

6 ADALAH

Buletin Hukum & Keadilan

Regulasi Kecerdasan Buatan (AI) dalam Perspektif Hukum Indonesia: Menimbang Kesenjangan, Risiko Keamanan Nasional, dan Cetak Biru Tata Kelola yang Berdaulat

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51877](https://doi.org/10.15408/adalah.v9i7.51877)

Abstract:

Artificial Intelligence (AI) is a general-purpose technology that is transforming economic, political, and security systems. However, Indonesia lacks a specific AI regulatory framework and still relies on outdated legal instruments. This article analyzes Indonesia's current AI governance, identifies regulatory gaps, and proposes improvements for rights protection and national security. Using normative legal research with conceptual and comparative approaches based on the EU AI Act, the study finds that the absence of an AI law creates legal uncertainty and increases risks of algorithmic discrimination, surveillance, and AI-related crimes. Existing draft regulations remain non-binding and insufficient. The article concludes that a risk-based AI law and independent oversight are urgently needed.

Keywords: Artificial Intelligence, AI Regulation, Algorithmic Discrimination, Digital Surveillance, Governance.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Kecerdasan Buatan atau *Artificial Intelligence* (AI) tidak lagi sekadar gagasan futuristik dalam narasi fiksi ilmiah. Ia telah menjelma menjadi fondasi utama gelombang Revolusi Industri 4.0, mengubah cara manusia berinteraksi, bekerja, dan mengambil keputusan. Di satu sisi, AI menjanjikan lompatan efisiensi yang revolusioner, otomatisasi cerdas, hingga akurasi diagnostik medis. Namun, di sisi lain, kemampuannya yang eksponensial menyimpan potensi destruktif: diskriminasi algoritmik, pengawasan massal, manipulasi sosial-politik, hingga pengangguran struktural. Dualisme inilah yang menempatkan regulasi AI sebagai isu kritis dalam diskursus hukum kontemporer.

Di tengah percepatan global, Indonesia masih tertatih dalam menyusun kerangka hukum yang memadai. Pengaturan AI masih terserak dalam berbagai regulasi sektoral yang tidak dirancang spesifik untuknya, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP). Belum ada satu pun payung hukum komprehensif yang secara spesifik mendefinisikan, mengklasifikasikan risiko, dan menetapkan batasan tanggung jawab dalam pemanfaatan AI. Kondisi ini menempatkan Indonesia pada posisi yang paradoks: sebagai salah satu pasar digital terbesar di Asia Tenggara, tetapi dengan tingkat kesiapan regulasi yang masih prematur.

Beberapa pakar hukum telah menyuarakan kegelisahan serupa. Satu studi menyimpulkan bahwa kerangka hukum Indonesia saat ini "belum memadai untuk melindungi hak asasi manusia (HAM) di tengah penggunaan AI yang semakin luas dan kompleks". Hal ini diperparah dengan fakta bahwa AI telah digunakan dalam sektor-sektor strategis seperti pengawasan publik dan pengenalan wajah tanpa disertai kewajiban transparansi algoritma, mekanisme audit, maupun pertanggungjawaban hukum yang jelas. Ketiadaan regulasi ini tidak hanya menciptakan ketidakpastian hukum, tetapi juga membuka celah bagi pelanggaran hak konstitusional warga negara, sebagaimana dijamin dalam Pasal 28G ayat (1) UUD 1945.

Tulisan ini memfokuskan pada rumusan masalah: Pertama, bagaimana potret kesenjangan regulasi AI di Indonesia saat ini? Kedua, bagaimana implikasi kekosongan regulasi tersebut terhadap keamanan nasional? Ketiga, bagaimana kerangka ideal regulasi AI nasional yang berdaulat? Tujuannya adalah untuk mengelaborasi kelemahan regulasi eksisting serta menawarkan cetak biru tata kelola AI yang responsif, adaptif, dan humanis.

B. LANDASAN TEORETIS DAN KONSEPTUAL

Konsep negara hukum digital menuntut adanya kepastian hukum dalam setiap aspek kehidupan, termasuk dalam pemanfaatan teknologi baru. Merujuk pada pemikiran Lessig, regulasi di

ruang siber ditentukan oleh empat modalitas: hukum, norma sosial, pasar, dan arsitektur kode. Ketika hukum absen, maka kode dan pasar akan mengambil alih kendali, yang seringkali mengarah pada ketidakadilan dan eksploitasi (Lessig, 2006). Dalam konteks AI, pendekatan berbasis risiko (*risk-based approach*) menjadi standar emas global, sebagaimana diadopsi oleh *EU AI Act*. Pendekatan ini tidak melarang atau membiarkan AI sepenuhnya, melainkan mengklasifikasikan sistem AI berdasarkan tingkat risikonya: dari risiko yang tidak dapat diterima (*unacceptable risk*), risiko tinggi (*high risk*), risiko terbatas (*limited risk*), hingga risiko minimal.

Oleh karena itu, kerangka teori dalam studi ini bertumpu pada tiga pilar utama. Pertama, konsep negara hukum modern yang menekankan supremasi hukum, persamaan di hadapan hukum, dan perlindungan HAM harus dioperasionalkan ulang dalam konteks kedaulatan digital. Asshiddiqie (2021) menegaskan bahwa perlindungan terhadap privasi dan data pribadi merupakan wujud hak konstitusional warga negara yang inheren. Kedua, teori Responsive Regulation yang menawarkan pendekatan piramida penegakan hukum, di mana sanksi pidana merupakan *ultimum remedium*, bukan *premium remedium*. Teori ini menekankan pentingnya dialog antara regulator dan industri untuk menciptakan regulasi yang adaptif (Braithwaite, 2017). Ketiga, konsep *Legal Cybernetics*

yang menekankan perlunya interoperabilitas sistemik antara kode pemrograman, norma hukum, dan dinamika pasar (Lessig, 2006).

Mengabaikan salah satu dari empat modalitas regulasi ini hanya akan menciptakan kebijakan yang pincang. Dalam banyak kasus di Indonesia, regulasi cenderung mengandalkan pendekatan represif tanpa menyentuh dimensi preventif dan edukatif, apalagi memodifikasi arsitektur sistem digitalnya. Oleh karena itu, tinjauan teoretis ini menjadi fondasi penting dalam merumuskan cetak biru tata kelola AI nasional yang ideal.

C. ANALISIS UTAMA

Analisis utama mengidentifikasi setidaknya tiga ranah krusial yang mencerminkan kesenjangan dan kebutuhan mendesak akan rekonstruksi hukum siber di Indonesia, khususnya dalam tata kelola AI: (1) fragmentasi dan ketidakpastian hukum akibat pengaturan yang tersedak; (2) ancaman sistemik terhadap keamanan nasional; serta (3) dilema tanggung jawab hukum atas output AI. Pembahasan ini akan merujuk pada hukum positif, perbandingan global, dan data empirik.

1. Fragmentasi Regulasi: Tidak Ada Definisi, Tidak Ada Kepastian

Problem mendasar tata kelola AI di Indonesia adalah ketiadaan definisi hukum yang spesifik. UU

ITE hanya mengenal istilah "Agen Elektronik" yang didefinisikan sebagai "perangkat dari suatu Sistem Elektronik yang dibuat untuk mewujudkan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis". Definisi ini jelas tidak cukup untuk merespons karakteristik AI modern yang otonom, adaptif, dan mampu menghasilkan konten atau keputusan baru tanpa campur tangan manusia.

Akibatnya, terjadi fragmentasi pengaturan yang sangat sektoral. Di sektor keuangan, Otoritas Jasa Keuangan bersama Asosiasi Fintech Indonesia (AFTECH) menerbitkan kode etik penggunaan AI dalam industri fintech pada 2023. Di bidang politik, Mahkamah Konstitusi melarang penggunaan AI untuk manipulasi foto atau gambar kandidat pemilu sebagai kampanye politik pada awal 2025. Namun, langkah-langkah ini bersifat *ad-hoc* dan reaktif, bukan merupakan bagian dari kebijakan nasional yang koheren. Tidak ada satu pun ketentuan yang mewajibkan transparansi algoritma, mekanisme audit, atau pengawasan manusia (*human oversight*) secara umum.

Keadaan ini dikritik tajam oleh para akademisi. Seorang mahasiswa magister hukum Universitas Indonesia dalam tesisnya menyoroti bahwa "instrumen tersebut tidak dirancang untuk merespons karakteristik AI yang otonom, adaptif, dan berbasis pengambilan keputusan otomatis". Lebih lanjut, ia menekankan bahwa tanpa regulasi

khusus, masyarakat tidak memiliki mekanisme hukum yang jelas untuk meminta pertanggungjawaban atau pemulihan hak apabila dirugikan oleh sistem AI. Ketiadaan standar transparansi ini menjadikan subjek data sebagai pihak yang paling rentan dalam ekosistem digital.

2. Ancaman terhadap Keamanan Nasional: Dari *Deepfake* hingga Pengawasan Massal

Kekosongan regulasi yang lebih komprehensif membuka pintu bagi ancaman keamanan nasional yang nyata. Beberapa di antaranya meliputi:

- **Deepfake dan Disinformasi Politik:** Tim Siber Bareskrim Polri telah mengungkap sejumlah kasus penyalahgunaan AI yang mencolok, salah satunya adalah penyebaran data palsu seolah-olah Menteri Keuangan (waktu itu) menjanjikan hadiah kepada masyarakat. Ini menunjukkan bahwa teknologi *deepfake* telah digunakan untuk menciptakan disinformasi yang dapat merusak reputasi, stabilitas politik, dan kepercayaan publik terhadap institusi negara. Kerangka hukum untuk menanganinya masih sangat dasar, mengandalkan UU ITE dan UU Pornografi yang tidak secara spesifik mendefinisikan dan mengkriminalisasi *deepfake*.

- **Pengawasan Massal dan Diskriminasi Algoritmik:** Pemerintah telah mulai memanfaatkan AI untuk pengawasan publik, pengenalan wajah, dan pemrosesan data pribadi. Namun, tanpa

kerangka etik yang jelas, praktik ini berpotensi melanggar hak privasi dan rasa aman warga negara. Telah disoroti bahwa penggunaan AI di sektor-sektor ini belum disertai kewajiban transparansi algoritma, mekanisme audit, pengawasan manusia, serta pertanggungjawaban hukum yang jelas apabila terjadi pelanggaran.

· Senjata Otonom dan Serangan Siber: Meskipun belum terungkap secara luas, potensi penggunaan AI untuk mengembangkan senjata otonom atau melakukan serangan siber yang lebih canggih merupakan ancaman nyata. Polri mencatat bahwa pelaku *cyber crime* di Indonesia umumnya adalah warga negara asing, menandakan dimensi transnasional dari ancaman ini.

3. Problem Pertanggungjawaban Hukum: *Lex Specialis* yang Belum Ada

Salah satu perdebatan hukum paling fundamental adalah menyangkut pertanggungjawaban atas kerugian yang disebabkan oleh AI. Secara perdata, kerugian yang disebabkan oleh AI hanya dapat dimintai pertanggungjawaban kepada pemilik atau operatornya berdasarkan Pasal 1367 KUHPerdata, yang pada dasarnya adalah rezim tanggung jawab atas perbuatan orang lain (*vicarious liability*). Ini adalah solusi pragmatis, tetapi tidak memadai untuk menangani skenario di mana AI mengambil keputusan di luar kendali atau prediksi pembuatnya.

Secara pidana, perdebatannya lebih kompleks. Apakah AI dapat dipidana? Teori subjek hukum positif Indonesia hanya mengakui "orang" (*natuurlijke persoon*) dan "badan hukum" (*rechts persoon*) sebagai subjek hukum. AI bukanlah keduanya. Oleh karena itu, sebagian besar ahli hukum berpendapat bahwa pertanggungjawaban pidana harus dibebankan kepada pembuat atau operator AI sebagai manus domina (pelaku intelektual), dengan AI hanya dianggap sebagai alat (manus ministra). Namun, hal ini terlihat dari cara kerja tindakan yang dilakukan oleh AI, pertanggungjawaban pidana untuk AI tidak dapat disamakan dengan orang atau badan hukum. Ini menandakan adanya celah hukum (*legal gap*) yang mendesak untuk diisi dengan undang-undang khusus (*lex specialis*).

D. ANOMALI PENERAPAN PASAL KARET DAN DEFISIT REGULASI

Beberapa studi kasus berikut mengkristalkan urgensi regulasi AI yang spesifik:

Kebocoran Data dan Pengawasan Finansial.

Di sektor keuangan, Otoritas Jasa Keuangan bersama AFTECH telah mengeluarkan kode etik penggunaan AI dalam industri *fintech* pada 2023. Namun, langkah ini masih bersifat *self-regulatory* tanpa sanksi yang tegas. Tanpa pengawasan yang ketat, penggunaan AI untuk *profiling* dan skor kredit

berpotensi menimbulkan diskriminasi terhadap kelompok tertentu. Hal ini menunjukkan bahwa kode etik tanpa binding force bukanlah solusi yang cukup.

Manipulasi Politik di Era Digital.

Pada awal 2025, Mahkamah Konstitusi mengeluarkan putusan yang melarang penggunaan AI untuk foto atau gambar kandidat pemilihan umum (pemilu) sebagai kampanye politik. Putusan ini penting, tetapi sifatnya reaktif dan hanya berlaku untuk kontestasi elektoral. Ia tidak memberikan kerangka umum untuk melarang penggunaan AI dalam menciptakan disinformasi di luar konteks pemilu.

Deepfake Pornografi dan Kekerasan Seksual

Kasus *deepfake* yang paling meresahkan adalah penyalahgunaan untuk menciptakan konten pornografi non-konsensual. Seorang penulis kolom hukum beropini bahwa untuk *deepfake* pornografi non-konsensual, penerapan Pasal 5 UU TPKS sangat relevan sebagai bentuk kekerasan seksual berbasis elektronik. Namun, ketiadaan definisi *deepfake* dalam hukum positif membuat penegak hukum harus menggunakan ketentuan yang ada dengan interpretasi yang luas, yang berpotensi menimbulkan ketidakpastian.

E. CETAK BIRU TATA KELOLA AI NASIONAL YANG BERDAULAT

Dari perbandingan dengan kerangka hukum yang lebih maju, seperti *EU AI Act* yang menerapkan pendekatan berbasis risiko dengan klasifikasi ketat dan sanksi tegas bagi pelanggaran, terlihat jelas ketertinggalan Indonesia. Untuk mengejar ketertinggalan ini, solusi tidak cukup hanya dengan menerbitkan Peraturan Presiden (Perpres). Kedua Perpres yang tengah digodok, tentang Peta Jalan dan Etika AI, memang penting, tetapi keduanya tidak akan memuat sanksi dan lebih bersifat sebagai panduan moral dan operasional. Tanpa kekuatan memaksa, panduan etis ini hanya akan menjadi "macan kertas".

Oleh karena itu, cetak biru tata kelola AI nasional harus mencakup:

1. Pembentukan Undang-Undang Khusus tentang AI. DPR RI telah mendorong pembentukan undang-undang yang khusus mengatur AI. Undang-undang ini harus mengadopsi pendekatan berbasis risiko, mengklasifikasikan sistem AI (risiko tinggi, terbatas, minimal), dan menetapkan larangan tegas untuk praktik yang tidak dapat diterima seperti social scoring.
2. Harmonisasi Regulasi. Pemerintah perlu menciptakan harmonisasi dengan

menyesuaikan undang-undang agar Indonesia tidak tersandung masalah kepatuhan saat pelaku usaha nasional berekspansi ke pasar global.

3. Penguatan Kapasitas Forensik Digital. Pemerintah dapat membentuk *National Deepfake Detection Consortium* yang melibatkan Bareskrim, universitas teknik, dan lembaga keamanan siber untuk mengatasi keterbatasan jumlah analisis forensik digital.
4. Pembentukan Otoritas Pengawas Independen. Otoritas ini bertugas mengawasi kepatuhan, memberikan rekomendasi kebijakan, serta menerima dan menindaklanjuti keluhan masyarakat terkait dampak merugikan dari sistem AI.

F. KESIMPULAN

Era AI adalah keniscayaan yang menghadirkan peluang dan ancaman secara bersamaan. Indonesia masih dalam tahap awal merespons fenomena ini, dengan kerangka regulasi yang fragmentaris dan bertumpu pada instrumen hukum yang tidak lagi memadai. Belum adanya undang-undang khusus AI telah menciptakan ketidakpastian hukum dan menempatkan warga negara dalam posisi rentan terhadap potensi pelanggaran HAM dan ancaman keamanan nasional. Berdasarkan temuan di atas, pengaturan berbasis

risiko seperti yang diterapkan dalam *EU AI Act* menjadi model yang paling relevan untuk diadaptasi oleh Indonesia. Namun, adaptasi tersebut harus disertai dengan penguatan kapasitas kelembagaan, transparansi, dan perlindungan hak asasi digital yang kuat. Singularitas hukum siber di Indonesia bergantung pada keberanian untuk tidak sekadar merespons, tetapi mengantisipasi dan membentuk arah perkembangan teknologi itu sendiri. Dengan merekonstruksi pendekatan dari reaktif menuju proaktif dan berlapis, Indonesia dapat membangun ekosistem AI yang inovatif, aman, dan berlandaskan nilai-nilai keadilan.

REFERENSI:

- Asshiddiqie, J. (2021). *Hukum dan Teknologi: Pergulatan Konstitusi dalam Masyarakat Digital*. Rajawali Pers.
- Braithwaite, J. (2017). *Restorative Justice & Responsive Regulation*. Oxford University Press.
- Greenleaf, G. (2022). Asian Data Privacy Laws: Trade and Human Rights Perspectives. *International Data Privacy Law*, 12(3), 189–210. <https://doi.org/10.1093/idpl/ipac008>
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

- Mahfud MD, M. (2022). Negara Hukum dan Demokrasi Pasca Reformasi. Gramedia Pustaka Utama.
- Marpaung, E. M., & Rumapea, E. (2024). Etika dan Pertanggungjawaban Penggunaan Artificial Intelligence di Indonesia. *Jurnal Hukum Lex Generalis*, 5(10), 1–18.
- Negara, P. M. (2026). Urgensitas Pembentukan Undang-Undang Kecerdasan Buatan dalam Menghadapi Ancaman Keamanan Nasional melalui Perspektif HAM dan Good Governance [Tesis Magister Hukum, Fakultas Hukum Universitas Indonesia].
- Oh, P. P. (2026). Risiko Sosial-Etika Mengintai, Regulasi AI Indonesia Masih Tambal Sulam. *Hukumonline.com*.
<https://www.hukumonline.com/berita/a/risiko-sosial-etika-mengintai--regulasi-ai-indonesia-masih-tambal-sulam-lt68dba03af1c9d/>
- Rahardjo, S. (2023). Smart Contract dan Masa Depan Online Dispute Resolution di Indonesia. *Jurnal Hukum dan Peradilan*, 12(1), 33–54.
<https://doi.org/10.25216/jhp.12.1.2023.33-54>
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843)

sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

