Jurnal Kritis Studi Hukum

Vol. 10 No. 8 Tahun 2025
Halaman 6-13

BATAS PERTANGGUNGJAWABAN PIDANA PENGEMBANG ARTIFICIAL INTELLIGENCE PADA KEJAHATAN SIBER DI INDONESIA

Kesya Novita Angel[1], Evi Retno Wulan[2]
kesya0511@gmail.com[1] , evi.retno@narotama.ac.id[2],
Universitas Narotama

Abstrak

Perkembangan teknologi Artificial Intelligence (AI) membawa dampak besar dalam berbagai aspek kehidupan, termasuk munculnya peluang baru bagi terjadinya kejahatan siber. Salah satu isu penting yang muncul adalah mengenai batas pertanggungjawaban pidana pengembang AI dalam konteks hukum positif Indonesia. Permasalahan utamanya terletak pada bagaimana asas kesalahan yang menjadi dasar pemidanaan dalam hukum pidana dapat diterapkan terhadap pengembang yang keterlibatannya dengan tindak pidana sering kali bersifat tidak langsung. Penelitian ini menggunakan pendekatan yuridis normatif dengan menelaah Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 Undang-Undang No. 1 Tahun 2024, serta literatur hukum dan wacana internasional mengenai regulasi AI. Hasil kajian menunjukkan bahwa pengembang dapat dimintai pertanggungjawaban pidana apabila terbukti secara sengaja menciptakan atau memodifikasi AI untuk melakukan atau memfasilitasi kejahatan siber, maupun apabila terbukti lalai dalam melaksanakan kewajiban kehati-hatian sehingga menimbulkan risiko penyalahgunaan. Jika penyalahgunaan AI dilakukan oleh pihak ketiga tanpa adanya kesalahan dari pengembang, maka tanggung jawab pidana tidak dapat dibebankan. Kondisi ini menunjukan adanya kekosongan norma dalam UU ITE yang belum mengatur secara spesifik posisi pengembang. Untuk menghindari ketidakpastian hukum, diperlukan pengaturan eksplisit mengenai batas pertanggungjawaban pengembang AI, termasuk kriteria kesalahan, indikator hubungan kausal, serta kewajiban due diligence. Dengan demikian, hukum Indonesia dapat memberikan kepastian hukum sekaligus mendorong iklim inovasi yang aman.

Kata Kunci: Artificial Intelligence, Kejahatan Siber, Pertanggungjawaban Pidana, Hukum Positif Indonesia, UU ITE.

Abstract

The development of Artificial Intelligence (AI) technology has had a significant impact on various aspects of life, including the emergence of new opportunities for cybercrime. One important issue that has emerged is the limits of criminal liability for AI developers within the context of Indonesian positive law. The main problem lies in how the principle of fault, which is the basis for criminal punishment in criminal law, can be applied to developers whose involvement in criminal acts is often indirect. This study uses a normative juridical approach by examining the Criminal Code (KUHP), Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments through Law Number 19 of 2016 and Law Number 1 of 2024, as well as legal literature and international discourse on AI regulation. The results of the study indicate that developers can be held criminally liable if proven to have intentionally created or modified AI to commit or facilitate cybercrime, or if proven negligent in carrying out their duty of care, thus creating a risk of misuse. If the misuse of AI is carried out by a third party without any fault on the part of the developer, criminal responsibility cannot be imposed. This situation indicates a gap in the ITE Law, which does not specifically regulate the position of developers. To avoid legal uncertainty, explicit regulations are needed regarding the limits of AI developers' liability, including criteria for fault, indicators of causal relationships, and due diligence obligations. This way, Indonesian law can provide legal certainty while fostering a safe innovation climate.

***Keywords**: Artificial Intelligence, Criminal Liability, Cybercrime, Indonesian Positive Law, ITE Law.*

PENDAHULUAN

Dalam satu dekade terakhir, Artificial Intelligence (AI) telah berkembang menjadi salah satu teknologi paling berpengaruh di dunia. AI kini digunakan dalam berbagai sektor, mulai dari industri manufaktur, transportasi, kesehatan, pendidikan, hingga layanan publik. Perkembangan teknologi digital pada abad ke-21 menghadirkan perubahan besar dalam kehidupan manusia. Salah satu inovasi yang paling menonjol adalah hadirnya Artificial Intelligence (AI) atau kecerdasan buatan yang telah memasuki berbagai lini kehidupan, mulai dari sektor ekonomi, kesehatan, pendidikan, transportasi, hingga keamanan siber. AI tidak hanya mempermudah pekerjaan manusia, tetapi juga membuka peluang baru bagi efisiensi dan produktivitas. Namun, seiring dengan manfaat yang dihadirkan, AI juga menimbulkan tantangan hukum, etika, serta persoalan tanggung jawab pidana ketika teknologi tersebut digunakan secara tidak tepat atau bahkan disalahgunakan untuk melakukan tindak pidana, khususnya kejahatan siber.

Di Indonesia, percepatan transformasi digital telah mendorong adopsi Artificial Intelligence (AI) pada skala yang semakin luas. Pemerintah, sektor swasta, hingga masyarakat memanfaatkan teknologi ini untuk mengotomatisasi pekerjaan, meningkatkan akurasi analisis data, serta mempercepat proses pengambilan keputusan dalam berbagai bidang. AI pada dasarnya menawarkan efisiensi dan inovasi yang signifikan, namun kemajuan ini juga membawa konsekuensi hukum yang tidak sederhana. Salah satu konsekuensi tersebut terlihat dalam konteks kejahatan siber (cybercrime), yakni bentuk kejahatan modern yang memanfaatkan jaringan komputer, internet, maupun perangkat digital sebagai sarana utama. Kejahatan siber mencakup berbagai modus, mulai dari peretasan (hacking), penyebaran malware, pencurian data pribadi, hingga penyalahgunaan teknologi deepfake yang memanipulasi visual maupun audio. Dalam perkembangannya, AI tidak hanya menjadi alat bantu, melainkan juga berpotensi menjadi instrumen utama yang memungkinkan pelaku kejahatan beroperasi dengan cara yang semakin kompleks.

AI memiliki kemampuan untuk memproses informasi, mengambil keputusan, bahkan melakukan tindakan tertentu secara otonom tanpa keterlibatan manusia secara langsung. Keunggulan ini di satu sisi memberikan manfaat besar, namun di sisi lain juga menimbulkan risiko baru ketika AI disalahgunakan. Fenomena seperti deepfake, manipulasi data biometrik, serangan siber otomatis, hingga penipuan berbasis rekayasa visual atau suara merupakan bentuk nyata dari ancaman yang ditimbulkan. Kejahatan berbasis AI sering kali sulit dideteksi maupun dilacak, karena pelaku dapat memanfaatkan sifat anonim internet serta kecanggihan algoritma untuk menghindari identifikasi

Di sisi lain, sistem hukum pidana Indonesia berpegang pada prinsip geen straf zonder schuld (tiada pidana tanpa kesalahan) yang mengharuskan adanya kesengajaan (dolus) atau kelalaian (culpa) dari pelaku. Namun, problematika muncul ketika AI, yang diciptakan oleh pengembang, memiliki kemampuan untuk belajar, beradaptasi, bahkan mengambil keputusan secara mandiri tanpa instruksi langsung dari penciptanya. Pada titik tertentu, batas antara tanggung jawab pengembang sebagai pencipta dan otonomi AI sebagai entitas teknologi menjadi semakin kabur. Permasalahan yang muncul adalah bagaimana prinsip pertanggungjawaban pidana dapat diterapkan kepada pengembang AI yang pada dasarnya tidak memiliki niat atau pengetahuan bahwa teknologi yang mereka hasilkan akan digunakan untuk melakukan tindak pidana. Pertanyaan mendasar pun timbul: apakah seorang pengembang dapat dimintai pertanggungjawaban pidana hanya karena menciptakan teknologi yang kemudian disalahgunakan oleh pihak lain?

Dalam konteks hukum Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi , Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 , dan perubahan terakhir melalui Undang-Undang Nomor 1 Tahun 2024

yang disebutkan sebagai UU ITE memang telah mengatur berbagai bentuk tindak pidana siber. Namun, undang-undang tersebut belum secara spesifik membedakan posisi serta tanggung jawab antara pengguna, penyedia layanan, dan pengembang teknologi. Kekosongan norma ini menimbulkan ruang abu-abu dalam praktik penegakan hukum, yang pada akhirnya membuka peluang bagi interpretasi subjektif aparat penegak hukum.

Kondisi demikian tentu berisiko menimbulkan kriminalisasi berlebihan terhadap pengembang AI yang sejatinya tidak memiliki kesalahan maupun niat jahat dalam penggunaan teknologinya. Perubahan lanjutan melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE memang membawa sejumlah pembaruan signifikan, seperti penghapusan pasal yang kerap dianggap multitafsir, penambahan ketentuan mengenai perlindungan anak dalam ruang digital, hingga pemberian kewenangan lebih luas kepada aparat penegak hukum untuk melakukan pemblokiran maupun penutupan akses terhadap akun atau sistem elektronik tertentu. Meskipun demikian, revisi terbaru ini tetap belum menyentuh isu fundamental mengenai pertanggungjawaban pidana pengembang AI. Artinya, sekalipun UU ITE telah mengalami dua kali perubahan, regulasi yang ada masih belum mampu menjawab secara tegas bagaimana menempatkan posisi pengembang ketika teknologi ciptaannya digunakan untuk melakukan tindak pidana, sehingga problem kekosongan hukum (legal gap) dalam hal ini masih berlanjut

Ketiadaan pengaturan yang jelas semakin mempertegas adanya legal gap dalam sistem hukum nasional. UU ITE pada dasarnya dirancang untuk menghadapi tindak pidana siber dengan subjek hukum manusia dan korporasi, namun belum mampu menjangkau kemungkinan kejahatan yang melibatkan AI sebagai entitas yang berperan dalam pengambilan keputusan secara otonom. Hal ini berpotensi menimbulkan ketidakpastian hukum, baik bagi aparat penegak hukum maupun para pengembang AI. Sementara itu, standar internasional pun masih berada dalam tahap pencarian format regulasi yang ideal. Uni Eropa, misalnya, tengah mengembangkan AI Act yang secara komprehensif membahas risiko serta tanggung jawab baik pengembang maupun pengguna AI. Perkembangan ini menunjukkan bahwa isu mengenai batas pertanggungjawaban pidana pengembang AI tidak hanya menjadi persoalan domestik, melainkan juga merupakan isu global yang menuntut adaptasi cepat dari setiap sistem hukum, termasuk Indonesia.

Urgensi pembahasan mengenai batas pertanggungjawaban pidana pengembang AI dalam kejahatan siber di Indonesia semakin nyata karena tiga hal. Pertama, penggunaan AI dalam berbagai aspek kehidupan digital kian meluas dan berpotensi besar untuk disalahgunakan. Kedua, keterbatasan kerangka hukum nasional membuat Indonesia belum memiliki instrumen hukum yang memadai untuk menghadapi fenomena baru tersebut. Ketiga, adanya kebutuhan mendesak untuk menciptakan kepastian hukum yang mampu melindungi masyarakat dari dampak negatif kejahatan siber sekaligus mencegah kriminalisasi berlebihan terhadap pengembang teknologi yang tidak bersalah.

Sehubungan dengan hal tersebut diatas, penelitian ini penting dilakukan untuk menelaah sejauh mana UU ITE mampu mengakomodasi perkembangan teknologi AI, khususnya dalam menentukan batas pertanggungjawaban pidana pengembang. Melalui kajian mendalam, diharapkan dapat dirumuskan konstruksi hukum yang lebih tepat, sehingga tercapai keseimbangan antara perlindungan masyarakat dari bahaya kejahatan siber dengan perlindungan terhadap pengembang AI agar tidak dibebani tanggung jawab pidana secara tidak proporsional.Keseimbangan antara perlindungan masyarakat dari dampak negatif teknologi dan perlindungan kebebasan berinovasi menjadi isu krusial. Regulasi yang terlalu ketat dapat menghambat perkembangan teknologi, sedangkan regulasi yang terlalu longgar berpotensi membuka celah penyalahgunaan. Oleh karena itu, diperlukan kajian yang mendalam untuk menentukan sejauh mana pengembang AI dapat dimintai pertanggungjawaban pidana atas kejahatan siber, sehingga dapat dirumuskan pengaturan yang adil, jelas, dan sejalan dengan perkembangan teknologi.

METODE

Penelitian ini menggunakan metode hukum normatif (yuridis normatif) yang bertumpu pada studi kepustakaan dengan menelaah bahan hukum yang relevan. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan mengkaji Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, Kitab Undang-Undang Hukum Pidana (KUHP), serta regulasi terkait lainnya; pendekatan konseptual (*conceptual approach*) dengan menelaah doktrin hukum pidana, asas pertanggungjawaban pidana, serta konsep tanggung jawab pengembang teknologi; dan pendekatan komparatif (*comparative approach*) dengan membandingkan praktik internasional, misalnya *European Union AI Act*, guna memperkaya analisis terhadap kekosongan norma dalam hukum Indonesia. Sumber bahan hukum terdiri atas bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa buku, jurnal, artikel ilmiah, serta pendapat pakar, dan bahan hukum tersier berupa kamus hukum serta sumber penunjang lainnya. Seluruh bahan hukum dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis menggunakan metode deskriptif-kualitatif, yaitu dengan menguraikan serta menafsirkan aturan dan doktrin yang ada untuk kemudian dikaitkan dengan permasalahan penelitian. Analisis ini diharapkan dapat mengidentifikasi kekosongan hukum sekaligus memberikan tawaran konsep mengenai batas pertanggungjawaban pidana pengembang *AI* dalam kejahatan siber di Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/AI) di Indonesia telah menghadirkan peluang sekaligus tantangan yang signifikan. Dalam era transformasi digital, *AI* dimanfaatkan tidak hanya oleh sektor swasta, melainkan juga oleh pemerintah dan masyarakat luas untuk menunjang produktivitas, mengotomatisasi pekerjaan, serta meningkatkan kualitas analisis data.[1] Namun, kemajuan ini juga menimbulkan risiko baru berupa penyalahgunaan teknologi untuk tujuan yang melanggar hukum, khususnya dalam ranah kejahatan siber (*cybercrime*). Kejahatan berbasis siber di Indonesia kian beragam, meliputi peretasan sistem komputer, pencurian data pribadi, penyebaran *malware*, hingga penggunaan teknologi *deepfake* untuk menyebarkan konten manipulatif baik secara visual maupun audio. Fenomena ini tidak hanya mengganggu stabilitas keamanan digital, tetapi juga menimbulkan persoalan serius dalam aspek hukum pidana.[2]

Salah satu tantangan mendasar adalah bagaimana menentukan batas pertanggungjawaban pidana terhadap pengembang *AI*. Sebab, *AI* memiliki karakteristik unik berupa kemampuan mengambil keputusan secara otonom, memproses data secara mandiri, dan menghasilkan output yang tidak selalu dapat diprediksi bahkan oleh penciptanya sendiri.[3] Dengan kata lain, *AI* bukan sekadar alat pasif, melainkan sistem yang dapat bertindak berdasarkan algoritma kompleks. Hal ini menimbulkan dilema hukum, karena hukum pidana Indonesia selama ini didasarkan pada asas klasik yang menempatkan manusia sebagai subjek hukum yang dapat dimintai pertanggungjawaban.[4]

Prinsip fundamental hukum pidana Indonesia, sebagaimana juga dianut secara

---

[1] Sinta Dewi Rosadi, *Hukum Siber Indonesia*, Refika Aditama bandung 2020 h 56.

[2] Imam Subekti, Heru Sukrisno, Sugeng Wahyudi, et al., "*Reformulasi Kebijakan Kriminal Dalam Penanggulangan Kejahatan Berbasis Teknologi Kecerdasan Buatan*" Setara jurnal ilmu hukum 2024 h. 68.

[3] Muhammad Dahria, "*Kecerdasan Buatan (Artificial Intelligence)*," Jurnal Saintikom vol V no 2 agustus 2008, h 187.

[4] Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, dan Femmy Silaswaty Faried, "*Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia,*" Jurnal USM Law Review, h 3.

universal, adalah asas *geen straf zonder schuld* (tiada pidana tanpa kesalahan). Asas ini menekankan bahwa seseorang hanya dapat dipidana apabila memiliki kesalahan yang nyata, baik dalam bentuk kesengajaan (*dolus*) maupun kelalaian (*culpa*). Dengan demikian, untuk dapat menjerat pengembang *AI* ke ranah pidana, harus terlebih dahulu dibuktikan adanya unsur kesalahan yang melekat pada dirinya. Apabila seorang pengembang merancang *AI* dengan tujuan yang sah, mematuhi standar teknis yang berlaku, serta melakukan langkah-langkah *preventif* untuk mencegah penyalahgunaan, maka pada dasarnya ia tidak dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukan oleh pengguna atau pihak ketiga.[5]

Dalam, pengaturan mengenai kejahatan siber terutama terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan diperbarui kembali melalui Undang-Undang Nomor 1 Tahun 2024. Undang-undang ini memang telah mengatur sejumlah tindak pidana seperti akses ilegal, manipulasi data elektronik, serta penyebaran konten terlarang. Akan tetapi, UU ITE maupun UU 1 tahun 2024 belum secara tegas membedakan kedudukan hukum antara pengguna, penyedia platform, dan pengembang teknologi. Akibatnya, terdapat kekosongan norma yang menimbulkan ruang abu-abu dalam praktik penegakan hukum. Kondisi ini berpotensi menyebabkan kriminalisasi berlebihan terhadap pengembang *AI* yang sesungguhnya tidak memiliki niat jahat ataupun keterlibatan langsung dalam tindak pidana yang dilakukan melalui teknologinya.[6]

Untuk menilai batasan pertanggungjawaban pidana pengembang *AI*, terdapat beberapa parameter yang dapat dianalisis dari sudut hukum pidana Indonesia. [7]Pertama, unsur kesengajaan (*dolus*). Jika terbukti bahwa pengembang secara sadar merancang *AI* untuk tujuan melawan hukum misalnya menciptakan malware otomatis, aplikasi peretasan, atau sistem botnet untuk serangan siber maka pertanggungjawaban pidana jelas dapat dibebankan. Kedua, unsur kelalaian (*culpa*). Dalam hal pengembang tidak bermaksud jahat, tetapi lalai memenuhi kewajiban kehati-hatian, ia tetap dapat dimintai pertanggungjawaban. Kelalaian dapat berupa tidak memasang fitur keamanan dasar, tidak melakukan uji risiko, atau membiarkan celah keamanan yang seharusnya dapat dicegah dengan standar keahlian yang wajar.[8]

Ketiga, adanya hubungan kausalitas. Pertanggungjawaban pidana tidak mungkin dibebankan apabila tidak terdapat hubungan sebab akibat antara tindakan pengembang dengan tindak pidana yang terjadi. Misalnya, apabila *AI* telah dirancang dengan standar tinggi namun diretas dan dimodifikasi oleh pihak ketiga, maka pengembang tidak dapat dipidana karena tindak pidana timbul akibat perbuatan orang lain. Keempat, adanya kewajiban kehati-hatian *(duty of care)*. Dalam konteks ini, pengembang dituntut untuk mematuhi standar tertentu dalam desain, uji coba, dan penerapan teknologi agar risiko penyalahgunaan dapat diminimalkan. Kewajiban ini bersifat preventif dan bertujuan melindungi pengguna maupun masyarakat dari potensi bahaya *AI*.

Contoh Bayangkan seorang pengembang menciptakan aplikasi *deepfake* untuk kepentingan industri kreatif. Aplikasi ini digunakan dalam produksi film atau iklan dengan

---

[5] Irawati Nastasia *Analisis yuridis atas kedudukan hukum & peran artificial intelligence (AI) dalam sistem hukum acara perdata indonesia*, Skripsi Fakultas Hukum Universitas Kristem Indonesia Tahun 2024, h 8

[6] Bunga Dewi, "*Politik Hukum Pidana Terhadap Penanggulangan Cybercrime*" Jurnal Legislasi Indonesia, Vol 16, No. 1 (2019): h 1–5.

[7] Ni Made Yordha Ayu Astiti," *Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban?*" undayana master law jounal, 2023.

[8] Nasman, Pudji Astuti dan Dita Perwitasari *Etika Dan Pertanggungjawaban Penggunaan Artificial Intelligence Di Indonesia* Jurnal Hukum Lex Generalis. (2024).

izin pihak terkait. Namun, salah satu pengguna memanfaatkan aplikasi tersebut untuk membuat konten pornografi palsu dengan wajah tokoh publik, lalu menyebarkannya secara daring.[9] Dalam situasi ini, pelaku tindak pidana jelas adalah penyebar konten, bukan pengembang. Akan tetapi, apabila terbukti bahwa pengembang tidak memasang filter peringatan, mekanisme kontrol, atau panduan penggunaan yang jelas, maka ia bisa dianggap lalai dan berpotensi dimintai pertanggungjawaban.[10]

Contoh lain, seorang pengembang membuat chatbot berbasis *AI* untuk layanan perbankan. Chatbot ini didesain untuk menjawab pertanyaan nasabah. Namun karena lemahnya sistem keamanan, chatbot justru dapat dimanipulasi untuk membocorkan data pribadi nasabah. Jika terbukti pengembang tidak memenuhi standar keamanan minimum, maka ia dapat dinilai lalai sehingga pertanggungjawaban pidana menjadi relevan. Sebaliknya, jika standar keamanan sudah diterapkan tetapi serangan siber canggih tetap mampu menembusnya, maka pengembang tidak dapat dipidana karena telah menjalankan kewajiban kehati-hatiannya.

Dari uraian tersebut, dapat disimpulkan bahwa batas pertanggungjawaban pidana pengembang AI dalam hukum positif Indonesia setidaknya meliputi tiga kriteria utama:

a) adanya kesalahan baik dalam bentuk kesengajaan maupun kelalaian;
b) adanya hubungan kausalitas yang jelas antara perbuatan pengembang dengan tindak pidana yang terjadi; dan
c) adanya pelanggaran terhadap kewajiban kehati-hatian dalam merancang serta mengimplementasikan teknologi. Tanpa terpenuhinya ketiga kriteria ini, pemidanaan terhadap pengembang berpotensi bertentangan dengan asas legalitas dan asas kesalahan yang menjadi dasar sistem hukum pidana nasional.

Urgensi pengaturan lebih lanjut dalam peraturan perundang-undangan menjadi semakin jelas. Mengingat AI memiliki potensi penyalahgunaan yang tinggi, pengembang memang tidak bisa sepenuhnya dilepaskan dari tanggung jawab. Akan tetapi, regulasi yang tidak jelas justru menimbulkan ketidakpastian hukum dan risiko kriminalisasi. Oleh karena itu, pembaruan UU ITE maupun pembentukan undang-undang khusus yang mengatur AI sangat diperlukan. Regulasi ini dapat mencakup penetapan standar teknis minimal, prosedur uji risiko, hingga kewajiban audit etika teknologi. Dengan adanya pengaturan yang lebih tegas, pengembang yang beritikad baik akan terlindungi, sementara pengembang yang lalai atau sengaja menyalahgunakan AI tetap dapat dimintai pertanggungjawaban pidana secara proporsional.

SIMPULAN

Berdasarkan uraian dan analisis yang telah dilakukan, dapat disimpulkan bahwa pertanggungjawaban pidana pengembang *Artificial Intelligence (AI)* dalam konteks kejahatan siber di Indonesia masih menghadapi problematika konseptual maupun yuridis. Hukum pidana Indonesia, yang berlandaskan pada asas kesalahan sebagaimana termuat dalam KUHP, pada dasarnya hanya memungkinkan seseorang dipidana apabila dapat dibuktikan adanya unsur kesengajaan atau kelalaian. Prinsip ini menjadi tantangan ketika dihadapkan pada persoalan pengembang *AI*, sebab hubungan antara pengembang dengan tindak pidana yang dilakukan melalui atau dengan menggunakan *AI* sering kali bersifat tidak langsung.

Dalam khususnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 serta diperbarui dengan Undang-Undang Nomor 1 Tahun 2024, belum

[9] Renata Christha Auli, "*Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya*," Hukum Online, January 19, 2024.

[10] Adnasohn Aqilla Respati., "*Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban*" Media Hukum Indonesia (MHI). (2024).

terdapat ketentuan yang secara eksplisit memisahkan ataupun merinci tanggung jawab pidana antara pengguna, penyedia layanan, dan pengembang teknologi. Kekosongan norma ini menimbulkan ruang abu-abu dalam penegakan hukum, yang membuka peluang interpretasi subjektif aparat penegak hukum dan berpotensi menyebabkan kriminalisasi berlebihan terhadap pengembang yang sebenarnya tidak memiliki niat jahat maupun keterlibatan langsung dalam suatu tindak pidana.

Batasan pertanggungjawaban pidana pengembang *AI* idealnya harus dirumuskan dengan mempertimbangkan indikator kesalahan. Pengembang dapat dimintai pertanggungjawaban apabila terbukti secara sadar menciptakan, mengembangkan, atau menyediakan teknologi dengan maksud untuk melakukan atau memfasilitasi tindak pidana siber. Unsur kesengajaan terpenuhi apabila pengembang sejak awal mengetahui dan menghendaki akibat yang melanggar hukum dari teknologinya. Sementara itu, dalam hal kelalaian, pengembang dapat dipertanggungjawabkan jika terbukti tidak melakukan kewajiban kehati-hatian atau kelaziman tertentu, misalnya dengan tidak melengkapi sistem *AI* dengan fitur pengamanan yang layak, sehingga membuka celah bagi penyalahgunaan oleh pihak lain. Namun, jika *AI* diciptakan untuk tujuan sah dan penyalahgunaan dilakukan sepenuhnya oleh pihak ketiga tanpa adanya kesalahan dari pengembang, maka seharusnya pertanggungjawaban pidana tidak dibebankan kepadanya.

Dalam konteks internasional, muncul gagasan mengenai penerapan *strict liability* terhadap pengembang *AI* dalam kondisi tertentu, terutama apabila produk teknologi yang diciptakan berisiko tinggi. Akan tetapi, penerapan konsep ini di Indonesia perlu dipertimbangkan secara hati-hati karena berpotensi bertentangan dengan asas kesalahan yang menjadi prinsip fundamental hukum pidana nasional. Alternatif yang lebih proporsional adalah dengan mengadopsi *due diligence obligation*, yakni kewajiban pengembang untuk memastikan bahwa teknologi yang dibuat telah dirancang secara aman, disertai mekanisme pencegahan terhadap penyalahgunaan, serta memberikan transparansi dan akuntabilitas atas potensi risiko.

Dengan demikian, batasan pertanggungjawaban pidana bagi pengembang *AI* atas kejahatan siber dalam perspektif hukum positif Indonesia hanya dapat dibebankan apabila terpenuhi syarat adanya kesalahan dalam bentuk kesengajaan atau kelalaian yang dapat dibuktikan, serta adanya hubungan kausal yang jelas antara tindakan pengembang dengan akibat pidana yang ditimbulkan. Pengaturan hukum yang lebih spesifik dan eksplisit sangat diperlukan, baik melalui pembaruan UU ITE maupun regulasi khusus mengenai *AI*, agar tercipta kepastian hukum, keadilan, serta keseimbangan antara perlindungan masyarakat dari dampak negatif kejahatan siber dan perlindungan terhadap pengembang *AI* agar tidak menjadi korban kriminalisasi yang tidak proporsional.

DAFTAR PUSTAKA

Buku

Sinta Dewi Rosadi, Hukum Siber Indonesia, Refika Aditama bandung 2020 h 56.

Jurnal

Adnasohn Aqilla Respati., "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban" Media Hukum Indonesia (MHI). (2024).

Budi Raharjo , Teori Etika Dalamn Kecerdasan Buatan Artificel Intelligence , Yayasan prima agus Teknik , Semarang , h.110.

Bunga Dewi, "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime" Jurnal Legislasi Indonesia, Vol 16, No. 1 (2019): h 1–5.

Irawati Nastasia Analisis yuridis atas kedudukan hukum & peran artificial intelligence (AI) dalam sistem hukum acara perdata indonesia, Skripsi Fakultas Hukum Universitas Kristem Indonesia Tahun 2024, h 8

Muhammad Dahria, "Kecerdasan Buatan (Artificial Intelligence)," Jurnal Saintikom vol V no 2 agustus 2008, h 187.

Muhammad Dhafin Saptari , Arificial Intellicence sebagai entitas subjek hukum perdata , Skripsi

Fakultas Hukum Universitas Katolik Parahryangan , Tahun 2022, h 10.
Nasman, Pudji Astuti dan Dita Perwitasari Etika Dan Pertanggungjawaban Penggunaan Artificial Intelligence Di Indonesia Jurnal Hukum Lex Generalis. (2024).
Ni Made Yordha Ayu Astiti," Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban?" undayana master law jounal, 2023.
Renata Christha Auli, "Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya," Hukum Online, January 19, 2024.
Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, dan Femmy Silaswaty Faried, "Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia," Jurnal USM Law Review, h 3.

Website

Grace Shao, What 'DEEPFAKE' are and how they may be dangerous, CNBC, 13 September 2019, https://www.cnbc.com/2019/10/14/what-is-DEEPFAKE-and-how-it-might-be-dangerous.html, diakses pada 29 Maret 2025