal/privacy, data science, audit, dan customer experience. Risk classification membantu menentukan intensitas kontrol. Sistem rekomendasi konten dengan dampak rendah tidak memerlukan mekanisme yang sama dengan sistem yang dapat memblokir rekening, menilai kredit, atau mengakses data identitas sensitif.

Penerapan kerangka menghadapi hambatan nyata. Organisasi kecil mungkin kekurangan kompetensi pengujian model, anggaran PETs, dan inventaris data lintas vendor; organisasi besar menghadapi silo proses bisnis, sistem lama, serta ketergantungan terhadap model tertutup. Selain itu, konflik antara akurasi prediksi dan minimisasi data dapat memicu kompromi yang tidak transparan. Strategi bertahap yang realistis adalah menetapkan pemilik risiko, menginventaris data dan vendor, mengklasifikasikan keputusan berdampak tinggi, menguji satu layanan prioritas, lalu memperluas audit dan pelatihan lintas fungsi. Kelayakan implementasi sebaiknya dinilai melalui indikator terukur, seperti waktu penanganan permohonan hak konsumen, jumlah insiden berulang, hasil uji privasi model, dan proporsi keputusan berisiko tinggi yang memperoleh peninjauan manusia.

Bagi konsumen, desain yang bertanggung jawab harus mengurangi asymmetry of information. Konsumen tidak semestinya dipaksa memahami detail teknis model, tetapi berhak memperoleh penjelasan yang cukup untuk memahami bagaimana data mereka digunakan dan konsekuensi penting yang mungkin timbul. Pendekatan ini sejalan dengan gagasan bahwa explainability harus disesuaikan dengan konteks, bukan diperlakukan sebagai satu bentuk penjelasan untuk semua situasi (Papagni et al., 2023). Pada saat yang sama, explainability tidak boleh membuka terlalu banyak detail yang justru meningkatkan risiko keamanan atau kebocoran model, sehingga organisasi perlu menyeimbangkan kebutuhan transparansi dan confidentiality (Nguyen et al., 2025).

Kesimpulan

Artificial intelligence menghasilkan dampak ganda terhadap keamanan data konsumen karena kapabilitas yang meningkatkan perlindungan juga dapat memperluas risiko. AI mampu memperkuat deteksi fraud, anomali, autentikasi adaptif, serta otomasi respons insiden. Teknologi seperti federated learning, differential privacy, dan homomorphic encryption juga membuka jalur untuk pemrosesan yang lebih menjaga privasi. Namun, AI secara bersamaan meningkatkan risiko over-collection,

function creep, inferensi atribut sensitif, kebocoran melalui model dan antarmuka, profiling yang tidak transparan, serta serangan berbasis generative AI.

Sintesis menghasilkan enam gerbang tata kelola yang menghubungkan bukti teknis dan perilaku konsumen dengan kewajiban hukum: legalitas/minimisasi, privacy/security by design, model assurance, transparansi dan kontrol, human oversight, serta audit dan respons insiden. Perspektif amanah, keadilan, kemaslahatan, dan pencegahan mudarat menjadi dimensi etika Islam yang melintasi keenam gerbang tersebut. Kontribusi baru kajian terletak pada pemetaan kontrol dan bukti audit yang dapat diturunkan dari kerangka, bukan pada penemuan teknik keamanan atau klaim efektivitas empiris yang belum diuji.

Kerangka berpotensi mendukung praktik layanan digital di Indonesia melalui inventaris data, pengujian risiko model, dokumentasi keputusan, dan mekanisme pemenuhan hak konsumen. Batasannya terletak pada sifat konseptual, heterogenitas sumber, serta tidak tersedianya catatan lengkap hasil penyaringan literatur awal. Penelitian mendatang perlu mendokumentasikan penelusuran sistematis yang replikabel serta menguji pengaruh tiap gerbang pada penurunan risiko kebocoran, utilitas model, kepercayaan konsumen, dan biaya implementasi pada sektor spesifik.

References

Abdirahman, A. A., Hashi, A. O., Dahir, U. M., et al. (2026). HE-CloudML: A privacy-preserving framework for secure machine learning inference over encrypted cloud data using homomorphic encryption. Scientific Reports. https://doi.org/10.1038/s41598-026-69466-7

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Alabdulatif, A. (2025). GuardianAI: Privacy-preserving federated anomaly detection with differential privacy. Array, 26, 100381. https://doi.org/10.1016/j.array.2025.100381

Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: An exploration into possible solutions. Cogent Business & Management, 11(1), 2393743. https://doi.org/10.1080/23311975.2024.2393743

Bozorgpanah, A., & Torra, V. (2024). Explainable machine learning models with privacy. Progress in Artificial Intelligence, 13, 31–50. https://doi.org/10.1007/s13748-024-00315-2

Brough, A. R. (2026). When the vault is never opened: AI-enabled inference and the future of consumer privacy. Consumer Psychology Review. Advance online publication. https://doi.org/10.1002/arcp.70014

Bunko, T., Johnstone, M. N., Yang, W., & Scott, B. A. (2026). A survey of privacy-preserving federated learning for intrusion detection systems. Artificial Intelligence Review, 59, 125. https://doi.org/10.1007/s10462-026-11519-4

Cai, H., & Mardani, A. (2023). Research on the impact of consumer privacy and intelligent personalization technology on purchase resistance. Journal of Business Research, 161, 113811. https://doi.org/10.1016/j.jbusres.2023.113811

Cloarec, J. (2022). Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. Journal of Business Research, 152, 144–153. https://doi.org/10.1016/j.jbusres.2022.07.045

Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. Journal of the Academy of Marketing Science, 48, 24–42. https://doi.org/10.1007/s11747-019-00696-0

Gorian, E., & Osman, N. D. (2024). Digital ethics of artificial intelligence (AI) in Saudi Arabia and United Arab Emirates. Malaysian Journal of Syariah and Law, 12(3), 583–597. https://doi.org/10.33102/mjsl.vol12no3.798

Habib, Z. (2025). Ethics of artificial intelligence in Maqāṣid al-Sharīa's perspective. KARSA Journal of Social and Islamic Culture, 33(1), 105–134. https://ejournal.uinmadura.ac.id/index.php/karsa/article/view/19617

Huang, M.-H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. Journal of the Academy of Marketing Science, 49, 30–50. https://doi.org/10.1007/s11747-020-00749-9

Judijanto, L., Basri, T. S., Harsya, R. M. K., Vandika, A. Y., & Utama, A. S. (2024). Kajian hukum dampak kecerdasan buatan terhadap perlindungan privasi data dalam hukum siber Indonesia. Sanskara Hukum dan HAM, 3(2). https://doi.org/10.58812/shh.v3i02.498

Junaidi, & Fadzil, R. M. (2024). Urgency of legal personal data protection in e-commerce transactions involving artificial intelligence. Walisongo Law Review, 6(2). https://doi.org/10.21580/walrev.2024.6.2.25548

Jurewicz, M., Klein Kafer, N., & Kran, E. (2024). Artificial intelligence and privacy: Causes for concern. Privacy Studies Journal, 3, 1–32. https://doi.org/10.7146/psj.v3i.143099

Kelleher, J. D. (2019). Deep learning. MIT Press.

Liu, Y., Huang, J., Li, Y., Wang, D., & Xiao, B. (2025). Generative AI model privacy: A survey. Artificial Intelligence Review, 58, 33. https://doi.org/10.1007/s10462-024-11024-6

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. Journal of Business Research, 122, 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006

Martin, K. D., & Zimmermann, J. (2024). Artificial intelligence and its implications for data privacy. Current Opinion in Psychology, 58, 101829. https://doi.org/10.1016/j.copsyc.2024.101829

Nguyen, T. T., Huynh, T. T., Ren, Z., Nguyen, T. T., Nguyen, P. L., Yin, H., & Nguyen, Q. V. H. (2025). Privacy-preserving explainable AI: A survey. Science China Information Sciences, 68, 111101. https://doi.org/10.1007/s11432-024-4123-4

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.

Papagni, G., de Pagter, J., Zafari, S., Filzmoser, M., & Koeszegi, S. T. (2023). Artificial agents' explainability to support trust: Considerations on timing and context. AI & Society, 38, 947–960. https://doi.org/10.1007/s00146-022-01462-7

Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. Journal of Marketing, 85(1), 131–151. https://doi.org/10.1177/0022242920953847

Putra, T. I., Fakhis, A. Z. P., Tussaleha, A., Firdhausya, M. U., Aflah, M. H. N., Ezzerouali, S. A., & Banane, M. C. (2024). Legal gaps and risks in consumer data processing: An analysis of Indonesian e-commerce under the Personal Data Protection Law. Journal of Private and Commercial Law, 8(2), 199–230. https://doi.org/10.15294/jpcl.v8i2.20081

Russell, S. J., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

Shuqair, S., Pinto, D. C., Lancelot Miltgen, C., & Viglia, G. (2024). When powerful artificial intelligence backfires. International Journal of Hospitality Management, 120, 103778. https://doi.org/10.1016/j.ijhm.2024.103778

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Swani, K., Milne, G. R., & Brown, B. P. (2023). The benefits of meeting buyer privacy expectations across information, time, and space dimensions. Industrial Marketing Management, 112, 14–26. https://doi.org/10.1016/j.indmarman.2023.04.013

Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. Journal of Advanced Nursing, 52(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x

Wicaksana, K. P., Alfath, T. P., & Kuswanto, H. (2026). Personal data protection in the digital era: A Maqasid al-Shariah perspective on contemporary legal challenges. MIZAN: Journal of Islamic Law, 10(1), 114–122. https://doi.org/10.32832/mizan.v14i1.24363

Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. Telecommunications Policy, 48, 102851. https://doi.org/10.1016/j.telpol.2024.102851

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.