CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

IMPLIKASI HUKUM PEMANFAATAN ARTIFICIAL INTELLIGENCE TERHADAP HAK PRIVASI PENGGUNA

Anisya Auriana Dewi[1], Sabrina Tamala[2], Dewi Asri Puannandini[3]
Ilmu Hukum Fakultas Hukum Universitas Islam Nusantara, Kota Bandung, 40286, Indonesia

E-mail: nisyaauriana@gmail.com, tamalasabrina@gmail.com, dewipuannandini@gmail.com

Abstract: Pesatnya perkembangan dan pemanfaatan Artificial Intelligence (AI) dalam berbagai sektor publik dan swasta menimbulkan tantangan hukum yang signifikan, khususnya terkait dengan perlindungan hak privasi pengguna. AI bekerja dengan mengandalkan pengolahan data pribadi dalam skala besar, termasuk data perilaku, preferensi, dan biometrik, yang berpotensi menimbulkan pelanggaran hak privasi apabila tidak diatur secara memadai. Artikel ini bertujuan untuk menganalisis implikasi hukum pemanfaatan Artificial Intelligence terhadap hak privasi pengguna dalam perspektif hukum positif Indonesia. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan hukum, melalui kajian terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta perbandingan dengan rezim hukum Uni Eropa, khususnya General Data Protection Regulation dan EU Artificial Intelligence Act. Hasil kajian menunjukkan bahwa meskipun Undang-Undang Perlindungan Data Pribadi telah memberikan landasan normatif penting bagi perlindungan data pribadi, pengaturan tersebut belum secara spesifik mengantisipasi karakteristik dan risiko khas Artificial Intelligence, seperti pengambilan keputusan otomatis, profiling, dan kurangnya transparansi algoritmik. Oleh karena itu, diperlukan penguatan regulasi dan kebijakan hukum Artificial Intelligence yang berbasis perlindungan hak privasi guna menjamin keseimbangan antara inovasi teknologi dan perlindungan hak asasi manusia dalam kerangka negara hukum.

Keywords: Regulasi Artificial Intelligence, Perlindungan Hak Privasi, Hukum Perlindungan Data Pribadi, Pengambilan Keputusan Otomatis, Artificial Intelligence Berpusat Pada Manusia

Article History
Received: Januari 2026
Reviewed: Januari 2026
Published: Januari 2026

Plagirism checker no 631
Doi : prefix doi :
10.8734/causa.v1i2.365
Copyright : author
Publish by : causa

This work is licensed under a creative commons attribution-noncommercial 4.0 international license

A. PENDAHULUAN

Perkembangan teknologi digital dewasa ini ditandai dengan pemanfaatan Artificial Intelligence (AI) yang semakin masif dan sistemik dalam berbagai sektor kehidupan manusia, mulai dari layanan keuangan, kesehatan, pendidikan, transportasi, pemerintahan, hingga media sosial dan platform digital berbasis ekonomi data. AI tidak lagi berfungsi sebagai alat bantu teknis semata, melainkan telah menjadi sistem otonom yang mampu melakukan pengambilan keputusan, pembelajaran mandiri (*machine learning*), serta analisis prediktif berbasis data dalam skala besar (*big data*).[1] Pemanfaatan AI meliputi pengolahan data pribadi, analisis perilaku pengguna, pengenalan wajah (*facial recognition*), pemrosesan bahasa alami (*natural language*

[1] Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). New Jersey: Pearson Education, p. 1–5.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

processing), serta sistem rekomendasi dan penilaian otomatis (*automated decision-making systems*).

Di satu sisi, pemanfaatan AI membawa manfaat signifikan berupa efisiensi, kecepatan layanan, peningkatan akurasi analisis, dan inovasi di berbagai sektor strategis. Namun di sisi lain, penggunaan AI yang sangat bergantung pada data pribadi pengguna memunculkan berbagai tantangan hukum dan etika, khususnya yang berkaitan dengan perlindungan hak privasi pengguna. Ketergantungan AI terhadap pengumpulan dan pemrosesan data dalam jumlah besar menjadikan privasi sebagai aspek yang sangat rentan terlanggar, terutama ketika data diproses tanpa transparansi, tanpa persetujuan yang sah, atau digunakan untuk kepentingan komersial dan pengawasan yang berlebihan.

Hak privasi merupakan bagian integral dari hak asasi manusia yang dijamin secara konstitusional dan internasional. Di Indonesia, perlindungan hak privasi berakar pada Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menjamin perlindungan atas diri pribadi, keluarga, kehormatan, martabat, serta rasa aman setiap warga negara. Dalam perkembangan hukum internasional, hak privasi juga diakui dalam *Universal Declaration of Human Rights* dan *International Covenant on Civil and Political Rights*. Dalam konteks masyarakat digital, hak privasi mengalami transformasi makna, tidak lagi terbatas pada perlindungan fisik dan ruang personal, melainkan juga mencakup perlindungan data pribadi, identitas digital, dan jejak elektronik individu.

Pemanfaatan AI semakin memperbesar potensi pelanggaran hak privasi karena teknologi ini memungkinkan pengumpulan, pemrosesan, penyimpanan, dan distribusi data pribadi pengguna secara masif, otomatis, dan lintas batas negara. Sistem AI kerap bekerja secara *black box*, sehingga sulit dipahami bagaimana data diproses dan untuk tujuan apa data tersebut digunakan. Kondisi ini menimbulkan ketimpangan informasi (*information asymmetry*) antara pengguna sebagai subjek data dan penyedia layanan digital sebagai pengendali data.[2] Akibatnya, pengguna sering kali tidak memiliki kendali yang memadai atas data pribadinya sendiri.

Permasalahan menjadi semakin kompleks ketika AI digunakan untuk melakukan *profiling* dan prediksi perilaku pengguna tanpa adanya persetujuan yang jelas (*informed consent*). AI juga berpotensi menggunakan data pribadi di luar tujuan awal pengumpulan data (*function creep*), yang bertentangan dengan prinsip pembatasan tujuan (*purpose limitation*) dalam perlindungan data pribadi. Praktik ini tidak hanya berpotensi melanggar hak privasi, tetapi juga dapat menimbulkan diskriminasi algoritmik, penyalahgunaan data, serta praktik pengawasan massal (*mass surveillance*) yang mengancam kebebasan sipil dan demokrasi.[3]

Sejumlah penelitian terdahulu telah membahas hubungan antara perkembangan teknologi digital dan perlindungan data pribadi. Floridi et al. (2018) menekankan pentingnya pendekatan etika dalam pengembangan dan pemanfaatan AI untuk melindungi hak-hak fundamental individu. Zuboff (2019) memperkenalkan konsep *surveillance capitalism* untuk menggambarkan praktik eksploitasi data pribadi pengguna oleh korporasi digital yang berorientasi pada keuntungan ekonomi. Di tingkat regional, Uni Eropa telah mengadopsi General Data Protection Regulation (GDPR) sebagai instrumen hukum yang komprehensif dalam melindungi data pribadi, serta mengembangkan EU Artificial Intelligence Act yang menempatkan perlindungan hak fundamental sebagai prinsip utama pengaturan AI.

[2] Solove, D. J. (2021). *Understanding Privacy*. Cambridge: Harvard University Press, p. 102–110.
[3] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, p. 54–67.

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

Di Indonesia, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah penting dalam memperkuat perlindungan hak privasi di era digital. Sejumlah penelitian nasional telah mengkaji UU PDP dari perspektif normatif dan implementatif, namun sebagian besar masih berfokus pada aspek umum pengelolaan data pribadi dan belum secara khusus menelaah implikasi penggunaan AI terhadap hak privasi pengguna. Padahal, karakteristik AI yang bersifat otonom, adaptif, dan prediktif menimbulkan tantangan hukum yang berbeda dibandingkan dengan pengelolaan data konvensional.

Berdasarkan telaah literatur tersebut, terdapat gap analisis berupa belum optimalnya kajian hukum yang secara komprehensif mengaitkan pemanfaatan AI dengan perlindungan hak privasi pengguna dalam perspektif hukum positif Indonesia. Selain itu, masih terbatas penelitian yang mengkaji kecukupan UU PDP dan regulasi sektoral dalam menghadapi risiko pelanggaran privasi yang ditimbulkan oleh sistem AI, serta minimnya kajian perbandingan dengan praktik terbaik internasional (*best practices*) dalam pengaturan AI yang berorientasi pada perlindungan hak asasi manusia.

Urgensi kajian ini semakin menguat mengingat perkembangan pemanfaatan AI di Indonesia berlangsung jauh lebih cepat dibandingkan dengan kesiapan kerangka hukum, kelembagaan, dan mekanisme pengawasan yang tersedia. Tanpa regulasi yang adaptif, prinsip akuntabilitas algoritmik, serta penegakan hukum yang efektif, hak privasi pengguna berpotensi terdegradasi oleh kepentingan ekonomi, efisiensi teknologi, dan dominasi korporasi digital. Oleh karena itu, diperlukan analisis hukum yang mendalam dan sistematis guna memastikan bahwa pemanfaatan AI tetap berada dalam koridor negara hukum dan prinsip perlindungan hak asasi manusia.

Penelitian ini bertujuan untuk menganalisis implikasi hukum pemanfaatan Artificial Intelligence terhadap hak privasi pengguna dengan menelaah pengaturan hukum yang berlaku di Indonesia, mengidentifikasi potensi pelanggaran hak privasi akibat penggunaan AI, serta merumuskan rekomendasi penguatan regulasi dan kebijakan hukum di bidang teknologi informasi. Kebaruan (novelty) dari kajian ini terletak pada pendekatan analitis yang secara khusus mengintegrasikan kajian AI dengan rezim perlindungan data pribadi dan hak privasi pengguna dalam perspektif hukum Indonesia, sehingga diharapkan dapat memberikan kontribusi konseptual dan praktis bagi pengembangan hukum teknologi informasi yang responsif terhadap dinamika AI.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang memandang hukum sebagai seperangkat norma atau kaidah yang mengatur kehidupan bermasyarakat. Penelitian hukum normatif bertujuan untuk mengkaji asas hukum, sistematika peraturan perundang-undangan, tingkat harmonisasi norma, serta penerapan kaidah hukum dalam menjawab isu hukum tertentu. Dalam penelitian ini, pendekatan normatif digunakan untuk menganalisis implikasi hukum pemanfaatan Artificial Intelligence terhadap perlindungan hak privasi pengguna dengan bertumpu pada peraturan perundang-undangan, doktrin hukum, serta prinsip-prinsip hak asasi manusia.

1. Jenis Penelitian

   Jenis penelitian yang digunakan adalah penelitian hukum normatif dengan karakter preskriptif-analitis. Penelitian ini tidak hanya menguraikan norma hukum yang berlaku, tetapi juga menyusun argumentasi hukum serta memberikan rekomendasi normatif atas permasalahan yang dikaji. Melalui pendekatan tersebut, penelitian ini berupaya merumuskan

konstruksi hukum yang ideal guna memperkuat perlindungan hak privasi pengguna dalam konteks meningkatnya pemanfaatan teknologi Artificial Intelligence.

2. Metode Pendekatan

Pendekatan yang digunakan dalam penelitian ini meliputi:

a. Pendekatan Perundang-undangan *(statute approach)*

Pendekatan perundang-undangan dilakukan dengan mengkaji berbagai peraturan yang berkaitan dengan perlindungan data pribadi dan pemanfaatan teknologi informasi, antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta regulasi sektoral lainnya yang relevan. Pendekatan ini bertujuan untuk menilai kecukupan, konsistensi, dan efektivitas norma hukum dalam mengatur implikasi penggunaan AI terhadap hak privasi pengguna.

b. Pendekatan Konseptual *(conceptual approach)*

Pendekatan konseptual dilakukan dengan menelaah konsep, asas, dan doktrin hukum yang berkembang dalam literatur hukum, khususnya yang berkaitan dengan hak privasi, perlindungan data pribadi, pertanggungjawaban hukum, serta etika Artificial Intelligence. Pendekatan ini digunakan untuk membangun kerangka konseptual dalam memahami karakteristik AI dan dampaknya terhadap perlindungan hak asasi manusia.

c. Pendekatan Perbandingan *(comparative approach)*

Pendekatan perbandingan dilakukan dengan membandingkan pengaturan perlindungan data pribadi dan Artificial Intelligence di Indonesia dengan praktik pengaturan di tingkat internasional, khususnya General Data Protection Regulation (GDPR) dan kebijakan pengaturan AI di Uni Eropa. Pendekatan ini dimaksudkan untuk memperoleh perspektif komparatif sebagai dasar perumusan rekomendasi kebijakan hukum yang lebih adaptif dan relevan bagi Indonesia.

3. Sumber Bahan Hukum

Sumber bahan hukum yang digunakan dalam penelitian ini terdiri atas:

a. Bahan Hukum Primer, yaitu bahan hukum yang bersifat mengikat, meliputi peraturan perundang-undangan nasional dan instrumen hukum internasional yang berkaitan dengan perlindungan hak privasi dan data pribadi.

b. Bahan Hukum Sekunder, yaitu bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, berupa buku teks hukum, jurnal ilmiah nasional dan internasional, hasil penelitian, serta pendapat para ahli yang relevan dengan topik Artificial Intelligence dan hak privasi.

c. Bahan Hukum Tersier, yaitu bahan hukum pendukung yang memberikan penjelasan tambahan, seperti kamus hukum, ensiklopedia hukum, dan sumber informasi hukum lainnya.

4. Teknik Pengumpulan Bahan Hukum

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan cara menelusuri, menginventarisasi, dan mengkaji peraturan perundang-undangan, literatur hukum, jurnal ilmiah, serta dokumen kebijakan yang relevan. Penelusuran bahan hukum dilakukan secara sistematis guna menjamin kelengkapan dan relevansi data dengan isu hukum yang dianalisis.

5. Teknik Analisis Bahan Hukum

Analisis bahan hukum dilakukan secara kualitatif normatif, yaitu dengan menafsirkan norma dan doktrin hukum melalui penalaran hukum (*legal reasoning*). Seluruh bahan hukum yang telah dikumpulkan dianalisis secara sistematis untuk menjawab permasalahan

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

penelitian, mengidentifikasi kelemahan pengaturan hukum yang ada, serta merumuskan rekomendasi penguatan perlindungan hak privasi pengguna dalam pemanfaatan Artificial Intelligence. Hasil analisis disajikan secara deskriptif-argumentatif dengan penarikan kesimpulan secara deduktif.

C. PEMBAHASAN

1. Pemanfaatan Artificial Intelligence dalam Pengolahan Data Pribadi Pengguna

Pemanfaatan Artificial Intelligence (AI) dalam ekosistem digital modern sangat bergantung pada ketersediaan dan pengolahan data pribadi pengguna dalam skala besar (*big data-driven technology*). AI bekerja melalui mekanisme pengumpulan (*data collection*), pemrosesan (*data processing*), dan analisis data secara otomatis untuk menghasilkan pola, prediksi, serta rekomendasi yang bersifat adaptif dan berkelanjutan. Kemampuan AI untuk melakukan pembelajaran mandiri (*machine learning*) menjadikan data pribadi sebagai elemen fundamental yang menentukan tingkat akurasi dan efektivitas sistem AI itu sendiri.[4]

Dalam konteks ini, data pribadi tidak lagi dipahami secara sempit sebagai informasi identitas dasar, seperti nama atau alamat, melainkan mencakup spektrum data yang jauh lebih luas, termasuk data perilaku, preferensi konsumsi, riwayat pencarian, lokasi geografis, data biometrik, hingga pola interaksi digital pengguna.[5] Data-data tersebut memungkinkan AI membangun *digital profile* yang merepresentasikan karakteristik dan kecenderungan individu secara mendalam. Profiling semacam ini memberikan keuntungan ekonomi dan efisiensi bagi penyedia layanan digital, namun sekaligus meningkatkan risiko pelanggaran hak privasi pengguna apabila tidak diatur secara ketat oleh hukum.

Dari perspektif hukum, pengolahan data pribadi oleh AI menimbulkan persoalan krusial terkait prinsip pengendalian data (*data controllership*). Pengguna sebagai subjek data sering kali tidak memiliki pemahaman yang memadai mengenai bagaimana data pribadinya dikumpulkan, dianalisis, dan digunakan oleh sistem AI. Kondisi ini menciptakan ketimpangan relasi kuasa (*power imbalance*) antara pengguna dan pengendali data, yang bertentangan dengan prinsip transparansi dan persetujuan yang sah (*informed consent*) dalam perlindungan data pribadi.

Selain itu, karakteristik AI yang bekerja secara otomatis dan kompleks (*algorithmic complexity*) menyebabkan proses pengambilan keputusan menjadi sulit dijelaskan (*lack of explainability*). Fenomena ini dikenal sebagai *algorithmic opacity* atau *black box*, di mana pengguna tidak dapat mengetahui dasar pertimbangan sistem AI dalam memproses data pribadinya. Dalam konteks hak privasi, ketertutupan algoritma tersebut berpotensi melanggar hak individu untuk mengetahui, mengakses, dan mengendalikan penggunaan data pribadinya sebagaimana diakui dalam doktrin perlindungan data modern.

Dengan demikian, pemanfaatan AI dalam pengolahan data pribadi pengguna tidak hanya merupakan isu teknologis, tetapi juga isu hukum yang berkaitan erat dengan perlindungan hak asasi manusia. Tanpa kerangka hukum yang memadai, penggunaan AI berpotensi menggeser hak privasi dari hak fundamental menjadi sekadar komoditas digital yang dapat dieksploitasi untuk kepentingan ekonomi dan pengawasan. Oleh karena itu, penguatan

[4] Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). New Jersey: Pearson Education, p. 28–35.
[5] Solove, D. J. (2021). *Understanding Privacy*. Cambridge: Harvard University Press, p. 101–108.

regulasi dan prinsip hukum yang berorientasi pada perlindungan hak privasi menjadi kebutuhan mendesak dalam menghadapi perkembangan AI yang semakin kompleks.

a. Karakteristik Pengolahan Data Pribadi oleh Sistem AI

Pengolahan data pribadi oleh sistem Artificial Intelligence memiliki karakteristik utama berupa otomatisasi penuh, kompleksitas algoritmik, dan kemampuan pembelajaran mandiri (*self-learning*). Berbeda dengan sistem teknologi informasi konvensional yang bekerja berdasarkan instruksi statis, AI mampu memperbarui model analisisnya secara dinamis berdasarkan data baru yang diproses. Kemampuan ini memungkinkan AI untuk menghasilkan keputusan dan rekomendasi yang semakin presisi, namun sekaligus memperluas ruang lingkup pengolahan data pribadi tanpa intervensi manusia secara langsung.

Karakteristik otomatisasi dalam AI menyebabkan proses pengumpulan dan pemrosesan data berlangsung secara terus-menerus (*continuous data processing*), sering kali tanpa disadari oleh pengguna sebagai subjek data. Dalam banyak kasus, pengguna hanya memberikan persetujuan awal yang bersifat umum, sementara pemrosesan lanjutan dilakukan oleh sistem AI untuk tujuan-tujuan baru yang tidak selalu diinformasikan secara jelas. Praktik ini berpotensi bertentangan dengan prinsip pembatasan tujuan (*purpose limitation*) dan minimasi data (*data minimization*) yang menjadi pilar utama perlindungan data pribadi.

Selain itu, kompleksitas algoritmik AI melahirkan fenomena ketertutupan algoritma (*algorithmic opacity*), yakni kondisi di mana proses pengambilan keputusan oleh AI sulit dipahami, baik oleh pengguna maupun oleh pengendali sistem itu sendiri. Sistem AI kerap berfungsi sebagai *black box* yang hanya menampilkan hasil akhir tanpa penjelasan memadai mengenai dasar pertimbangan pemrosesan data pribadi. Ketertutupan ini menimbulkan persoalan hukum serius karena menghambat hak pengguna untuk memperoleh informasi, mengakses data, dan meminta pertanggungjawaban atas pemrosesan data pribadinya.

Kemampuan *self-learning* pada AI juga memunculkan risiko eskalasi penggunaan data pribadi secara tidak proporsional. AI dapat mengombinasikan berbagai kategori data untuk membangun profil pengguna yang semakin detail dan sensitif, termasuk data yang semula tidak dikategorikan sebagai data pribadi sensitif. Kondisi ini meningkatkan potensi pelanggaran hak privasi, diskriminasi algoritmik, serta penggunaan data di luar tujuan awal pengumpulan (*function creep*).

Dengan demikian, karakteristik pengolahan data pribadi oleh sistem AI menunjukkan bahwa risiko pelanggaran hak privasi tidak hanya bersumber dari niat jahat pengendali data, tetapi juga dari desain dan cara kerja teknologi itu sendiri. Oleh karena itu, penulis berpandangan bahwa pengaturan hukum terhadap AI harus memperhatikan aspek teknis algoritma dan menempatkan prinsip transparansi, akuntabilitas, serta pengawasan manusia (*human oversight*) sebagai syarat utama dalam pemanfaatan AI yang menghormati hak privasi pengguna.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

b. Risiko Hukum dalam Penggunaan Data Pribadi oleh AI

Pemanfaatan Artificial Intelligence dalam pengolahan data pribadi pengguna menimbulkan berbagai risiko hukum yang bersifat struktural dan sistemik. Risiko pertama berkaitan dengan pengumpulan data pribadi tanpa dasar hukum yang sah, baik karena tidak adanya persetujuan yang jelas dari subjek data maupun karena persetujuan diberikan secara umum dan tidak spesifik. Dalam praktik, pengguna sering kali hanya menyetujui *terms and conditions* yang bersifat baku tanpa pemahaman memadai mengenai jenis data yang dikumpulkan dan tujuan pemrosesannya. Kondisi ini berpotensi melanggar prinsip legalitas dan persetujuan yang sah (*lawful and informed consent*) dalam perlindungan data pribadi.

Risiko berikutnya adalah pemrosesan data pribadi di luar tujuan awal pengumpulan data (*function creep*). Sistem AI, melalui kemampuan pembelajaran mandiri dan analisis lintas data, kerap menggunakan data pribadi untuk tujuan baru yang tidak diinformasikan kepada pengguna sejak awal. Praktik ini bertentangan dengan prinsip pembatasan tujuan (*purpose limitation*) dan prinsip keadilan (*fairness*) yang menjadi fondasi doktrin hukum privasi modern. Apabila tidak dikendalikan, penggunaan data di luar tujuan awal berpotensi menimbulkan penyalahgunaan data dan pelanggaran hak privasi secara sistematis.

Selain itu, pengambilan keputusan otomatis (*automated decision-making*) oleh AI menimbulkan risiko hukum yang signifikan ketika keputusan tersebut berdampak langsung terhadap hak dan kepentingan individu, seperti penentuan kelayakan kredit, rekrutmen tenaga kerja, atau penilaian risiko hukum. Keputusan otomatis yang tidak disertai mekanisme peninjauan manusia (*human intervention*) dapat melanggar prinsip akuntabilitas dan hak atas perlakuan yang adil. Dalam perspektif hak asasi manusia, individu berhak mengetahui dasar pengambilan keputusan yang memengaruhi dirinya serta memiliki kesempatan untuk mengajukan keberatan.

Lebih lanjut, kompleksitas algoritma AI juga meningkatkan risiko diskriminasi algoritmik, yaitu perlakuan berbeda terhadap individu atau kelompok tertentu berdasarkan data historis yang bias. Diskriminasi semacam ini sulit dideteksi karena tersembunyi di balik proses algoritmik yang tidak transparan. Praktik diskriminasi algoritmik tidak hanya melanggar prinsip non-diskriminasi, tetapi juga berpotensi menimbulkan tanggung jawab hukum bagi pengendali data dan pengembang sistem AI.

Dengan demikian, risiko hukum dalam penggunaan data pribadi oleh AI mencerminkan adanya ketegangan antara kepentingan inovasi teknologi dan perlindungan hak privasi pengguna. Penulis berpandangan bahwa tanpa kerangka hukum yang tegas, mekanisme pengawasan yang efektif, serta prinsip akuntabilitas algoritmik, pemanfaatan AI berpotensi mereduksi hak privasi menjadi sekadar instrumen ekonomi. Oleh karena itu, penguatan regulasi dan penerapan prinsip *privacy by design* dan *privacy by default* menjadi keharusan dalam pemanfaatan AI yang berorientasi pada perlindungan hak asasi manusia.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

2. Implikasi Pemanfaatan Artificial Intelligence terhadap Hak Privasi Pengguna

Pemanfaatan Artificial Intelligence menimbulkan implikasi hukum yang signifikan terhadap hak privasi pengguna, terutama karena teknologi ini beroperasi dengan logika prediktif yang mampu memengaruhi hak dan kebebasan individu secara langsung. AI tidak hanya berfungsi sebagai alat bantu pengambilan keputusan, tetapi juga sebagai aktor yang menentukan bagaimana data pribadi diklasifikasikan, dianalisis, dan dimanfaatkan untuk tujuan tertentu. Kondisi ini menjadikan privasi sebagai aspek yang sangat rentan terdegradasi apabila tidak diimbangi dengan perlindungan hukum yang memadai.

Implikasi tersebut semakin nyata ketika AI digunakan untuk membentuk profil digital pengguna (*digital profiling*) yang mencerminkan preferensi, perilaku, dan kecenderungan personal seseorang. Profil digital ini dapat digunakan untuk memengaruhi pilihan individu, membatasi akses terhadap layanan tertentu, atau bahkan menentukan perlakuan hukum dan administratif yang diterima oleh pengguna. Dalam perspektif hukum hak asasi manusia, praktik tersebut berpotensi mengancam prinsip otonomi individu (*individual autonomy*) dan martabat manusia (*human dignity*), yang merupakan inti dari perlindungan hak privasi.

Selain itu, penggunaan AI dalam pengawasan digital dan pengambilan keputusan otomatis berpotensi memperluas praktik pengawasan yang bersifat invasif dan tidak proporsional. AI memungkinkan pemantauan aktivitas individu secara terus-menerus dan sistematis, sehingga batas antara kepentingan publik dan ruang privat menjadi semakin kabur. Apabila pengawasan berbasis AI tidak diatur secara ketat, maka hak privasi berisiko direduksi menjadi sekadar hak formal tanpa perlindungan substantif. Oleh karena itu, implikasi pemanfaatan AI terhadap hak privasi pengguna perlu dianalisis lebih lanjut melalui identifikasi bentuk-bentuk konkret pelanggaran privasi serta pengujian kecukupan instrumen hukum yang tersedia.

Berdasarkan uraian tersebut, pembahasan selanjutnya akan difokuskan pada analisis implikasi spesifik pemanfaatan AI terhadap hak privasi pengguna, yang meliputi praktik *profiling* dan pengambilan keputusan otomatis, serta penggunaan AI dalam pengawasan massal dan dampaknya terhadap perlindungan hak privasi.

a. Profiling dan Pengambilan Keputusan Otomatis

Artificial Intelligence memungkinkan dilakukannya profiling, yaitu pemrosesan data pribadi secara sistematis untuk mengevaluasi atau memprediksi aspek-aspek tertentu dari kehidupan seseorang, seperti perilaku, preferensi, kondisi ekonomi, kesehatan, hingga kecenderungan sosial. Profiling berbasis AI dilakukan melalui analisis korelatif atas berbagai jenis data yang dikombinasikan, sehingga menghasilkan gambaran digital individu yang sangat rinci (*granular digital identity*). Dalam praktiknya, profiling tidak hanya digunakan untuk tujuan personalisasi layanan, tetapi juga untuk pengambilan keputusan yang berdampak langsung terhadap hak dan kepentingan individu.

Penggunaan profiling oleh AI menjadi bermasalah ketika dilakukan tanpa persetujuan eksplisit dan spesifik (*explicit informed consent*) dari subjek data. Persetujuan yang bersifat umum dan tidak transparan tidak memenuhi standar perlindungan hak privasi, karena pengguna tidak mengetahui secara pasti bagaimana data pribadinya dianalisis dan untuk tujuan apa hasil profiling digunakan. Kondisi ini berpotensi melanggar prinsip

keadilan (*fairness*) dan transparansi (*transparency*) dalam doktrin perlindungan data pribadi modern.

Implikasi hukum semakin kompleks ketika profiling menjadi dasar pengambilan keputusan otomatis (*automated decision-making*) yang berdampak signifikan terhadap individu, seperti penentuan kelayakan kredit, seleksi tenaga kerja, penetapan premi asuransi, atau pemeringkatan risiko. Keputusan otomatis yang sepenuhnya diserahkan kepada AI tanpa mekanisme peninjauan manusia (*human review*) berpotensi meniadakan hak individu untuk mendapatkan penjelasan dan keberatan. Dalam perspektif hukum, kondisi ini bertentangan dengan prinsip akuntabilitas dan hak atas perlakuan yang adil.

Lebih jauh, profiling berbasis AI berisiko menimbulkan diskriminasi algoritmik apabila data yang digunakan mengandung bias historis atau struktural. AI dapat mereproduksi dan bahkan memperkuat ketidakadilan sosial melalui keputusan yang tampak netral secara teknis, namun diskriminatif secara substansial. Praktik diskriminasi algoritmik bertentangan dengan prinsip non-diskriminasi dan perlindungan martabat manusia, yang merupakan prinsip fundamental dalam hukum hak asasi manusia.[4] Oleh karena itu, penulis berpandangan bahwa profiling dan pengambilan keputusan otomatis oleh AI harus dibatasi secara ketat melalui pengaturan hukum yang menjamin persetujuan yang sah, transparansi algoritmik, serta hak pengguna atas intervensi manusia.

b. Pengawasan Massal dan Erosi Hak Privasi

Pemanfaatan Artificial Intelligence dalam teknologi pengenalan wajah (*facial recognition*), pelacakan lokasi, dan analisis perilaku digital telah membuka peluang terjadinya pengawasan massal (*mass surveillance*) yang bersifat sistematis dan berkelanjutan. Berbeda dengan bentuk pengawasan konvensional, pengawasan berbasis AI memungkinkan pemantauan individu dalam skala luas, real time, dan lintas ruang, tanpa memerlukan keterlibatan manusia secara langsung. Teknologi ini mampu mengidentifikasi, melacak, dan mengaitkan berbagai aktivitas individu dengan tingkat akurasi yang tinggi, sehingga ruang privat pengguna menjadi semakin tereduksi.[1]

David Lyon menyatakan bahwa pengawasan berbasis teknologi digital telah mentransformasi privasi dari hak individual menjadi komoditas yang dapat dikumpulkan, dianalisis, dan diperdagangkan untuk kepentingan ekonomi maupun politik.[6] Dalam konteks ini, data pribadi pengguna menjadi sumber daya strategis yang dieksploitasi melalui sistem AI untuk kepentingan keamanan, pemasaran, maupun pengendalian sosial. Kondisi tersebut menunjukkan adanya pergeseran paradigma, di mana pengawasan tidak lagi bersifat pengecualian, melainkan menjadi praktik yang dilembagakan dalam kehidupan digital sehari-hari.

Dari perspektif negara hukum, praktik pengawasan massal berbasis AI menimbulkan persoalan serius apabila dilakukan tanpa dasar hukum yang jelas, pembatasan tujuan yang ketat, serta prinsip proporsionalitas. Pengawasan yang tidak terkontrol berpotensi melanggar hak privasi, kebebasan berekspresi, dan kebebasan bergerak, yang merupakan bagian dari kebebasan sipil yang dilindungi secara konstitusional. Dalam sistem demokrasi, pengawasan massal yang berlebihan juga dapat menciptakan efek *chilling*

[6] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, p. 21–30.

effect, yaitu kondisi di mana individu membatasi perilakunya karena merasa selalu diawasi.

Lebih lanjut, penggunaan AI dalam pengawasan publik sering kali tidak disertai mekanisme akuntabilitas dan pengawasan independen yang memadai. Ketertutupan algoritma dan minimnya transparansi memperlemah kemampuan masyarakat untuk mengawasi penggunaan teknologi tersebut. Oleh karena itu, penulis berpandangan bahwa pengawasan berbasis AI hanya dapat dibenarkan secara hukum apabila memenuhi prinsip legalitas, kebutuhan yang sah (*legitimate aim*), dan proporsionalitas, serta dilengkapi dengan mekanisme perlindungan hak privasi yang efektif. Tanpa pembatasan tersebut, pengawasan massal berbasis AI berpotensi menggerus sendi-sendi negara hukum dan demokrasi.

3. Perlindungan Hak Privasi Pengguna dalam Hukum Positif Indonesia

Perlindungan hak privasi di Indonesia mengalami penguatan signifikan dengan diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini menjadi landasan normatif utama dalam mengatur seluruh siklus pengolahan data pribadi, mulai dari pengumpulan, pemrosesan, penyimpanan, hingga penghapusan data, termasuk pengolahan yang dilakukan melalui sistem berbasis Artificial Intelligence. Kehadiran UU PDP menandai pergeseran paradigma hukum nasional dari perlindungan sektoral menuju perlindungan data pribadi yang bersifat komprehensif dan lintas sektor.[1]

Secara normatif, UU PDP mengadopsi prinsip-prinsip perlindungan data pribadi yang sejalan dengan standar internasional, seperti prinsip legalitas, pembatasan tujuan, minimalisasi data, akurasi, keamanan, dan akuntabilitas. Prinsip-prinsip tersebut menjadi instrumen hukum penting dalam mengendalikan pemanfaatan AI yang cenderung bersifat eksesif dan invasif terhadap privasi pengguna. Dalam konteks AI, prinsip pembatasan tujuan dan akuntabilitas memiliki peran krusial untuk mencegah praktik pemrosesan data di luar tujuan awal serta memastikan adanya pihak yang bertanggung jawab atas keputusan yang dihasilkan oleh sistem otomatis.[2]

Selain itu, UU PDP secara eksplisit mengakui hak subjek data, seperti hak atas informasi, hak akses, hak koreksi, hak penghapusan, dan hak untuk menolak pemrosesan data tertentu. Pengakuan hak-hak ini menjadi bentuk perlindungan preventif dan represif terhadap potensi pelanggaran hak privasi akibat penggunaan AI. Namun demikian, implementasi hak-hak tersebut dalam praktik pemrosesan data berbasis AI masih menghadapi tantangan, terutama terkait keterbatasan transparansi algoritma dan kesulitan menjelaskan logika pengambilan keputusan otomatis (*explainability*).[3] Kondisi ini menunjukkan bahwa meskipun kerangka hukum telah tersedia, efektivitas perlindungan hak privasi sangat bergantung pada pengaturan teknis dan penegakan hukum yang konsisten.

a. Prinsip Perlindungan Data Pribadi dalam UU PDP

UU PDP mengatur seperangkat prinsip fundamental dalam perlindungan data pribadi, antara lain prinsip legalitas, pembatasan tujuan, minimasi data, akurasi, keamanan, dan akuntabilitas, yang wajib dipatuhi oleh setiap pengendali dan prosesor data pribadi. Prinsip-prinsip ini berfungsi sebagai norma dasar (normative safeguards) untuk memastikan bahwa pengolahan data pribadi dilakukan secara sah, proporsional, dan

tidak melampaui kepentingan subjek data. Dalam konteks pemanfaatan Artificial Intelligence, prinsip legalitas dan pembatasan tujuan menjadi sangat penting mengingat AI bekerja dengan mekanisme pembelajaran berkelanjutan (*continuous learning*) yang berpotensi memperluas tujuan pemrosesan data di luar maksud awal pengumpulan.[7]

Secara substansial, prinsip-prinsip yang diatur dalam UU PDP menunjukkan keselarasan dengan rezim perlindungan data internasional, khususnya General Data Protection Regulation (GDPR) Uni Eropa, yang menempatkan perlindungan hak fundamental sebagai inti pengaturan pemrosesan data pribadi. Prinsip minimasi data dan akurasi, misalnya, menjadi instrumen penting untuk membatasi kecenderungan sistem AI dalam mengumpulkan dan mengolah data secara eksesif (*data over-collection*), serta mencegah pengambilan keputusan berbasis data yang tidak relevan atau bias. Dengan demikian, prinsip-prinsip tersebut secara teoritis dapat menjadi mekanisme pengendalian risiko pelanggaran hak privasi akibat penggunaan AI.

Namun demikian, UU PDP belum secara eksplisit mengatur karakteristik khusus sistem AI, seperti pengambilan keputusan otomatis (automated decision-making), profiling, dan transparansi algoritmik. Ketiadaan pengaturan khusus ini berpotensi menimbulkan celah hukum, terutama dalam hal pertanggungjawaban atas keputusan yang dihasilkan oleh sistem AI yang bersifat otonom dan sulit dijelaskan (*black box problem*). Tanpa kewajiban hukum yang jelas mengenai keterjelasan logika algoritma dan mekanisme pengawasan manusia (*human oversight*), prinsip akuntabilitas dalam UU PDP berisiko menjadi normatif semata dan sulit diterapkan secara efektif dalam praktik pemanfaatan AI.

b. Kelemahan Normatif dalam Menghadapi Tantangan AI

Ketiadaan pengaturan spesifik mengenai Artificial Intelligence dalam UU PDP menimbulkan celah hukum (legal gap) yang signifikan, terutama dalam mengantisipasi karakteristik AI yang bersifat otonom, adaptif, dan berbasis pembelajaran mesin. UU PDP masih berangkat dari paradigma pengolahan data konvensional yang mengasumsikan adanya kontrol langsung manusia dalam setiap tahapan pemrosesan data. Padahal, dalam sistem AI modern, keputusan dapat dihasilkan secara otomatis tanpa intervensi manusia (*fully automated decision-making*), sehingga menimbulkan persoalan serius terkait penentuan subjek hukum yang bertanggung jawab atas akibat hukum dari keputusan tersebut.

Kelemahan normatif ini semakin terlihat dalam absennya pengaturan mengenai mekanisme pengawasan algoritma (algorithmic oversight) dan kewajiban transparansi logika pengambilan keputusan AI. UU PDP belum mengatur secara tegas hak subjek data untuk memperoleh penjelasan yang bermakna (*meaningful explanation*) atas keputusan otomatis yang berdampak signifikan terhadap dirinya. Kondisi ini berpotensi mengurangi efektivitas prinsip akuntabilitas dan membuka ruang terjadinya pelanggaran hak privasi

[7] European Union. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679)*. Official Journal of the European Union, L119, 1–88.

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

yang bersifat sistemik, mengingat kompleksitas algoritma AI sering kali sulit dipahami bahkan oleh pengembangnya sendiri.[8]

Selain itu, UU PDP juga belum memberikan pengaturan yang memadai terkait pembagian tanggung jawab antara pengendali data, prosesor data, dan pengembang sistem AI. Dalam praktik, kegagalan sistem AI dapat disebabkan oleh berbagai faktor, seperti desain algoritma yang bias, kualitas data pelatihan yang buruk, atau penggunaan sistem di luar konteks awal perancangannya. Tanpa norma yang jelas mengenai alokasi tanggung jawab hukum, upaya penegakan hukum terhadap pelanggaran hak privasi berpotensi mengalami hambatan serius. Hal ini berbeda dengan pendekatan Uni Eropa yang mulai mengadopsi regulasi berbasis risiko melalui EU Artificial Intelligence Act, yang secara eksplisit mengklasifikasikan tingkat risiko AI dan menetapkan kewajiban hukum yang proporsional.

Oleh karena itu, kelemahan normatif dalam UU PDP menuntut adanya pengembangan regulasi turunan dan kebijakan sektoral yang lebih adaptif terhadap perkembangan AI. Regulasi tersebut tidak hanya harus memperkuat perlindungan hak privasi pengguna, tetapi juga memastikan kepastian hukum bagi pelaku usaha dan pengembang teknologi. Tanpa langkah normatif yang progresif, pemanfaatan AI berpotensi berjalan lebih cepat daripada kemampuan hukum untuk mengendalikannya, sehingga mengancam prinsip negara hukum dan perlindungan hak asasi manusia dalam ruang digital.[9]

4. Perbandingan Pengaturan Perlindungan Hak Privasi dalam Pemanfaatan AI

Pendekatan perbandingan hukum (*comparative legal approach*) diperlukan untuk menilai kecukupan dan efektivitas pengaturan nasional dalam melindungi hak privasi pengguna di tengah pesatnya pemanfaatan Artificial Intelligence. Melalui perbandingan dengan rezim hukum Uni Eropa, dapat diidentifikasi posisi hukum Indonesia, baik dari segi norma, prinsip, maupun mekanisme perlindungan, serta ditemukan praktik terbaik (*best practices*) yang relevan untuk diadopsi dalam pengembangan hukum nasional.

Uni Eropa dipilih sebagai objek perbandingan karena merupakan kawasan yang paling progresif dalam mengintegrasikan perlindungan hak asasi manusia dengan pengaturan teknologi digital, khususnya AI. GDPR dan rancangan EU Artificial Intelligence Act menempatkan hak privasi dan perlindungan data pribadi sebagai bagian dari hak fundamental yang tidak dapat dikompromikan oleh kepentingan inovasi teknologi. Sebaliknya, Indonesia melalui UU PDP masih berada pada tahap awal penguatan rezim perlindungan data dan belum secara eksplisit mengantisipasi risiko spesifik AI.

[8] Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12, p. 5.
[9] Brownsword, R. (2019). Law, technology and society: Re-imagining the regulatory environment. *Law, Innovation and Technology*, 11(1), 1–23, p. 18.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

Tabel 1. Perbandingan Pengaturan Perlindungan Privasi dalam Pemanfaatan AI

Aspek	Indonesia (UU PDP)	Uni Eropa (GDPR & EU AI Act)
Dasar hukum perlindungan privasi	Konstitusi (UUD 1945) & UU PDP	EU Charter of Fundamental Rights
Pengaturan AI secara khusus	Belum diatur secara spesifik	Diatur secara komprehensif
Keputusan otomatis	Belum diatur secara rinci	Hak menolak keputusan otomatis
Transparansi algoritma	Terbatas	Kewajiban transparansi

Sumber Tabel: Diolah dari UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan General Data Protection Regulation serta EU Artificial Intelligence Act Draft.

Berdasarkan tabel tersebut, terlihat perbedaan mendasar dalam pendekatan pengaturan. Uni Eropa mengadopsi pendekatan rights-based dan risk-based regulation, di mana sistem AI diklasifikasikan berdasarkan tingkat risikonya terhadap hak fundamental, termasuk hak privasi. GDPR secara tegas memberikan hak kepada subjek data untuk menolak keputusan yang semata-mata didasarkan pada pemrosesan otomatis, termasuk profiling, apabila keputusan tersebut menimbulkan dampak hukum atau dampak signifikan lainnya. Ketentuan ini diperkuat dalam EU AI Act yang menempatkan AI berisiko tinggi di bawah rezim pengawasan ketat dan kewajiban transparansi algoritmik.

Sebaliknya, UU PDP Indonesia masih bersifat umum dan netral teknologi (*technology-neutral regulation*). Meskipun pendekatan ini memberikan fleksibilitas, ketiadaan pengaturan khusus mengenai AI menyebabkan lemahnya perlindungan terhadap risiko khas teknologi tersebut, seperti *algorithmic bias*, *black box decision-making*, dan *function creep*. Hak subjek data dalam UU PDP belum mencakup secara eksplisit hak atas penjelasan algoritma maupun hak untuk menolak keputusan otomatis, sehingga posisi pengguna relatif lebih lemah dibandingkan dengan subjek data di Uni Eropa.

Penulis berpendapat bahwa Indonesia perlu mulai mengadopsi prinsip human-centric AI, yaitu pendekatan yang menempatkan manusia dan hak asasinya sebagai pusat pengembangan dan pemanfaatan AI. Prinsip ini tidak hanya menuntut transparansi dan akuntabilitas teknologi, tetapi juga menegaskan pentingnya kontrol manusia (*human oversight*) atas sistem AI. Dengan mengadaptasi prinsip-prinsip tersebut ke dalam regulasi nasional, baik melalui peraturan pelaksana UU PDP maupun regulasi sektoral AI, Indonesia dapat memastikan bahwa inovasi teknologi berjalan seiring dengan perlindungan hak privasi dan prinsip negara hukum.

5. Urgensi Penguatan Regulasi dan Kebijakan Hukum AI Berbasis Hak Privasi

Urgensi penguatan regulasi Artificial Intelligence di Indonesia didorong oleh realitas empiris bahwa pemanfaatan AI telah meluas secara signifikan di sektor publik maupun swasta, mulai dari layanan administrasi pemerintahan, sistem perbankan dan keuangan digital, hingga platform media sosial dan e-commerce. Perkembangan ini berlangsung lebih cepat dibandingkan dengan kesiapan kerangka hukum nasional, sehingga menimbulkan risiko terjadinya kekosongan norma (*normative vacuum*) dalam melindungi hak privasi pengguna. Dalam perspektif teori hukum

Jurnal Hukum dan Kewarganegaraan
Vol. 16 No. 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

progresif, hukum tidak boleh tertinggal oleh dinamika sosial dan teknologi, melainkan harus hadir sebagai instrumen untuk melindungi kepentingan manusia dan menjamin keadilan substantif.[10]

Dalam konteks pemanfaatan AI, perlindungan hak privasi harus ditempatkan sebagai prinsip utama (*primary guiding principle*) dalam pembentukan kebijakan hukum. Hal ini sejalan dengan paradigma human-centric AI yang menekankan bahwa teknologi dikembangkan untuk melayani manusia, bukan sebaliknya. Tanpa perlindungan privasi yang kuat, AI berpotensi menjadi alat kontrol sosial, eksploitasi data, dan penguatan ketimpangan kekuasaan antara pemilik teknologi dan pengguna. Oleh karena itu, regulasi AI tidak dapat semata-mata berorientasi pada pertumbuhan ekonomi dan inovasi, tetapi harus secara eksplisit mengintegrasikan perlindungan hak asasi manusia sebagai fondasi normatifnya.

Penulis berpendapat bahwa penguatan regulasi dan kebijakan hukum AI di Indonesia perlu dilakukan melalui beberapa langkah strategis. Pertama, diperlukan regulasi khusus mengenai AI yang mengatur klasifikasi risiko, larangan praktik AI berisiko tinggi terhadap hak privasi, serta kewajiban *human oversight* dalam pengambilan keputusan otomatis. Regulasi ini dapat berbentuk undang-undang tersendiri atau peraturan pelaksana UU PDP yang secara spesifik mengatur karakteristik dan implikasi hukum AI.

Kedua, perlu dilakukan penguatan kewenangan lembaga pengawas perlindungan data pribadi, baik dari segi independensi, kapasitas teknis, maupun kewenangan penegakan hukum. Lembaga pengawas harus memiliki kemampuan untuk melakukan audit algoritma, investigasi pelanggaran berbasis AI, serta menjatuhkan sanksi yang efektif, proporsional, dan bersifat preventif. Tanpa pengawasan yang kuat, norma hukum berisiko menjadi deklaratif dan tidak efektif dalam praktik.

Ketiga, pengaturan AI harus memuat kewajiban transparansi dan akuntabilitas algoritmik, termasuk hak pengguna untuk memperoleh penjelasan yang bermakna atas keputusan otomatis yang berdampak signifikan terhadap dirinya. Transparansi algoritmik bukan dimaksudkan untuk membuka rahasia dagang, melainkan untuk memastikan bahwa proses pengambilan keputusan AI dapat diuji secara hukum dan etis. Dengan demikian, prinsip akuntabilitas dalam negara hukum tetap terjaga meskipun keputusan dihasilkan oleh sistem berbasis teknologi canggih.

Langkah-langkah tersebut penting untuk memastikan bahwa pemanfaatan Artificial Intelligence di Indonesia berjalan sejalan dengan prinsip negara hukum, perlindungan hak asasi manusia, dan keadilan sosial. Tanpa penguatan regulasi yang berbasis hak privasi, perkembangan AI justru berpotensi melemahkan posisi individu sebagai subjek hukum dan mereduksi hak privasi menjadi sekadar kepentingan administratif dalam ekosistem digital.

6. P E N U T U P

Berdasarkan hasil kajian dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa pemanfaatan Artificial Intelligence dalam ekosistem digital membawa implikasi hukum yang signifikan terhadap perlindungan hak privasi pengguna. AI beroperasi dengan mengandalkan pengolahan data pribadi dalam skala besar, termasuk data perilaku, preferensi, dan biometrik, yang berpotensi menimbulkan pelanggaran hak privasi apabila tidak diatur secara ketat dan komprehensif. Praktik profiling, pengambilan keputusan otomatis, serta

[10] Rahardjo, S. (2009). *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing, p. 12–14.

pengawasan massal berbasis AI menunjukkan adanya risiko nyata terhadap hak atas perlindungan diri pribadi dan martabat manusia.

Dalam konteks hukum positif Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan normatif yang penting dalam menjamin perlindungan data pribadi dan hak privasi pengguna. Namun demikian, UU PDP masih memiliki keterbatasan normatif karena belum secara spesifik mengatur karakteristik dan risiko khas Artificial Intelligence, seperti keputusan otomatis, transparansi algoritmik, serta mekanisme pengawasan dan pertanggungjawaban hukum atas sistem AI yang bersifat otonom.

Hasil perbandingan dengan rezim hukum Uni Eropa menunjukkan bahwa pengaturan perlindungan privasi dalam pemanfaatan AI di Indonesia masih tertinggal. Uni Eropa telah mengintegrasikan perlindungan hak fundamental ke dalam pengaturan AI melalui GDPR dan EU Artificial Intelligence Act dengan pendekatan berbasis hak dan risiko. Perbandingan tersebut menegaskan perlunya penguatan regulasi nasional agar mampu mengimbangi perkembangan teknologi AI dan memberikan perlindungan hukum yang efektif bagi pengguna.

Sehubungan dengan kesimpulan tersebut, penulis merekomendasikan perlunya penguatan regulasi dan kebijakan hukum Artificial Intelligence di Indonesia yang berbasis pada perlindungan hak privasi pengguna. Penguatan tersebut dapat dilakukan melalui pembentukan regulasi khusus mengenai AI, pengembangan peraturan pelaksana UU PDP yang mengatur pengambilan keputusan otomatis dan transparansi algoritmik, serta penguatan peran dan kewenangan lembaga pengawas perlindungan data pribadi. Dengan langkah tersebut, pemanfaatan Artificial Intelligence diharapkan dapat berjalan sejalan dengan prinsip negara hukum, perlindungan hak asasi manusia, dan keadilan dalam ruang digital.

DAFTAR PUSTAKA

Azheri, B. (2012). *Corporate Social Responsibility Dari Voluntary Menjadi Mandatory*. Jakarta: Raja Grafindo Persada.

Brownsword, R. (2019). Law, technology and society: Re-imagining the regulatory environment. *Law, Innovation and Technology*, 11(1), 1–23. https://doi.org/10.1080/17579961.2019.1579038

Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12. https://doi.org/10.1177/2053951715622512

European Commission. (2021). *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels: European Union.

European Union. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679)*. Official Journal of the European Union, L119, 1–88.

Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, 1(6), 261–262. https://doi.org/10.1038/s42256-019-0055-y

Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Kuner, C. (2020). The rise of AI and the challenges for data protection law. *International Data Privacy Law*, 10(1), 1–12. https://doi.org/10.1093/idpl/ipz025

Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The GDPR: A Commentary*. Oxford: Oxford University Press.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Rahardjo, S. (2009). *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.