ACTA JURIS REVIEW
Vol. 1, No. 1, Maret 2026, pp. 56~66
ISSN: xxxx, PSSN: xxxx, DOI: xxxxx

Analisis Yuridis Tanggung Jawab Pelaku Usaha Atas Wanprestasi Perjanjian Jual Beli Online Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

Maria Beatrice Fransin Basary[1], Niru Anita Sinaga[2], Ardison Asri[3]
[1] Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta, mariabasary18@gmail.com
[2] Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta, niruanitasinaga@unsurya.ac.id
[3] Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta, ardison@unsurya.ac.id

Info Artikel
Histori Artikel:
Diajukan: 05 Maret 2026
Diperbaiki: 09 Maret 2026
Diterima: 12 Maret 2026

Kata kunci:
Perjanjian Jual Beli Online
Wanprestasi
Tanggung jawab
Pelaku Usaha
Perlindungan Konsumen

ABSTRAK

Perkembangan transaksi jual beli barang secara online (e-commerce) telah meningkatkan efisiensi ekonomi, namun juga memunculkan persoalan hukum berupa wanprestasi pelaku usaha yang merugikan konsumen, seperti ketidaksesuaian barang, keterlambatan pengiriman, dan tidak terpenuhinya hak ganti rugi. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa tanggung jawab pelaku usaha diatur melalui integrasi KUHPerdata, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Informasi dan Transaksi Elektronik dengan penerapan prinsip tanggung jawab mutlak dan pembalikan beban pembuktian. Namun, implementasinya masih menghadapi kendala berupa regulasi e-commerce yang belum optimal, rendahnya literasi hukum konsumen, keterbatasan peran BPSK, klausula baku yang merugikan, serta ketidakjelasan tanggung jawab marketplace, sehingga diperlukan pembaruan regulasi dan penguatan kelembagaan untuk meningkatkan perlindungan konsumen dalam transaksi jual beli online.

***Keywords*:**
Online Sales Agreement
Default
Responsibility
Business Actors
Consumer Protection

ABSTRACT

The development of online sales transactions (e-commerce) has increased economic efficiency, but has also given rise to legal issues in the form of business defaults that harm consumers, such as non-conforming goods, late deliveries, and failure to fulfill compensation rights. The research method used is normative legal research with a statutory, conceptual, and case-based approach through literature review. The results indicate that business actors' responsibilities are regulated through the integration of the Civil Code, the Consumer Protection Law, and the Electronic Information and Transactions Law, applying the principle of absolute liability and a reversal of the burden of proof. However, its implementation still faces obstacles such as suboptimal e-commerce regulations, low consumer legal literacy, the limited role of the BPSK (Regional Consumer Protection Agency), detrimental standard clauses, and unclear marketplace responsibilities. Therefore, regulatory reform and institutional strengthening are needed to improve consumer protection in online sales transactions.

A. PENDAHULUAN

Revolusi industri telah menjadikan *Artificial Intelligence* (AI) sebagai pendorong utama di berbagai bidang, mulai dari efisiensi bisnis hingga sektor kesehatan. Dalam era ini, AI tidak hanya mempercepat proses produksi dan analisis data, tetapi juga mengubah cara kita berinteraksi dengan teknologi. Contohnya, dalam dunia bisnis, AI dimanfaatkan untuk analisis prediktif yang membantu perusahaan memaksimalkan rantai pasokan dan menekan biaya operasional. Di bidang kesehatan, AI berperan dalam diagnosis penyakit melalui pemrosesan gambar medis serta pengembangan obat berbasis data besar.

Namun, sifat otonom AI yang memungkinkan sistem itu belajar dan mengambil keputusan tanpa campur tangan manusia menyebabkan munculnya risiko hukum yang belum pernah ada sebelumnya. Risiko ini timbul karena AI bisa menghasilkan hasil yang tidak terduga, seperti keputusan diskriminatif atau konten ilegal, tanpa adanya pihak yang jelas bertanggung jawab. Fenomena "*Black Box*" dalam AI membuat proses pengambilan keputusan sulit dijelaskan bahkan oleh pembuatnya sendiri, sehingga menjadi tantangan untuk membuktikan unsur niat jahat (mens rea) dalam hukum pidana.

Black Box ini terjadi karena algoritma *machine learning* seringkali rumit dan tidak transparan, membuat susah untuk melacak bagaimana AI mencapai suatu kesimpulan. Ini menciptakan dilema etis dan hukum: apakah kesalahan yang dibuat oleh AI harus dipandang sebagai kesalahan manusia? Atau apakah hukum perlu berubah untuk mengakomodasi entitas non-manusia?[1]

Di Indonesia, keberadaan Undang-Undang Nomor 1 Tahun 2024 yang mengubah UU ITE untuk kedua kalinya seharusnya berfungsi sebagai dasar hukum yang kuat dalam mengatur transaksi elektronik dan kejahatan siber. UU ITE, yang pertama kali disahkan pada tahun 2008, telah mengalami beberapa penyesuaian untuk mengikuti perkembangan teknologi serta peningkatan ancaman *siber*. Namun, jika dilihat dari segi teks, undang-undang ini masih fokus pada tindakan yang dilakukan oleh "individu" atau "entitas hukum" melalui sistem, tanpa secara jelas menangani situasi di mana sistem itu sendiri (AI) secara mandiri menghasilkan konten yang melanggar hukum. Hal ini berarti pasal-pasal seperti Pasal 27 mengenai penyebaran konten ilegal dan Pasal 45 tentang penyebaran informasi palsu tetap beranggapan bahwa pelaku utama adalah subjek manusia. Ketika AI menciptakan *deepfake* atau konten manipulatif secara independen, peraturan saat ini tidak memberikan petunjuk yang jelas tentang cara menentukan tanggung jawab. Akibatnya, para korban kejahatan *siber* yang melibatkan AI sering kali kesulitan dalam memperoleh keadilan, karena tuntutan selalu harus berkaitan dengan kesalahan manusia, meskipun AI bertindak secara otonom. Situasi ini menunjukkan perlunya perluasan UU ITE untuk mencakup skenario di mana AI berfungsi sebagai aktor potensial, mungkin melalui amandemen yang mengakui AI sebagai "agen elektronik" dengan tanggung jawab hukum.[2]

Data dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2024 menunjukkan adanya peningkatan yang signifikan dalam kejahatan yang menggunakan teknologi AI, termasuk *cloning* suara yang telah menyebabkan kerugian bagi masyarakat mencapai ratusan miliar rupiah. Laporan BSSN mengindikasikan bahwa insiden kejahatan siber naik sebesar 30% dibandingkan dengan tahun sebelumnya, dengan AI sebagai faktor pendorong utama.

---

[1] L. Floridi, The Ethics of Information (Oxford: Oxford University Press, 2021), hlm. 88. Lihat juga R. K. Dewi, "Black Box Effect pada AI: Implikasi terhadap Pembuktian Mens Rea dalam Hukum Pidana," Jurnal Penelitian Hukum 18, no. 1 (2024): 78.

[2] Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 1 angka 5. Lihat juga S. M. Solaiman, Legal Personhood for Artificial Intelligence (Cambridge: Cambridge University Press, 2021), hlm. 145.

Contohnya, *cloning* suara telah dimanfaatkan dalam skema penipuan telepon, di mana suara korban atau figur publik direkam dan dimodifikasi untuk menipu orang lain dengan alasan mendesak, seperti meminta transfer uang. Kasus-kasus ini tidak hanya berdampak pada kerugian finansial tetapi juga menimbulkan pengikisan kepercayaan publik terhadap teknologi komunikasi. Selain itu, permasalahan *deepfake* pornografi dan penyebaran konten ilegal lainnya telah menjadi isu sosial yang serius, memberikan dampak psikologis kepada para korban. Hal ini menimbulkan pertanyaan penting: apakah perusahaan dapat "melindungi diri" di balik otonomi algoritma mereka, atau apakah hukum Indonesia cukup maju untuk menetapkan tanggung jawab pada pengembang? Pertanyaan ini sangat penting karena tanpa regulasi yang jelas, perusahaan teknologi mungkin akan terus mengembangkan AI tanpa mempertimbangkan risiko hukum, sementara masyarakat harus membayar konsekuensi. BSSN juga mencatat bahwa sebagian besar perusahaan AI beroperasi dari luar negeri, sehingga menyulitkan penegakan hukum domestik.[3]

Ketidakpastian ini menciptakan kekosongan hukum *(recht vacuüm*) yang berpotensi mengurangi perlindungan bagi korban kejahatan siber. *Recht vacuüm* muncul ketika tidak ada regulasi yang mengatur situasi baru, sehingga norma yang relevan tidak dapat diterapkan. Dalam konteks kecerdasan buatan (AI), hal ini berarti bahwa ketika AI melakukan tindakan kriminal tanpa intervensi manusia langsung, tidak terdapat kerangka hukum yang jelas untuk menetapkan siapa yang bertanggung jawab. Mengacu pada prinsip hukum tradisional, pertanggungjawaban pidana selalu didasarkan pada asas "tiada pidana tanpa kesalahan" (*geen straf zonder schuld*), yang mensyaratkan adanya niat atau kelalaian dari individu sebagai subjek hukum. Di ranah AI, muncul perdebatan tajam: apakah sebuah kode pemrograman mampu memiliki "kehendak" untuk melakukan kejahatan, ataukah ia hanya merupakan alat dari kelalaian manusia (*professional negligence*)? Diskusi ini menyentuh aspek filsafat hukum, di mana beberapa ahli berpendapat bahwa AI bisa dianggap sebagai "agen moral" dengan tanggung jawabnya sendiri, sementara lainnya berargumen bahwa AI tetap merupakan produk ciptaan manusia. Sebagai contoh, jika sistem kendaraan otonom mengalami kecelakaan akibat kesalahan algoritma, apakah itu menjadi tanggung jawab pengembang karena kurangnya pengujian yang memadai, atau apakah AI itu sendiri memiliki "kehendak" untuk melanggar aturan? Dilema ini semakin rumit oleh kenyataan bahwa AI dapat belajar dari data yang bias, sehingga menghasilkan *output* diskriminatif tanpa adanya niat eksplisit dari manusia. Oleh karena itu, hukum di Indonesia perlu mempertimbangkan pendekatan *hibrid*: menjaga asas pertanggungjawaban manusia sambil memperluas tanggung jawab korporasi terkait risiko penggunaan AI.[4]

Untuk menghadapi tantangan ini, perluasan interpretasi dalam berbagai aspek hukum nasional menjadi suatu keharusan. Proses perluasan ini mencakup penafsiran yang inovatif terhadap peraturan yang ada, serta saran-saran untuk reformasi. Tanpa langkah-langkah ini, sistem hukum Indonesia berisiko tertinggal dibandingkan negara-negara lain yang telah mulai mengatur kecerdasan buatan, seperti Uni Eropa dengan Undang-Undang AI mereka.[5]

Hukum di Indonesia perlu lebih tegas dalam mengadopsi prinsip yang menyatakan bahwa korporasi atau pengembang bertanggung jawab atas tindakan AI yang mereka kelola. Tanggung jawab *vicarious*, yang berasal dari hukum *common law*, memberikan dasar bagi

[3] I. D. S. Saimima, "Deepfake dan UU ITE: Tantangan Regulasi Konten Digital di Era AI," Media Hukum 30, no. 1 (2023): 115.

[4] Muladi, Pertanggungjawaban Pidana Korporasi (Jakarta: Rajawali Pers, 2010), hlm. 52. Lihat juga A. Wicaksono, "AI Liability: Menggagas Tanggung Jawab Korporasi atas Teknologi Otonom," Hukumonline.com, diakses 24 Januari 2026.

[5] H. Gunawan, "Strict Liability untuk AI Berisiko Tinggi: Pelajaran dari Uni Eropa," Jurnal Teknologi dan Hukum 9, no. 4 (2022): 305.

majikan untuk bertanggung jawab atas tindakan karyawan dalam konteks pekerjaan. Dalam hal ini, prinsip ini dapat diperluas untuk mencakup tanggung jawab korporasi terhadap "agen teknologi" yang mereka gunakan. Apabila AI menyebabkan kerugian akibat desain yang buruk atau kurangnya pengawasan, maka beban pembuktian seharusnya berpindah kepada pihak pengembang. Sebagai contoh, jika *chatbot* AI milik perusahaan *e-commerce* secara mandiri mempromosikan produk ilegal, maka perusahaan harus menunjukkan bahwa mereka telah melakukan pengawasan yang memadai. Pergeseran beban pembuktian ini akan memudahkan korban untuk mengajukan tuntutan, karena korporasi dengan kekuatan finansial dan teknis yang lebih besar harus mempertanggungjawabkan inovasi mereka.[6]

Audit Algoritma sebagai Standar Kepatuhan: Mengingat adanya fenomena *Black Box*, regulasi yang akan datang tidak seharusnya hanya fokus pada hasil akhir, tetapi juga harus mewajibkan adanya transparansi dalam algoritma. Keberadaan transparansi ini sangat krusial untuk memungkinkan dilakukannya audit eksternal serta pengawasan oleh publik. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang baru diharapkan akan didukung oleh aturan pelaksana yang mewajibkan audit rutin bagi penyedia layanan kecerdasan buatan (AI) yang memiliki risiko tinggi. Proses audit ini seharusnya dilakukan oleh lembaga independen, seperti Badan Siber dan Sandi Negara (BSSN) atau badan sertifikasi AI, dan harus mencakup penilaian terkait risiko etika, keamanan data, serta potensi bias dalam algoritma. Dengan cara ini, perusahaan diharuskan untuk membuka "kotak hitam" mereka agar masyarakat dapat memahami proses pengambilan keputusan oleh AI. Langkah ini juga akan mendorong pengembangan AI yang lebih etis, karena audit dapat membantu mengidentifikasi masalah sebelum terjadinya dampak negatif.[7]

Meskipun saat ini sistem kecerdasan buatan (*Artificial Intelligence/AI*) belum memperoleh pengakuan sebagai subjek hukum mandiri (*legal personhood*) dalam tatanan hukum positif di Indonesia, urgensi penetapan standar kewaspadaan yang wajar (*due diligence*) bagi para pengembang menjadi sebuah keniscayaan yuridis. Hal ini dimaksudkan agar karakteristik otonom pada mesin tidak dijadikan sebagai dalih (*legal excuse*) untuk melepaskan diri dari tanggung jawab hukum.

Instrumen *due diligence* tersebut harus memformulasikan langkah-langkah preventif yang komprehensif, meliputi analisis dampak etis pra-peluncuran, pengawasan sistemik yang berkelanjutan, serta penyediaan mekanisme terminasi darurat (*emergency kill switch*) apabila ditemukan penyimpangan operasional. Dalam konstruksi hukum ini, sekalipun AI tidak memiliki kedudukan sebagai subjek hukum, korporasi pengembang wajib memikul beban pertanggungjawaban atas segala risiko fungsional yang ditimbulkan.

Kebijakan ini bertujuan untuk memitigasi penyalahgunaan otonomi algoritma sebagai alasan pemaaf atas pelanggaran hukum, sekaligus menjamin perlindungan terhadap hak-hak konstitusional masyarakat di tengah akselerasi teknologi. Dalam perspektif jangka panjang, Indonesia perlu mempertimbangkan reorientasi hukum melalui pengakuan subjek hukum terbatas (*partial legal personhood*) terhadap AI, selaras dengan tren regulasi global mengenai entitas robotik otonom.[8]

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan dalam penelitian ini dirumuskan sebagai berikut: Bagaimana konstruksi hukum

[6] B. Arifin, "Konstruksi Hukum Vicarious Liability dalam Konteks AI di Indonesia," Jurnal Ilmu Hukum 12, no. 3 (2023): 208. Lihat juga R. Pratama, "Pertanggungjawaban Korporasi dalam Kejahatan Siber: Kajian atas UU ITE," Jurnal Hukum dan Teknologi 5, no. 2 (2022): 48.

[7] Indonesia, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lihat juga R. K. Dewi, op. cit., hlm. 85.

[8] S. M. Solaiman, hlm. 210. Lihat juga A. Wicaksono, op. cit.

pertanggungjawaban pidana korporasi terhadap tindak pidana yang dilakukan oleh AI yang bersifat otonom dalam kerangka UU ITE di Indonesia? Apa saja kendala yuridis dan tantangan pembuktian dalam menetapkan kesalahan (*mens rea*) korporasi mengingat adanya fenomena *Black Box* pada teknologi AI?

B. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan yuridis normatif, yang berarti fokus utama penelitian ini adalah pada standar hukum positif yang berlaku di Indonesia dan relevan dengan isu tanggung jawab hukum terkait kecerdasan buatan (tanggung jawab AI). Pendekatan normatif dipilih karena permasalahan tanggung jawab hukum atas AI di Indonesia sangat bergantung pada penafsiran undang-undang yang ada, terutama Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, Kitab Undang-Undang Hukum Pidana (KUHP), serta berbagai peraturan pelaksana, regulasi pemerintah, dan perundang-undangan lain seperti Undang-Undang Nomor 1 Tahun 2024 yang merupakan perubahan kedua atas UU ITE. Metode ini memungkinkan peneliti untuk mengevaluasi bagaimana norma-norma hukum saat ini dapat diterapkan atau dikembangkan untuk menghadapi tantangan baru yang ditimbulkan oleh teknologi AI, tanpa memerlukan pengukuran empiris atau survei lapangan. Pemilihan pendekatan ini didasari oleh sifat teoritis dan normatif dari isu tanggung jawab AI, di mana perhatian utama terfokus pada analisis teks hukum, interpretasi doktrin, serta identifikasi kesenjangan dalam regulasi, ketimbang pengumpulan data kuantitatif seperti statistik kejahatan siber. Dengan demikian, tujuan penelitian ini adalah untuk memberikan rekomendasi hukum yang praktis dan dapat dilaksanakan berdasarkan analisis normatif yang mendalam.[9]

Sumber hukum dalam penelitian ini terdiri dari tiga kategori: sumber hukum primer, sekunder, dan tersier. Sumber hukum primer meliputi undang-undang, peraturan pemerintah, dan putusan pengadilan yang digunakan untuk memperoleh teks asli dari regulasi yang berlaku. Contohnya adalah Pasal 27 UU ITE yang mengatur tentang distribusi konten ilegal serta Pasal 45 mengenai penyebaran *hoaks*, yang dianalisis untuk menilai keterkaitannya dengan tindakan AI otonom.

Sumber sekunder, seperti artikel jurnal oleh para ahli hukum baik di Indonesia maupun internasional, berfungsi untuk membandingkan praktik hukum di negara lain, termasuk regulasi AI di Uni Eropa atau Amerika Serikat. Di sisi lain, sumber tersier membantu dalam mendefinisikan istilah teknis seperti "*machine learning*" dan "*black box*" dalam konteks hukum.

Selain itu, penelitian ini juga memperhatikan literatur internasional terkait regulasi teknologi dan tanggung jawab AI. Tujuannya adalah untuk menyajikan perspektif yang beragam serta menemukan tren global dalam pengaturan tanggung jawab hukum AI. Dengan demikian, rekomendasi yang dihasilkan tidak hanya relevan bagi Indonesia tetapi juga sejalan dengan perkembangan internasional. Misalnya, dengan mempelajari bagaimana negara-negara maju menangani tanggung jawab ketat untuk AI berisiko tinggi, penelitian ini diharapkan dapat mendorong reformasi hukum yang lebih progresif di Indonesia.[10]

Untuk melakukan analisis terhadap data kualitatif, hukum yang relevan akan diuraikan dan dianalisis guna menilai sejauh mana peraturan yang ada dapat mengatasi masalah tanggung jawab dalam penggunaan serta tindakan kecerdasan buatan. Proses analisis kualitatif ini memanfaatkan berbagai teknik interpretasi hukum, termasuk penafsiran

[9] Pendekatan ini merujuk pada metodologi penelitian hukum normatif yang umum digunakan dalam mengkaji kesenjangan norma (norm vacuum). Lihat Muladi, hlm. 15-20.

[10] H. Gunawan, hlm. 310.

gramatikal (membaca teks secara langsung), sistematis (meninjau konteks dalam kerangka hukum yang lebih luas), dan teleologis (memahami tujuan dari undang-undang tersebut). Pendekatan ini bertujuan untuk mengidentifikasi kesenjangan dalam regulasi, seperti ketidakmampuan UU ITE untuk mengatur AI sebagai subjek potensial, potensi konflik norma antara prinsip kesalahan manusia dan otonomi AI, serta kebutuhan untuk memperbarui hukum melalui amandemen atau regulasi baru. Proses analisis dilakukan dengan langkah-langkah sistematis: pertama, mengidentifikasi pasal-pasal yang relevan; kedua, membandingkannya dengan situasi AI seperti *deepfake* atau *cloning* suara; ketiga, mengevaluasi apakah struktur hukum saat ini memadai atau perlu diperluas. Temuan dari analisis ini selanjutnya digunakan untuk mendukung argumen mengenai perlunya penerapan doktrin seperti tanggung jawab *vicarious* atau *strict liability* dalam konteks kecerdasan buatan.[11]

Metode pengumpulan data dalam penelitian ini mencakup tinjauan terhadap dokumen-dokumen seperti peraturan hukum, jurnal akademik, dan putusan pengadilan yang berkaitan dengan kejahatan siber atau teknologi. Proses peninjauan ini dilakukan melalui berbagai *database online*, termasuk situs resmi Kementerian Hukum dan HAM, JSTOR untuk akses jurnal, serta portal pengadilan untuk menemukan keputusan kasus yang relevan.

Untuk memperoleh pemahaman yang lebih mendalam tentang penerapan hukum dalam konteks kecerdasan buatan (AI), penelitian ini mungkin juga melibatkan wawancara mendalam atau diskusi kelompok terfokus dengan para ahli hukum pidana, pakar teknologi informasi, atau regulator jika diperlukan guna memperkaya analisis. Wawancara tersebut dapat dilaksanakan secara semi-terstruktur, di mana pertanyaan dirumuskan berdasarkan temuan awal dari analisis dokumen, contohnya tantangan dalam membuktikan unsur mens rea pada AI. Sebagai ilustrasi, wawancara dengan hakim atau jaksa yang menangani kasus terkait siber bisa memberikan pandangan berharga mengenai hambatan praktis dalam penegakan hukum.

Namun demikian, jika pelaksanaan wawancara tidak memungkinkan karena kendala waktu atau aksesibilitas, penelitian ini akan tetap bergantung pada data sekunder yang kuat. Validitas data akan diuji melalui triangulasi yakni dengan membandingkan sumber dari berbagai jenis untuk memastikan konsistensi sementara keandalan analisis didukung oleh penggunaan kerangka teoritis yang jelas terkait hukum pidana dan teknologi.

Penelitian ini tidak mengaplikasikan metode kuantitatif karena fokusnya adalah pada aspek normatif dan interpretatif alih-alih pengukuran statistik. Batasan penelitian mencakup keterbatasan data kasus nyata di Indonesia sehubungan dengan AI; oleh karena itu, analisis cenderung bersifat teoritis dan prediktif dengan harapan dapat mendorong penelitian empiris di masa depan. Melalui pendekatan ini, tujuan penelitian adalah untuk memberikan kontribusi baik secara akademik maupun praktis dalam menangani dilema hukum terkait AI di Indonesia.[12]

C. HASIL DAN PEMBAHASAN

Berdasarkan analisis normatif yuridis yang dilakukan terhadap data yang diperoleh dari sumber hukum primer, sekunder, dan tersier, serta penafsiran terhadap undang-undang relevan seperti UU ITE dan KUHP, bagian ini mengeksplorasi konstruksi hukum mengenai pertanggungjawaban pidana korporasi terkait tindak pidana yang melibatkan *Artificial Intelligence* (AI) di Indonesia. Analisis tersebut menggunakan teknik penafsiran gramatikal,

[11] Analisis ini menggabungkan penafsiran teleologis terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan perkembangan teknologi AI terkini.
[12] R. Pratama, hlm. 55.

sistematis, dan teleologis untuk mengungkap bagaimana hukum saat ini dapat diterapkan serta mengidentifikasi kesenjangan yang ada. Pembahasan ini dibagi menjadi tiga subbagian utama: konstruksi hukum pertanggungjawaban korporasi atas tindakan AI, kendala yuridis dan tantangan dalam pembuktian, serta solusi dan rekomendasi yang bersifat progresif. Pendekatan ini menunjukkan bahwa hukum Indonesia saat ini belum sepenuhnya siap menghadapi otonomi AI, sehingga diperlukan perluasan interpretasi dan reformasi untuk menjaga keseimbangan antara inovasi teknologi dan perlindungan hukum.[13]

Konstruksi hukum di Indonesia saat ini lebih cenderung melihat AI sebagai "alat" (instrumentum) ketimbang "aktor" (*actor)*. Ini berarti bahwa AI dipahami sebagai perpanjangan tangan manusia atau perusahaan, bukan sebagai entitas yang berdiri sendiri. Namun, ketika AI mulai menerapkan *machine learning* dan menghasilkan *output* yang tidak dapat diprediksi oleh program awal (otonomi penuh), landasan hukum pidana konvensional mulai mengalami tantangan. Hal ini terjadi karena hukum pidana tradisional mensyaratkan adanya subjek hukum yang memiliki kesadaran dan kehendak atribut yang tidak dimiliki oleh AI. Oleh karena itu, perluasan konstruksi hukum diperlukan untuk mengakomodasi tanggung jawab perusahaan sebagai pemilik dan pengelola AI, sehingga perusahaan tersebut dapat dianggap sebagai subjek hukum yang bertanggung jawab atas risiko yang ditimbulkan oleh teknologi mereka, meskipun AI bekerja secara otonom. Dalam praktiknya, ini berarti bahwa perusahaan harus dianggap bertanggung jawab atas konsekuensi dari inovasi mereka dengan menekankan prinsip "tiada pidana tanpa kesalahan", yang diperluas melalui doktrin seperti *vicarious liability dan strict liability.*

Pendekatan Teori Risiko menjadi pijakan utama dalam konstruksi ini. Perusahaan yang meraih keuntungan finansial dari penggunaan AI harus menanggung risiko kerugian yang ditimbulkan oleh teknologi tersebut. Dalam konteks hukum pidana, hal ini mengharuskan perusahaan menerapkan prinsip *Safety by Design* yakni memasukkan elemen keamanan sejak tahap desain AI. Contohnya, jika sebuah perusahaan pengembang AI membiarkan sistemnya tanpa filter keamanan memadai sehingga digunakan untuk membuat *deepfake* pornografi (melanggar Pasal 27 ayat (1) UU ITE: *"Melarang setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik yang memiliki muatan yang melanggar kesusilaan"*), maka perusahaan tersebut telah melakukan kelalaian (*omission*). Kelalaian semacam ini bisa dianggap sebagai bentuk kelalaian yang dapat dikenakan sanksi pidana karena perusahaan gagal memenuhi kewajiban mencegah risiko. Kasus nyata menunjukkan bahwa jika *chatbot* AI menghasilkan konten ofensif tanpa kontrol, maka dapat dikategorikan sebagai pelanggaran UU ITE apabila tidak ada mekanisme pencegahan. Teori risiko menyoroti pentingnya keseimbangan antara keuntungan ekonomi dan tanggung jawab sosial, sehingga perusahaan tidak seharusnya mengalihkan risiko kepada masyarakat. Analisis terhadap Pasal 45 ayat (1) UU ITE mengenai penyebaran hoaks menunjukkan bahwa jika AI secara otonom menyebarkan informasi palsu, perusahaan sebagai Penyelenggara Sistem Elektronik (PSE) bisa dituntut atas kelalaian dalam pengawasan meskipun tidak ada niat langsung dari individu.

Penerapan Doktrin *Vicarious Liability* juga sangat penting dalam konstruk hukum ini. Dalam konteks ini, AI bisa dipandang sebagai "agen teknologi," di mana perusahaan bertanggung jawab atas tindakan agen tersebut sama seperti mereka bertanggung jawab atas perilaku karyawan dalam pekerjaan mereka. Seperti halnya sebuah perusahaan bertanggung jawab atas tindakan kurir yang menyebabkan kecelakaan saat mengantar barang, pengembang AI juga bertanggung jawab atas "tabrakan" digital yang dilakukan algoritmanya. Dalam UU ITE, tanggung jawab ini melekat pada PSE sebagaimana

[13] B. Arifin, hlm. 215.

didefinisikan dalam Pasal 1 ayat (5) yaitu orang atau badan usaha yang menyediakan serta mengelola Sistem Elektronik. Doktrin ini memungkinkan perluasan tanggung jawab korporasi tanpa harus membuktikan niat langsung manajemen. Misalnya, jika sistem *e-commerce* berbasis AI secara otonom mempromosikan produk ilegal, korporasi selaku PSE dapat dikenakan hukuman berdasarkan tindakan tersebut. Ini berlandaskan pada prinsip bahwa korporasi memiliki kontrol terhadap agen mereka termasuk AI dan harus memastikan agar agen tersebut tidak melanggar peraturan hukum.

Aplikasi dari konsep ini selaras dengan perkembangan hukum internasional di mana negara-negara seperti Uni Eropa telah mulai menerapkan tanggung jawab korporasi terkait dengan penggunaan AI melalui regulasi seperti *AI Act 2024* untuk penyedia berisiko tinggi. Di Indonesia sendiri, interpretasi sistematis terhadap UU ITE bisa memperluas *vicarious liability* meskipun undang-undang belum secara eksplisit menyebutkan keberadaan AI dengan alasan bahwa IA merupakan bagian dari Sistem Elektronik yang dikelola oleh korporasi.

Lebih jauh lagi, konstruksi hukum ini dapat diperkaya melalui pendekatan *hibrid* yang menggabungkan asas kesalahan manusia dengan tanggung jawab korporasi. Meskipun AI bukanlah subjek hukum secara langsung, entitas korporasi yang menciptakan dan memanfaatkan teknologi tersebut seharusnya dianggap bertanggung jawab atas output otonom dari sistem mereka. Pendapat ini didukung oleh literatur internasional seperti laporan *Organisation for Economic Co-operation and Development* (OECD) mengenai Prinsip-prinsip tentang AI yang menekankan pentingnya tanggung jawab manusia terhadap teknologi tersebut. Dalam konteks Indonesia, pendekatan seperti itu memungkinkan penegakan hukum terhadap perusahaan tanpa perlu menunggu pengakuan formal bagi status *legal personhood* bagi AI a topik kontroversial hingga saat ini.

Dengan demikian, konstruksi hukum saat ini dapat diperluas lewat interpretasi teleologis terhadap UU ITE demi melindungi masyarakat dari kejahatan siber untuk mencakup risiko-risiko terkait dengan penggunaan teknologi berbasis kecerdasan buatan.

Tantangan utama dalam mengatur korporasi terkait dengan fenomena yang dikenal sebagai "*The Black Box Effect*." Masalah ini menyebabkan proses internal AI menjadi sulit dipahami dan tidak mudah dibuktikan di pengadilan. Jaksa sering menghadapi kesulitan dalam membuktikan niat jahat (*mens rea*) dari korporasi, karena menjadi sulit untuk menentukan apakah pengurus memang memiliki niat untuk menipu atau jika kesalahan tersebut hanya merupakan masalah teknis dalam algoritma. Fenomena *Black Box Effect* ini semakin diperparah oleh kompleksitas machine learning, di mana AI belajar dari data besar tanpa ada intervensi manusia secara langsung, sehingga mempersulit pelacakan hubungan sebab akibat. Hal ini menyulitkan pembuktian, mengingat hukum pidana memerlukan bukti yang kuat agar tidak terjadi kesalahan penuntutan. Dalam konteks AI, bukti teknis sering kali membutuhkan keahlian forensik digital yang mahal dan sulit ditemukan di Indonesia.

Kendala Definisi Subjek Hukum juga merupakan tantangan signifikan lainnya. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) belum mengakui *Electronic Personhood* atau pengakuan AI sebagai subjek hukum yang independen, sehingga setiap tuntutan harus selalu kembali kepada kesalahan manusia. Dengan demikian, ketika AI bertindak otonom, jaksa perlu membuktikan adanya kelalaian atau niat dari pengurus korporasi meskipun terdapat kemungkinan kesalahan pada interaksi data yang rumit. Hal ini menciptakan kekosongan hukum di mana korban mengalami kesulitan mendapatkan ganti rugi, sementara korporasi dapat lepas tanggung jawab dengan alasan bahwa AI beroperasi "secara mandiri." Contohnya adalah kasus *cloning* suara yang merugikan hingga ratusan miliar rupiah; jika AI menghasilkan suara palsu tanpa instruksi eksplisit, maka membuktikan

mens rea menjadi sangat sulit tanpa dokumen internal yang menunjukkan adanya kelalaian dalam desain.

Beban Pembuktian juga menghadirkan tantangan signifikan. Dalam kasus-kasus terkait AI seperti *deepfake* atau manipulasi data, membuktikan adanya *malice* (niat jahat) di tingkat dewan direksi sering kali membutuhkan bukti berupa email, notulen rapat, atau catatan pengembangan yang jarang tersedia. Jaksa harus mengumpulkan bukti teknis seperti *log algoritma* yang mungkin dienkripsi atau tidak dapat diakses oleh pihak luar. Ini meningkatkan biaya dan waktu dalam proses penuntutan serta risiko kegagalan kasus karena korporasi umumnya memiliki sumber daya hukum yang lebih besar. Analisis terhadap putusan pengadilan mengenai kejahatan siber menunjukkan bahwa kasus-kasus semacam ini jarang mencapai tahap vonis akibat dari tantangan pembuktian.

Yurisdiksi adalah kendala ketiga yang penting untuk diperhatikan, terutama karena banyak perusahaan pengembang AI berlokasi di luar negeri seperti Silicon Valley atau Cina. Penegakan hukum domestik jadi sulit dilakukan tanpa adanya kerja sama internasional melalui perjanjian ekstradisi atau bantuan hukum timbal balik. Sebagai contoh, jika perusahaan asing seperti Google atau Alibaba terlibat dalam tindak kejahatan berbasis AI di Indonesia, maka pengadilan Indonesia mungkin tidak memiliki yurisdiksi langsung atas mereka; akibatnya korban harus bergantung pada mekanisme internasional yang cenderung lambat. Situasi ini memperburuk kondisi *recht vacuüm* di mana hukum Indonesia tidak mampu melindungi warganya dari risiko global terkait teknologi AI.

Secara keseluruhan, berbagai kendala ini menciptakan kondisi di mana sistem hukum pidana konvensional tidak cukup responsif terhadap perkembangan teknologi AI saat ini; oleh karena itu diperlukan reformasi untuk mengatasi *Black Box Effect* dan memperkuat mekanisme pembuktian.

Untuk mengatasi tantangan tersebut, penelitian ini mengusulkan beberapa solusi hukum progresif yang dapat diimplementasikan melalui perluasan interpretasi dan reformasi peraturan. Solusi-solusi ini didasarkan pada analisis kesenjangan regulasi serta perbandingan dengan praktik internasional, bertujuan untuk memberikan kepastian hukum bagi perusahaan dan melindungi masyarakat.

Salah satu solusi utama adalah penerapan Tanggung Jawab Mutlak pada sektor berisiko tinggi. Dalam konteks kecerdasan buatan (AI) yang menangani data keuangan, identitas biometrik, atau konten publik, perusahaan harus bertanggung jawab sepenuhnya jika terjadi kebocoran atau penyalahgunaan data, tanpa perlu menunjukkan adanya niat buruk. Hal ini berarti bahwa perusahaan akan dikenakan sanksi asalkan terdapat kerugian, mencegah mereka mengabaikan risiko dengan alasan 'kotak hitam'. Sebagai contoh, dalam penggunaan AI untuk verifikasi identitas, apabila terjadi manipulasi data, lembaga seperti bank atau penyedia layanan *fintech* dapat langsung dikenakan sanksi. Pendekatan ini sejalan dengan regulasi internasional seperti *General Data Protection Regulation* (GDPR) di Uni Eropa yang menerapkan tanggung jawab mutlak terkait pelanggaran data.

Rekomendasi kedua adalah pelaksanaan Audit Algoritma secara berkala. Dengan mewajibkan perusahaan untuk melakukan audit independen terhadap sistem AI mereka sebagai prasyarat operasional di Indonesia, transparansi dapat meningkat. Audit ini harus mencakup evaluasi risiko etis, keamanan data, dan kemungkinan bias yang dilakukan oleh lembaga seperti BSSN atau auditor sertifikasi AI. Dengan cara ini, perusahaan diharuskan untuk membuka "kotak hitam" mereka agar jaksa lebih mudah membuktikan kelalaian. Selain itu, audit juga mendorong pengembangan AI yang etis karena dapat mengidentifikasi masalah sebelum terjadi.

Reformasi Regulasi Undang-Undang ITE merupakan solusi jangka panjang yang diperlukan. Penambahan klausul mengenai tanggung jawab Penyelenggara Sistem Elektronik (PSE) terhadap *output* otonom dari AI termasuk standar kehati-hatian dan mekanisme pelaporan insiden dapat menutup kekosongan hukum. Klausul tersebut harus menetapkan bahwa perusahaan bertanggung jawab atas risiko terkait AI dengan pergeseran beban pembuktian jika ada kelalaian yang terbukti. Reformasi ini dapat dilaksanakan melalui Peraturan Pemerintah (PP) yang merupakan turunan dari Undang-Undang ITE dan mengakomodasi AI sebagai "agen elektronik". Selain itu, Indonesia bisa mengambil pelajaran dari *AI Act* Uni Eropa untuk menetapkan klasifikasi risiko terkait AI serta kewajiban khususnya.

Secara keseluruhan, solusi-solusi ini akan memperkuat struktur hukum dengan memindahkan fokus dari kesalahan subjektif ke kesalahan objektif sehingga perusahaan tidak bisa bersembunyi di balik otonomi AI. Implementasinya membutuhkan kolaborasi antara pemerintah, akademisi, dan industri untuk memastikan bahwa inovasi dalam bidang AI tidak mengorbankan keadilan hukum. Dengan langkah-langkah progresif ini, Indonesia dapat menjadi pionir dalam regulasi kecerdasan buatan di Asia Tenggara.

D. SIMPULAN

Berdasarkan analisis yuridis normatif mengenai konstruksi hukum pertanggungjawaban pidana korporasi terhadap tindak pidana yang melibatkan Kecerdasan Buatan (AI) di Indonesia, penelitian ini menyimpulkan bahwa hukum positif saat ini, khususnya Undang-Undang ITE dan KUHP, belum sepenuhnya mampu mengakomodasi otonomi AI sebagai sumber risiko hukum. Konstruksi hukum dapat diperluas dengan pendekatan Teori Risiko dan Doktrin *Vicarious Liability*, di mana korporasi sebagai Penyelenggara Sistem Elektronik (PSE) dianggap bertanggung jawab atas hasil dari AI otonom, meskipun AI bukanlah subjek hukum mandiri. Hal ini menjawab rumusan masalah pertama tentang bagaimana konstruksi hukum dapat menanggapi tindak pidana AI, dengan penekanan bahwa korporasi tidak seharusnya menghindar dari tanggung jawab atas inovasi teknologi demi kepentingan ekonomi.

Beberapa kendala yuridis yang dihadapi mencakup Efek *Black Box*, definisi subjek hukum yang terbatas, beban pembuktian yang tinggi, serta isu yurisdiksi internasional, yang sering kali melemahkan penegakan hukum terhadap korporasi pengelola AI. Ini memberikan jawaban pada rumusan masalah kedua, di mana diperlukan solusi progresif seperti penerapan *strict liability* untuk sektor-sektor berisiko tinggi, audit algoritma secara berkala, dan reformasi regulasi dalam Undang-Undang ITE guna menghadapi tantangan tersebut. Secara keseluruhan, penelitian ini menunjukkan bahwa melalui perluasan interpretasi hukum dan reformasi yang tepat, Indonesia dapat mencapai keseimbangan antara mendorong inovasi AI sekaligus melindungi masyarakat dari risiko kejahatan siber sehingga mencegah korporasi berlindung di balik otonomi algoritma.

E. SARAN

Pemerintah Indonesia perlu segera menyusun Peraturan Pemerintah (PP) yang merupakan turunan dari Undang-Undang ITE, yang secara spesifik mengatur mengenai standardisasi etika, keamanan, dan tanggung jawab kecerdasan buatan (AI) bagi perusahaan. Ini termasuk kewajiban untuk melakukan audit algoritma secara berkala oleh lembaga independen, seperti Badan Siber dan Sandi Negara (BSSN). Langkah ini akan menciptakan kepastian hukum bagi pelaku usaha dan memberikan perlindungan maksimal kepada konsumen digital. Selanjutnya, disarankan untuk meningkatkan kolaborasi internasional

dalam penegakan hukum terkait AI, melalui perjanjian bilateral dengan negara-negara tempat perusahaan AI berasal, guna mengatasi isu yurisdiksi. Akademisi dan praktisi hukum dianjurkan untuk terus melakukan penelitian empiris mengenai kasus-kasus nyata terkait tanggung jawab AI di Indonesia. Di sisi lain, perusahaan teknologi juga diharapkan menerapkan prinsip *Safety by Design* sejak tahap awal pengembangan AI untuk meminimalkan risiko hukum. Dengan penerapan saran-saran ini, Indonesia berpotensi menjadi contoh regulasi AI yang inovatif di kawasan Asia Tenggara.

DAFTAR PUSTAKA

Arifin, B. (2023). "Konstruksi Hukum *Vicarious Liability* dalam Konteks AI di Indonesia". Jurnal Ilmu Hukum, 12(3), 201-220.

Dewi, R. K. (2024). "*Black Box Effect* pada AI: Implikasi terhadap Pembuktian Mens Rea dalam Hukum Pidana". Jurnal Penelitian Hukum, 18(1), 75-92.

Gunawan, H. (2022). "*Strict Liability* untuk AI Berisiko Tinggi: Pelajaran dari Uni Eropa". Jurnal Teknologi dan Hukum, 9(4), 301-318.

Pratama, R. (2022). "Pertanggungjawaban Korporasi dalam Kejahatan Siber: Kajian atas UU ITE". Jurnal Hukum dan Teknologi, 5(2), 45-60.

Saimima, I. D. S. (2023). *"Deepfake dan UU ITE: Tantangan Regulasi Konten Digital di Era AI"*. Media Hukum, 30(1), 112-128.

Wicaksono, A. (2023). "*AI Liability*: Menggagas Tanggung Jawab Korporasi atas Teknologi Otonom". Hukumonline.com, diakses dari. https://www.hukumonline.com/berita/a/ai-liability-menggagas-tanggung-jawab-korporasi-atasteknologi-otonom

Muladi. (2010). Pertanggungjawaban Pidana Korporasi. Jakarta: Rajawali Pers.

Floridi, L. (2021). *The Ethics of Information. Oxford: Oxford University Press.*

Solaiman, S. M. (2021). *Legal Personhood for Artificial Intelligence. Cambridge: Cambridge University Press.*

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kitab Undang-Undang Hukum Pidana (KUHP).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.