Jurnal Ilmiah
F E N O M E N A
P-ISSN; 3047-7204, E-ISSN; 0215-1448
https://unars.ac.id/ojs/index.php/fenomena/index

REKONTRUKSI PERTANGGUNGJAWABAN HUKUM ATAS KEJAHATAN SIBER BERBASIS ARTIFICIAL INTELLIGENCE DALAM PERSPEKTIF HUKUM PIDANA INDONESIA

RECONSTRUCTION OF LEGAL RESPONSIBILITY FOR CYBERCRIMES BASED ON ARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF INDONESIAN CRIMINAL LAW

Dyah Silvana Amalia[1], Siti Masruroh[2], Safina Husnul Khotimah[3]
[1,2,3]Jurusan Hukum, Ilmu Hukum, Universitas Abdurachman Shaleh Situbondo
Email: [2]sitimasruroh1037@gmail.com

ABSTRAK

Perkembangan teknologi *Artificial Intelligence* (AI) telah memberikan dampak signifikan terhadap berbagai sektor kehidupan, termasuk dalam ranah kejahatan siber. Pemanfaatan AI dalam aktivitas digital tidak hanya membawa manfaat, tetapi juga menimbulkan potensi penyalahgunaan yang melahirkan bentuk-bentuk kejahatan siber baru yang semakin kompleks, seperti deepfake, automated hacking, hingga manipulasi data secara cerdas. Kondisi ini menimbulkan tantangan bagi sistem hukum pidana Indonesia, khususnya terkait dengan pertanggungjawaban hukum terhadap pelaku kejahatan siber yang melibatkan teknologi AI. Penelitian ini bertujuan untuk menganalisis konsep pertanggungjawaban hukum atas kejahatan siber berbasis AI serta merekonstruksi model pertanggungjawaban yang relevan dalam perspektif hukum pidana Indonesia.

***Kata kunci**: Artificial Intelligence* (AI), kejahatan siber, pertanggungjawaban hukum pidana, rekonstruksi hukum, hukum pidana Indonesia

ABSTRACT

including the realm of cybercrime. The use of AI in digital activities not only provides benefits but also creates the potential for misuse that leads to increasingly complex forms of cybercrime, such as deepfakes, automated hacking, and intelligent data manipulation. This condition poses challenges for the Indonesian criminal law system, particularly regarding legal liability for cybercrime offenders involving AI technology. This research aims to analyze the concept of legal liability for AI-based cybercrime and to reconstruct a relevant liability model within the perspective of Indonesian criminal law.

Keywords: *Artificial Intelligence (AI), cybercrime, criminal liability, legal reconstruction, Indonesian criminal law.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan besar terhadap tatanan kehidupan masyarakat global, termasuk di Indonesia. Perubahan ini ditandai dengan meluasnya penggunaan internet, perangkat digital, serta sistem berbasis *Artificial Intelligence* (AI) dalam berbagai bidang kehidupan manusia mulai dari pendidikan, bisnis, kesehatan, hingga pemerintahan dan interaksi sosial sehari-hari.

Namun, kemajuan ini tidak hanya membawa dampak positif. AI juga membuka celah baru bagi munculnya *Cyber Crime,* yaitu kejahatan yang dilakukan dengan menggunakan komputer, jaringan internet, atau perangkat digital sebagai sarana atau objek utama. Di era digital ini, *Cyber Crime* tidak hanya semakin kompleks, tetapi juga semakin sulit dideteksi dan ditindak secara hukum, terutama ketika para pelakunya memanfaatkan teknologi AI untuk mengaburkan identitas, memalsukan data, atau bahkan menjalankan kejahatan secara otomatis.[1]

Dalam sektor keuangan, AI digunakan untuk mendeteksi *fraud,* melakukan *credit scoring*, dan menjalankan *high- frequency trading*. Di bidang kesehatan, AI dimanfaatkan untuk diagnosis berbasis citra medis dan personalisasi pengobatan. Sementara itu, dalam sektor keamanan siber, AI digunakan untuk mendeteksi serangan siber secara *real-time* (Schwab, 2017). Namun demikian, sebagaimana teknologi pada umumnya, AI memiliki dua sisi: sebagai instrumen kemajuan sekaligus potensi risiko. AI dapat dimanfaatkan untuk melakukan berbagai bentuk tindak pidana, seperti *automated fraud*, manipulasi algoritma perdagangan saham, serangan siber terkoordinasi, pencurian data berbasis bot, hingga pembuatan *deepfake* untuk tujuan pemerasan atau disinformasi.[2]

---

[1] Barda Nawawi Arief, *Masalah Penegakan Hukum den Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Prenada Media, 2010, hlm. 76.

[2] Ancel, M. (1965). Social defence: *A modern approach to criminal problems*. Routledge & Kegan Paul.

Kemajuan teknologi *Artificial Intelligence* pada dasarnya memberikan berbagai manfaat dalam berbagai bidang kehidupan. Akan tetapi, di samping memberikan dampak positif, teknologi tersebut juga berpotensi disalahgunakan sebagai sarana untuk melakukan berbagai bentuk kejahatan siber. Pemanfaatan Artificial Intelligence dalam kejahatan siber dapat dilakukan melalui berbagai cara, seperti pembuatan dan penyebaran informasi palsu menggunakan teknologi *deepfake*, penipuan digital yang dilakukan secara otomatis, pencurian data pribadi, manipulasi sistem informasi, serta serangan siber yang dilakukan melalui jaringan komputer secara terstruktur.[3]

Kejahatan siber *(cyber crime*) sebagai kategori tindak pidana modern memiliki karakteristik unik yang membedakannya dari kejahatan konvensional. Aspek seperti anonimitas pelaku, kemudahan distribusi kejahatan secara massal, serta kemampuan melewati batas-batas yurisdiksi nasional menjadikan kejahatan ini sulit dijangkau dengan pendekatan hukum pidana tradisional. [4] Indonesia telah memiliki beberapa perangkat hukum yang mengatur tentang ruang siber, di antaranya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta didukung oleh instrumen lain seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Meskipun regulasi tersebut bertujuan untuk memberikan dasar hukum terhadap aktivitas elektronik dan menanggulangi kejahatan digital, praktik implementasinya tidak jarang menimbulkan kontroversi. Beberapa pasal dalam UU ITE, seperti Pasal 27 ayat (3) dan Pasal 28 ayat (2), sering kali dipandang mengandung ambiguitas normatif serta digunakan secara eksesif untuk membungkam ekspresi warga negara. Hal ini menunjukkan bahwa selain adanya kekosongan hukum pada jenis-jenis *cyber crime* tertentu, juga terdapat persoalan dalam aspek perlindungan hak konstitusional yang semestinya dijamin oleh UUD 1945. Situasi ini menunjukkan bahwa perangkat hukum yang ada belum

[3] Woodrow Barfield & Ugo Pagallo, "*Research Handbook on the Law of Artificial Intelligence*," *Edward Elgar Publishing*, 2018.

[4] Vannya Anastasya et al., "*Efektivitas Hukum Dan Kebijakan Publik Dalam Menghadapi Ancaman Siber Terhadap Keamanan Negara*" 3, no. 2 (2024): 1710–16.

sepenuhnya mampu mengimbangi kompleksitas kejahatan siber yang terus berkembang, baik secara teknis, yuridis, maupun filosofis.[5]

METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian hukum normatif, yaitu penelitian yang bertujuan menemukan kebenaran berdasarkan logika keilmuan hukum melalui penelaahan norma, asas, dan doktrin hukum. Penelitian ini memanfaatkan pendekatan konseptual dan pendekatan perundang-undangan untuk memahami konsep serta regulasi yang berkaitan dengan penegakan hukum pidana terhadap *Cyber Crime* berbasis AI di Indonesia. Sumber bahan penelitian terdiri dari bahan hukum primer seperti Pancasila, UUD 1945, KUHP, dan UU ITE; bahan hukum sekunder berupa publikasi dan kajian hukum; serta bahan hukum tersier seperti kamus dan ensiklopedia. Pengumpulan bahan dilakukan melalui studi kepustakaan dan penelusuran dokumen, kemudian diolah melalui proses sistematisasi berdasarkan tataran teknis, teleologis, dan sistematisasi eksternal.

Teknik pengolahan dilakukan melalui inventarisasi dan penyusunan sistematis peraturan perundang-undangan yang relevan, sedangkan teknik analisis menggunakan analisis kualitatif dengan mengaitkan bahan yang dihimpun dengan teori hukum dan penerapan dalam peraturan perundang-undangan. Kesimpulan penelitian ditarik dengan metode berpikir deduktif, yaitu berangkat dari pemahaman umum mengenai konsep dan kerangka hukum kemudian merumuskan kesimpulan khusus terkait kebijakan hukum pidana dalam menanggulangi *Cyber Crime* berbasis AI di Indonesia.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pidana terhadap Tindak Pidana *Cyber Crime* Berbasis *Artificial Intelligence* di Indonesia

Secara normatif, instrumen hukum pidana yang berlaku di Indonesia untuk menindak *Cyber Crime* masih mengacu pada Undang-Undang Nomor 11 Tahun

[5] Abdan Sifa, "Transformasi Digital E-Commerce Dalam Menguasai Kosentrasi Pasar Di Indonesia" 2, no. 12 (2024): 405–13.

2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang- Undang Nomor 1 Tahun 2024. Regulasi ini telah memberikan dasar hukum untuk menindak kejahatan yang menggunakan komputer dan jaringan internet. Meski instrumen ini memberikan dasar hukum terhadap tindak pidana cyber, namun terdapat kelemahan mendasar dan belum menyentuh secara spesifik karakteristik kejahatan yang dilakukan melalui atau dengan bantuan AI, yaitu:

Kekosongan definisi dan norma Definisi AI belum tersedia. Ketiadaan definisi yuridis yang jelas tentang apa yang dimaksud dengan AI menjadi hambatan utama dalam merumuskan hukum yang efektif, terutama dalam hukum pidana. Tanpa batasan yang jelas, sulit bagi penegak hukum untuk menerapkan norma-norma yang ada. Menurut penulis ada beberapa aspek yang menjelaskan mengapa ketiadaan definisi yuridis ini menjadi masalah: Pertama, Unsur Delik (*Corpus Delicti*). Dalam hukum pidana, unsur delik adalah fakta-fakta yang harus dibuktikan untuk menunjukkan bahwa suatu kejahatan telah terjadi. Tanpa definisi AI yang jelas, sulit untuk menentukan kapan suatu tindakan yang melibatkan AI dapat dianggap sebagai "tindakan kriminal". Ketiadaan definisi yang jelas membuat penentuan subjek hukum, objek hukum, dan perbuatan yang dilarang menjadi kabur. Kedua, Niat Jahat (*Mens Rea*). *Mens rea* adalah unsur psikologis dalam suatu tindak pidana, yang mengacu pada niat atau keadaan mental pelaku. Konsep ini menjadi sangat problematis dalam konteks AI karena: AI tidak memiliki kesadaran, niat, atau kehendak. AI beroperasi berdasarkan algoritma dan data yang diberikan. Bagaimana kita bisa membuktikan bahwa sebuah program memiliki niat jahat untuk melakukan sesuatu. Hukum pidana tradisional mengasumsikan bahwa pelaku adalah manusia yang memiliki akal budi dan kehendak bebas. Asumsi ini tidakberlaku pada AI. Akibatnya penegak hukum harus mencari "niat jahat" pada pencipta AI, *programmer*, atau pengguna, yang mungkin tidak memiliki niat jahat secara langsung.

Ketiga, Standar Pembuktian. Standar pembuktian adalah tingkat keyakinan yang diperlukan bagi hakim untuk memutuskan suatu perkara. Dalam kasus yang melibatkan AI, standar ini menjadi sulit diterapkan karena: Banyak model AI,

Kausalitas yang tidak jelas. Untuk mengatasi masalah ini menurut penulis, diperlukan kolaborasi yang erat antara ahli hukum, pembuat kebijakan, dan ahli teknologi. Karena beberapa negara dan organisasi internasional sudah mulai merancang kerangka hukum yang mencoba mendefinisikan AI berdasarkan fungsinya, risikonya, atau tingkat otonominya. Pendekatan ini mungkin lebih pragmatis dari pada mencoba memberikan satu definisi tunggal yang mencakup semua jenis AI.[6]

Dari sudut pandang sistem peradilan pidana, tantangan dalam penanganan kejahatan

Siber tidak hanya bersumber dari tidak jelasan norma, tetapi juga dari rendahnya kapasitas kelembagaan dalam menjawab dinamika kejahatan digital. Proses penyelidikan dan pembuktian dalam kasus *cyber crime* memerlukan keahlian forensik digital, infrastruktur teknologi mutakhir, serta kemampuan analisis data elektronik yang belum dimiliki secara merata oleh aparat penegak hukum. Hal ini menjadi hambatan serius dalam upaya penegakan hukum yang efektif dan akuntabel. Sebagai contoh, proses pelacakan pelaku kejahatan siber kerap terhambat oleh keterbatasan kerja sama internasional serta kurangnya mekanisme *mutual legal assistance* yang responsif dan cepat.

Dalam praktiknya, kejahatan siber sering kali melibatkan pelaku yang berada di yurisdiksi negara yang berbeda dengan lokasi korban maupun *server* tempat data disimpan. Kondisi ini menimbulkan kompleksitas dalam proses penegakan hukum karena aparat penegak hukum harus berkoordinasi dengan otoritas negara lain untuk memperoleh bukti elektronik maupun melakukan penangkapan terhadap pelaku. Tanpa adanya kerja sama internasional yang efektif, proses penegakan hukum terhadap kejahatan siber menjadi sulit dilakukan secara optimal

Selain itu, sifat kejahatan siber yang memungkinkan pelaku bertindak secara anonim serta memanfaatkan teknologi enkripsi semakin mempersulit proses

[6] Eka Nanda Ravizki dan Lintang Yudhantaka, "*Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia*", Notaire Journal of notarial law, Vol. 5 No. 3 Oktober 2022, hlm. 353.

pengungkapan identitas pelaku. Pelaku kejahatan dapat menyamarkan identitasnya dengan berbagai cara, seperti menggunakan *virtual private network* (VPN), jaringan anonim, maupun sistem komunikasi yang terenkripsi sehingga proses pelacakan oleh aparat penegak hukum menjadi lebih rumit. Kondisi tersebut menuntut aparat penegak hukum untuk memiliki kemampuan teknis yang memadai serta dukungan teknologi yang canggih agar proses penyelidikan dan investigasi dapat dilakukan secara efektif.

Oleh karena itu, diperlukan langkah-langkah strategis untuk memperkuat sistem peradilan pidana dalam menghadapi perkembangan kejahatan berbasis teknologi informasi. Salah satu langkah yang dapat ditempuh adalah dengan meningkatkan kompetensi aparat penegak hukum melalui pelatihan khusus di bidang forensik digital serta memperkuat kerja sama internasional dalam menangani kejahatan lintas negara. Di samping itu, pembaruan regulasi juga menjadi hal yang penting agar hukum dapat mengikuti perkembangan teknologi yang sangat cepat, sehingga mampu memberikan perlindungan yang optimal bagi masyarakat dari berbagai ancaman kejahatan siber.[7]

Kebijakan Hukum Pidana dalam Menanggulangi Cyber Crime Berbasis Artificial Intelligence di Indonesia yang Akan Datang

Regulasi hukum pidana mengenai penanggulangan *Cyber Crime* khusus nya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi instrumen utama yang sangat penting. Namun, meskipun undang-undang sudah ada, tetapi pelaksanaannya belum mampu mengakomodir permasalahan yang ada. Beberapa keterbatasan dalam hukum positif dalam rangka penanggulangan *Cyber Crime* berbasis AI diantaranya ialah:

a. Ketiadaan regulasi khususnya AI Cyber Crime
b. Definisi dan ruang lingkup Cyber Crime dalam UU ITE cenderung bersifat umum, sehingga belum mampu mencakup kejahatan berbasis AI

[7] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia* (Bandung: Refika Aditama, 2010), 95.

c. Kurangnya kapasitas kemampuan aparat penegak hukum khususnya berkaitan dengan identifikasi dan penanganan *Cyber Crime* berbasis kecerdasan buatan.

Pembaharuan kebijakan hukum mengenai penanggulangan kejahatan siber dengan basis AI saat ini sangat mendesak. Hal ini tentunya disebabkan karena adanya kekosongan hukum di mana belum ada regulasi yang mengatur secara detail dan rinci mengenai permasalahan *Cyber Crime* berbasis AI di Indonesia. Kekosongan hukum yang mengatur mengenai AI di Indonesia ini khususnya yang berkaitan dengan kedudukan tanggung jawab AI dalam industri hukum di Indonesia. Kekosongan hukum dalam bidang AI inilah yang menyebabkan banyak praktisi hukum masih memanfaatkan pengaturan yang berkaitan dengan regulasi bidang teknologi untuk menanggapi permasalahan di bidang kecerdasan buatan, salah satunya melalui UU ITE.[8]

Berdasarkan permasalahan kekosongan hukum di bidang AI, perlu antisipasi dari segala kemungkinan yang bisa muncul akibat kurangnya regulasi di bidang AI. Dalam regulasi baru ini nantinya diharapkan ada pertimbangan yang rinci dan jelas berkaitan dengan kedudukan AI dalam pertanggungjawaban hukum. Secara eksplisit, AI memang dapat melakukan perbuatan hukum layaknya subjek hukum yang ada. Namun dalam praktiknya, AI merupakan sistem yang dibangun manusia dan tidak dapat berperan sebagai subjek hukum. Oleh sebab itulah diperlukan adanya penafsiran secara terperinci dalam regulasi hukum baru yang mengatur secara jelas mengenai kecerdasan buatan, khususnya dalam rangka penanggulangan kejahatan siber berbasis AI dalam hukum Indonesia. Seperti yang diketahui bersama, AI kedudukannya masih sangat kabur di Indonesia. UU ITE dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi, dimana dua produk hukum ini pun tidak menyebutkan AI secara jelas, hanya diksi "Agen Elektronik" saja yang dijelaskan dalam kedua peraturan tersebut. Regulasi mengenai AI belum diatur dalam KUHP Nasional UU No 1 tahun 2023. Dalam KUHP Nasional UU No 1 tahun 2023, yang diatur hanyalah mengenai kejahatan siber atau *Cyber Crime*

[8] Ni Made Yordha Ayu Astiti. "*Strict Llliability of Artificial Intelegence: Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban*". Jurnal Magister Hukum Udayana. Vol. 12, No. 4, Desember 2023, hlm. 969.

saja. Namun instrumen *Cyber Crime* dalam KUHP Nasional UU No 1 tahun 2023 yang sudah disusun juga sangat penting sebagai salah satu instrumen hukum yang mengatur kejahatan dengan menggunakan media teknologi dan internet. Regulasi baru dalam menghadapi *Cyber Crime* dalam KUHP Nasional UU No 1 tahun 2023 diantaranya seperti *hacking*, pencurian data, hingga penyebaran *malware*. Ini menunjukkan bahwa Undang-Undang Nomor 1 Tahun 2024 memiliki landasan hukum yang lebih kuat dibandingkan regulasi sebelumnya dengan menjelaskan unsur-unsur tindak pidana secara lebih rinci.[9]

KESIMPULAN

Bahwa kejahatan siber yang dilakukan dengan memanfaatkan teknologi *Artificial Intelligence* pada dasarnya dapat dikualifikasikan sebagai tindak pidana dalam hukum pidana Indonesia. Hal ini dikarenakan penggunaan teknologi tersebut tetap dapat memenuhi unsur-unsur tindak pidana apabila terdapat perbuatan melawan hukum, kesalahan, serta kerugian yang ditimbulkan. Meskipun *Artificial Intelligence* berperan dalam proses terjadinya kejahatan, teknologi tersebut pada hakikatnya hanya merupakan alat yang digunakan oleh manusia. Oleh karena itu, ketentuan mengenai kejahatan siber tetap dapat diterapkan berdasarkan pengaturan yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE.

Selanjutnya, model pertanggungjawaban hukum terhadap penggunaan *Artificial Intelligence* sebagai sarana kejahatan tetap berfokus pada manusia sebagai subjek hukum. Dengan demikian, pihak yang merancang, mengoperasikan, maupun memanfaatkan teknologi *Artificial Intelligence* untuk melakukan kejahatan dapat dimintai pertanggungjawaban pidana sesuai dengan perannya masing-masing. Pertanggungjawaban tersebut dapat berupa pertanggungjawaban individu, pertanggungjawaban bersama apabila melibatkan beberapa pihak, maupun

[9] Yosua Hia. "*Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)*". Jurnal SELISIK. Vol. 10, No. 1, Juni 2024, hlm. 158

pertanggungjawaban korporasi apabila kejahatan tersebut dilakukan dalam lingkup badan usaha**.**

DAFTAR PUSTAKA

Agus Raharjo. 2017. "Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime di Indonesia." *Jurnal Dinamika Hukum*, Vol. 17 No. 2.

Barda Nawawi Arief. 2016. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Raja Grafindo Persada.

Danrivanto Budhijanto. 2019. "Tantangan Penegakan Hukum terhadap Kejahatan Siber di Era Digital." *Jurnal Hukum IUS QUIA IUSTUM*, Vol. 26 No. 4.

Eka Nanda Ravizki dan Lintang Yudhantaka. 2022. "Artificial Intelligence sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia." *Notaire: Journal of Notarial Law*, Vol. 5 No. 3.

Hia, Yosua. 2024. "Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan

Klaus Schwab. 2017. *The Fourth Industrial Revolution*. Geneva: World Economic Forum.

Maskun. 2013. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana Prenada Media Group.

Rizky Dwi Setiawan dan Budi Santoso. 2021. "Penegakan Hukum terhadap Kejahatan Siber dalam Perspektif Hukum Pidana Indonesia." *Jurnal Hukum IUS QUIA IUSTUM*, Vol. 28 No. 2.

Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)". Jurnal SELISIK.

Sinta Dewi Rosadi. 2018. "Implikasi Perkembangan Teknologi Informasi terhadap Hukum dan Penegakan Hukum di Indonesia." *Jurnal Hukum & Pembangunan*, Vol. 48 No. 3.

Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law)*. Yogyakarta: Aswaja Pressindo.