JURNAL MEDIA AKADEMIK (JMA)
Vol.4, No.2 Februari 2026
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

PERAN DAN TANTANGAN KECERDASAN BUATAN DALAM PENGIMPLEMENTASIANNYA PADA *CYBER LAW*

Oleh:

I Kadek Dwi Meret Adyaksa Putra

Universitas Pendidikan Ganesha
Alamat: Jl. Udayana No.11, Banjar Tegal, Singaraja, Kabupaten Buleleng, Bali (81116).
Korespondensi Penulis: dwi.meret@student.undiksha.ac.id.

Abstract. *Artificial Intelligence (AI) has emerged as a fundamental element in the transformation of modern cybersecurity systems, driven by its extraordinary capability to detect and prevent various digital threats effectively and in real-time. Amidst the escalation of increasingly complex cyberattacks, the implementation of AI provides a strategic solution through defense automation and the analysis of anomalous patterns that are difficult to reach by conventional systems. On the other hand, the utilization of this autonomous technology also presents a series of significant legal challenges that necessitate specific regulation within the Cyber Law framework. The primary issues arising include concerns over individual data privacy, legal uncertainty in establishing liability for systemic failures, and the potential misuse of AI technology by malicious actors to create more destructive attacks, such as deepfakes and generative malware. This research aims to identify the strategic role of AI in strengthening cybersecurity, evaluate the legal challenges faced within the current legal order, and formulate adaptive policy recommendations. By employing a qualitative-descriptive approach involving literature studies and thematic analysis, this research concludes that existing regulations often lag behind the pace of technological innovation, resulting in a regulatory gap. Therefore, the strengthening of a more responsive regulatory framework, international harmonization of rules, and cross-sectoral cooperation between the government and industry are essential to support the ethical and secure implementation of AI under Cyber Law. Through these enhancements, it is expected that an equilibrium can be achieved*

Received January 19, 2026; Revised January 29, 2026; February 26, 2026
*Corresponding author: *dwi.meret@student.undiksha.ac.id*

between fostering technological innovation and protecting the fundamental rights of society in the digital sphere.

Keywords: *Artificial Intelligence, Cyber Law, Cybersecurity, Data Privacy, Regulation.*

Abstrak. Kecerdasan Buatan atau *Artificial Intelligence* (AI) saat ini telah menjadi elemen fundamental dalam transformasi sistem keamanan siber modern karena kemampuannya yang luar biasa dalam mendeteksi dan mencegah berbagai ancaman digital secara efektif dan *real-time*. Di tengah eskalasi serangan siber yang semakin kompleks, penggunaan AI memberikan solusi melalui otomasi pertahanan dan analisis pola anomali yang sulit dijangkau oleh sistem konvensional. Namun, di sisi lain, pemanfaatan teknologi otonom ini juga menghadirkan serangkaian tantangan hukum yang signifikan dan memerlukan pengaturan khusus melalui instrumen *Cyber Law*. Permasalahan utama yang muncul mencakup kekhawatiran terhadap privasi data individu, ketidakpastian dalam penetapan tanggung jawab hukum (*legal liability*) saat terjadi kesalahan sistem, hingga potensi penyalahgunaan teknologi AI oleh aktor jahat untuk menciptakan serangan yang lebih destruktif seperti deepfake dan malware generatif. Penelitian ini bertujuan untuk mengidentifikasi peran strategis AI dalam memperkuat keamanan siber, mengevaluasi tantangan hukum yang dihadapi dalam tatanan hukum saat ini, serta merumuskan rekomendasi kebijakan yang adaptif. Dengan menggunakan pendekatan kualitatif-deskriptif yang melibatkan studi literatur dan analisis tematik, penelitian ini menyimpulkan bahwa regulasi yang ada saat ini masih sering kali tertinggal dibandingkan dengan laju inovasi teknologi atau mengalami regulatory gap. Oleh karena itu, penguatan kerangka regulasi yang lebih responsif, harmonisasi aturan di tingkat global, serta kerja sama lintas sektor antara pemerintah dan industri sangat diperlukan untuk mendukung implementasi AI yang beretika dan aman dalam kerangka *Cyber Law*. Melalui penguatan ini, diharapkan tercipta keseimbangan antara dorongan inovasi teknologi dengan perlindungan hak-hak fundamental masyarakat di ruang digital.

Kata Kunci: *Artificial Intelligence*, *Cyber Law*, Keamanan Siber, Privasi Data, Regulasi.

LATAR BELAKANG

Dalam era transformasi digital yang berkembang pesat dewasa ini, lanskap teknologi global telah mengalami pergeseran paradigma yang fundamental. Keamanan

siber telah menjadi salah satu isu krusial yang memengaruhi berbagai aspek kehidupan, mulai dari sektor pemerintahan, ekonomi, hingga privasi individu. Berpindahnya aktivitas manusia ke ruang siber membawa konsekuensi logis berupa peningkatan volume, variasi, dan kompleksitas ancaman digital.[1] Perkembangan teknologi Kecerdasan Buatan (*Artificial Intelligence* atau AI) telah menghadirkan potensi luar biasa untuk mendukung sistem keamanan siber dalam menghadapi ancaman yang semakin terstruktur dan persisten.[2] Dengan kemampuan analitik tingkat tinggi, AI mampu memproses dan menganalisis data dalam jumlah besar secara *real-time*, mendeteksi pola-pola anomali yang tidak kasat mata, serta merespons insiden secara otomatis. AI kini menjadi alat yang esensial dalam melindungi infrastruktur digital dari serangan yang beragam seperti *malware*, *ransomware*, hingga serangan *Distributed Denial of Service* (DDoS) yang kerap melumpuhkan layanan esensial.

Namun, di balik kemampuannya yang revolusioner, integrasi AI dalam sistem keamanan siber juga membawa tantangan besar, baik dari segi teknis maupun hukum. Salah satu tantangan utama yang kerap menjadi perdebatan akademis dan praktis adalah bagaimana *Cyber Law* dapat mengatur penggunaan teknologi otonom ini tanpa menghambat laju inovasi.[3] Di satu sisi, algoritma AI khususnya *Machine Learning* dan *Deep Learning* membutuhkan asupan data dalam jumlah besar untuk terus melakukan iterasi dan meningkatkan akurasi serta efektivitasnya. Tetapi di sisi lain, hal ini menimbulkan kekhawatiran serius tentang pelanggaran privasi dan perlindungan data individu. Selain itu, tidak adanya regulasi hukum yang komprehensif terkait tanggung jawab hukum (*legal liability*) dalam penggunaan AI sering kali menimbulkan ketidakpastian. Ketidakpastian ini memuncak terutama dalam kasus kesalahan sistem yang bersifat otonom atau penyalahgunaan teknologi oleh aktor jahat. Ironisnya, penggunaan AI juga membuka peluang baru bagi pelaku kejahatan siber untuk menciptakan serangan yang lebih canggih, adaptif, dan sulit dideteksi oleh sistem keamanan tradisional. Sebagai contoh, teknologi deepfake saat ini dapat digunakan untuk

---

[1] Siregar, A., & Sitompul, H. (2018). *Keamanan siber: Tantangan dan solusi di era digital*. Jakarta: RajaGrafindo Persada.

[2] Budiarto, R. (2019). Keamanan siber di era kecerdasan buatan. *Jurnal Hukum Teknologi*, 8(1), hlm. 45-59

[3] Hidayati, I., & Nurhasanah, S. (2021). *Cyber Law* dan tantangan hukum di era digital: Perspektif hukum Indonesia. *Jurnal Hukum dan Pembangunan*, 32(4), hlm. 123-139.

memalsukan identitas secara meyakinkan demi rekayasa sosial (*social engineering*), sedangkan AI generatif dapat membantu peretas menghasilkan malware yang lebih kompleks dan persisten.[4]

Dalam konteks dinamika inilah, instrumen hukum perlu berkembang dengan cepat untuk mengantisipasi potensi dampak negatif teknologi tersebut (Yuliana & Rahmawati, 2020:36).[5] *Cyber Law*, sebagai kerangka hukum yang mengatur segala bentuk aktivitas di dunia digital, memiliki peran yang sangat strategis dalam menciptakan keseimbangan (*equilibrium*) antara mendorong inovasi teknologi dan melindungi hak-hak fundamental masyarakat. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi secara komprehensif bagaimana AI berperan dalam meningkatkan sistem keamanan siber, membedah tantangan hukum yang muncul, dan merumuskan upaya integrasi AI yang beretika dalam kerangka *Cyber Law*.

KAJIAN TEORITIS

Cyber Law dipahami sebagai hukum yang berkaitan dengan pemanfaatan teknologi informasi, komunikasi, dan media elektronik secara global. Ruang lingkup hukum ini sangat luas, mencakup aspek yurisdiksi, hak kekayaan intelektual, privasi, hingga tindak pidana siber (*Cyber Crime*). Teori perlindungan hukum menjadi landasan utama dalam kajian ini untuk melihat bagaimana institusi negara hadir untuk menjamin keamanan warga negaranya di ruang digital yang nirbatas (*borderless*). Secara spesifik, pemanfaatan AI dalam keamanan siber didasarkan pada teori otomasi sistem pertahanan. Dalam teori ini, AI dipandang bukan sekadar alat pembantu mekanis (mechanical tool), melainkan sebagai subjek teknologi otonom yang mampu mengambil keputusan secara mandiri (*autonomous decision-making*). Hal ini menciptakan diskursus baru dalam ilmu hukum mengenai sejauh mana entitas non-manusia dapat dilibatkan dalam proses penegakan keamanan siber.

Kajian ini juga mengacu pada beberapa penelitian terdahulu yang relevan. Implementasi AI pada sistem keamanan mampu memberikan efisiensi waktu deteksi yang

[4] Sari, R. K., & Nugroho, A. S. (2023). Tantangan regulasi *Cyber Law* terhadap ancaman deepfake dan AI generatif. *Jurnal Keamanan Nasional*, hlm. 12-29

[5] Yuliana, D., & Rahmawati, S. (2020). Kecerdasan buatan dan dampaknya terhadap hukum siber: Analisis dan perspektif Indonesia. *Jurnal Ilmu Hukum*, hlm. 34-48

signifikan dibandingkan metode manual yang sering kali terlambat merespons intrusi.[6] Namun, dari perspektif hukum perkembangan teknologi yang begitu cepat sering kali meninggalkan celah hukum (*legal gap*), di mana regulasi yang ada umumnya bersifat reaktif dan tidak mampu mengakomodasi teknologi baru secara efektif dan komprehensif. Landasan teori ini memperkuat urgensi dilakukannya analisis mendalam terhadap kesesuaian antara inovasi teknologi AI dan instrumen perlindungan hak-hak masyarakat melalui regulasi yang bersifat adaptif.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif untuk mengeksplorasi dan membedah peran AI dalam sistem keamanan siber, serta tantangan hukum yang terkait dengan implementasinya dalam kerangka *Cyber Law*. Pendekatan ini dipilih secara sengaja karena fokus utama penelitian terletak pada analisis mendalam terhadap fenomena, makna, dan dinamika yang kompleks antara kemajuan teknologi, kekosongan hukum, dan kebutuhan akan keamanan digital.

Data yang digunakan dalam penelitian ini terdiri atas dua jenis utama, yakni data primer dan sekunder. Data primer diperoleh melalui proses wawancara mendalam (*in-depth interview*) dengan sejumlah informan kunci yang merepresentasikan tiga pilar utama: pakar keamanan siber independen, pengembang teknologi AI dari sektor swasta, dan pembuat kebijakan di bidang regulasi digital. Sementara itu, data sekunder dikumpulkan secara ekstensif melalui metode studi literatur. Kajian literatur ini melibatkan telaah kritis terhadap jurnal akademik bereputasi, buku referensi, laporan penelitian lembaga keamanan siber, serta analisis terhadap dokumen hukum, baik instrumen hukum nasional maupun internasional.

Teknik pengumpulan data berfokus pada studi pustaka untuk membangun dan memahami konsep teoretis yang kokoh, dipadukan dengan wawancara mendalam untuk mendapatkan wawasan dan perspektif praktis di lapangan (Yuliana & Rahmawati, 2020:38) . Seluruh data verbal dan tekstual kemudian dianalisis secara tematik. Proses analisis ini bertujuan untuk mengidentifikasi pola-pola utama mengenai peran AI, pemetaan tantangan regulasi yang berulang, dan penyusunan rekomendasi kebijakan yang

[6] Astuti, W. P., & Pratama, M. A. (2020). Penerapan kecerdasan buatan dalam sistem keamanan siber. *Jurnal Teknologi Informasi dan Komunikasi*, hlm. 85-100.

implementatif. Untuk memastikan keabsahan dan keandalan penelitian, validitas data dijaga dengan teknik triangulasi sumber, yakni dengan menguji silang informasi yang diperoleh dari wawancara, regulasi, dan literatur akademik demi memastikan konsistensi temuan.

HASIL DAN PEMBAHASAN

Dinamika Peran Kecerdasan Buatan dalam Transformasi Keamanan Siber

Implementasi Kecerdasan Buatan dalam ekosistem keamanan siber telah mengubah fundamental cara organisasi melindungi aset digital mereka. Berbeda dengan sistem keamanan konvensional yang bekerja berdasarkan aturan statis atau tanda tangan ancaman yang sudah diketahui sebelumnya, AI memberikan keunggulan pada aspek kecepatan serta volume pemrosesan data. Teknologi *Machine Learning* memungkinkan sistem untuk mempelajari pola perilaku normal dalam sebuah jaringan secara mandiri. Ketika muncul deviasi kecil yang berpotensi menjadi ancaman, sistem dapat melakukan mitigasi secara otomatis dalam hitungan milidetik sebelum kerusakan meluas. Hal ini sangat krusial dalam menghadapi serangan modern seperti *Distributed Denial of Service* (DDoS) atau ransomware yang memiliki kecepatan replikasi sangat tinggi. Keberadaan AI telah menggeser paradigma keamanan dari yang sebelumnya bersifat reaktif menjadi proaktif melalui kemampuan deteksi dini dan respons otomatis yang presisi.

Lebih lanjut, integrasi AI dalam keamanan siber memungkinkan adanya mekanisme Self-Healing Networks atau jaringan yang mampu memulihkan diri sendiri secara mandiri setelah terjadinya serangan. Dalam operasionalnya, AI tidak hanya berfungsi sebagai filter pasif, tetapi juga sebagai instrumen audit berkelanjutan yang mampu memetakan kerentanan sistem sebelum dieksploitasi oleh pihak eksternal. Sebagai contoh, penggunaan algoritma Deep Learning dapat membantu tim keamanan siber dalam mengklasifikasikan jutaan sampel kode berbahaya setiap harinya dengan tingkat akurasi yang jauh melampaui kapasitas kognitif manusia. Efisiensi ini secara langsung mengurangi beban kerja administratif bagi praktisi hukum teknologi dan ahli IT, sehingga fokus pengamanan dapat diarahkan pada mitigasi risiko yang lebih strategis dan bersifat preventif.[7]

[7] Budiarto, R. (2019). Keamanan siber di era kecerdasan buatan. *Jurnal Hukum Teknologi*, hlm. 52

Kesenjangan Regulasi dan Dilema Privasi Data dalam *Cyber Law*

Meskipun potensi teknisnya sangat besar, pemanfaatan AI menghadirkan tantangan hukum yang kompleks di bawah payung *Cyber Law*. Tantangan pertama berkaitan dengan adanya kesenjangan regulasi atau regulatory gap. Mayoritas instrumen hukum saat ini masih berfokus pada bentuk ancaman tradisional dan belum mengakomodasi sifat otonom dari teknologi AI. Di sisi lain, penggunaan AI memicu kekhawatiran serius mengenai privasi data. Algoritma AI membutuhkan asupan data dalam jumlah masif untuk meningkatkan akurasinya, namun hal ini sering kali berbenturan dengan prinsip perlindungan data pribadi. Dalam banyak kasus, pengumpulan data besar-besaran oleh sistem AI dilakukan tanpa mekanisme transparansi yang jelas bagi pemilik data, sehingga menciptakan risiko penyalahgunaan informasi sensitif yang bertentangan dengan semangat hak asasi manusia di ruang digital.

Kekhawatiran mengenai privasi data ini semakin meruncing ketika kita melihat cara kerja AI yang sering kali bersifat *Black Box* atau tidak transparan dalam pengambilan keputusannya. Di Indonesia, Undang-Undang Pelindungan Data Pribadi (UU PDP) menuntut adanya dasar pemrosesan data yang sah dan tujuan yang spesifik, namun AI cenderung mengumpulkan data secara ekstensif untuk proses pembelajaran mesin yang tidak selalu bisa diprediksi hasilnya. Hal ini menimbulkan risiko hukum bagi korporasi yang menggunakan AI keamanan, di mana mereka bisa terjebak dalam pelanggaran prinsip *limitation of purpose* atau pembatasan tujuan penggunaan data. Oleh karena itu, tantangan bagi *Cyber Law* adalah menciptakan mekanisme pengawasan yang memastikan bahwa proses pelatihan AI tetap menghormati hak subjek data tanpa melumpuhkan kecerdasan algoritma itu sendiri.[8]

Kompleksitas Tanggung Jawab Hukum dan Ancaman Siber Berbasis AI

Persoalan tanggung jawab hukum atau *legal liability* menjadi perdebatan krusial dalam pengimplementasian AI pada sistem keamanan siber. Muncul pertanyaan mendasar mengenai siapa yang harus bertanggung jawab ketika sistem AI melakukan kesalahan fatal, seperti gagal mendeteksi serangan nyata atau justru memblokir aktivitas legal yang dianggap sebagai ancaman. Secara hukum, saat ini masih sulit untuk

[8] Pratama, A. B., & Wijaya, K. (2022). Perlindungan data pribadi dalam penggunaan algoritma kecerdasan buatan di Indonesia. *Jurnal Hukum Lex Generalis*, hlm. 342-358.

menetapkan apakah kesalahan tersebut merupakan tanggung jawab pengembang perangkat lunak, penyedia layanan, atau pengguna akhir. Ketidakjelasan subjek hukum ini dapat menciptakan kekosongan pertanggungjawaban yang merugikan masyarakat. Lebih lanjut, risiko penyalahgunaan AI oleh aktor jahat memperkeruh suasana keamanan siber global. Teknologi *deepfake* untuk pemalsuan identitas dan penggunaan AI generatif untuk memproduksi malware yang mampu bermutasi menjadi bukti nyata bahwa AI dapat menjadi senjata yang destruktif jika jatuh ke tangan yang salah.

Dari perspektif doktrin hukum siber, masalah pertanggungjawaban ini bersinggungan dengan konsep Electronic Personhood atau status hukum entitas elektronik. Jika sebuah sistem AI melakukan tindakan yang merugikan pihak ketiga karena adanya bias dalam algoritma, maka pembuktian kesalahan dalam hukum acara menjadi sangat sulit dilakukan. Apakah kegagalan tersebut merupakan kesalahan manusia dalam memberikan data pelatihan yang bias, ataukah murni kegagalan sistemik yang tidak dapat diprediksi sebelumnya (unforeseeable events)? Tanpa adanya yurisprudensi yang jelas, penggunaan AI dalam sektor krusial seperti perbankan atau infrastruktur nasional akan terus dihantui oleh ketidakpastian mengenai siapa yang harus menanggung kerugian finansial maupun pidana yang timbul.[9]

Integrasi Kebijakan dan Harmonisasi Global sebagai Solusi Strategis

Menghadapi tantangan tersebut, diperlukan pembaruan regulasi *Cyber Law* yang dilakukan secara berkala agar tetap relevan dengan dinamika teknologi. Regulasi baru tersebut harus mencakup standar pengelolaan data, kejelasan hierarki tanggung jawab hukum, serta kewajiban transparansi sistem AI. Mengingat ancaman siber tidak mengenal batas negara, kerja sama internasional menjadi kunci utama dalam menciptakan ruang digital yang aman. Harmonisasi regulasi di tingkat global akan memudahkan koordinasi antarnegara dalam memitigasi serangan kolektif serta menegakkan hukum terhadap pelaku kejahatan siber lintas batas. Selain instrumen hukum yang kaku, pengembangan kerangka etika dan audit terhadap algoritma AI sangat penting untuk memastikan bahwa setiap inovasi tetap berorientasi pada nilai kemanusiaan dan transparansi publik.

[9] Ramadhan, F., & Putri, L. S. (2022). Tanggung jawab hukum penyedia layanan kecerdasan buatan dalam kasus kebocoran data siber. *Jurnal Riset Hukum*, hlm. 211-220.

Dalam konteks nasional, Indonesia perlu mempertimbangkan pembentukan badan pengawas khusus yang memiliki otoritas untuk melakukan audit algoritma secara berkala terhadap sistem AI yang memiliki dampak publik luas. Harmonisasi global bukan sekadar impian diplomatik, melainkan kebutuhan mendesak mengingat pelaku kejahatan siber sering kali berpindah-pindah yurisdiksi untuk menghindari jerat hukum. Dengan adanya standar global seperti AI Ethics Guidelines, negara-negara dapat saling berbagi informasi mengenai pola serangan baru yang digerakkan oleh AI secara lebih transparan. Langkah ini harus dibarengi dengan pendekatan Sandboxing atau uji coba regulasi, di mana inovasi teknologi AI diberikan ruang untuk berkembang dalam pengawasan ketat pemerintah sebelum dilepas sepenuhnya ke pasar luas.[10]

Harmonisasi AI dengan Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia

Implementasi AI dalam keamanan siber di Indonesia kini harus berhadapan dengan instrumen hukum terbaru, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Salah satu tantangan hukum yang muncul adalah pemenuhan hak-hak subjek data dalam pemrosesan data otomatis. AI keamanan siber sering kali melakukan profilasi (*profiling*) terhadap perilaku pengguna jaringan untuk mendeteksi ancaman. Namun, UU PDP memberikan hak kepada individu untuk keberatan atas pemrosesan data yang didasarkan pada keputusan otomatis yang menimbulkan akibat hukum. Jika sistem AI secara otomatis memblokir akses seorang karyawan karena dianggap sebagai ancaman keamanan tanpa adanya intervensi manusia, hal ini dapat memicu sengketa kepatuhan terhadap prinsip transparansi dan akuntabilitas yang diatur dalam UU tersebut (Pratama & Wijaya, 2022:355).[11]

Selain itu, prinsip pembatasan penyimpanan data menjadi kendala teknis bagi pengembang AI. Algoritma memerlukan data historis jangka panjang untuk mengenali pola serangan yang berevolusi, sementara hukum menuntut agar data dihapus segera setelah tujuan pemrosesan tercapai. Dalam konteks ini, Cyber Law di Indonesia perlu merumuskan pedoman spesifik mengenai jangka waktu retensi data untuk kepentingan

[10] Yuliana, D., & Rahmawati, S. (2020). Kecerdasan buatan dan dampaknya terhadap hukum siber: Analisis dan perspektif Indonesia. *Jurnal Ilmu Hukum*, hlm. 34-38

[11] Pratama, A. B., & Wijaya, K. (2022). Perlindungan data pribadi dalam penggunaan algoritma kecerdasan buatan di Indonesia. *Jurnal Hukum Lex Generalis*, hlm. 342-358.

keamanan nasional dan pertahanan siber yang menggunakan teknologi cerdas. Tanpa adanya sinkronisasi antara kebutuhan teknis AI dan batasan hukum PDP, organisasi di Indonesia akan berada dalam posisi dilematis antara menjaga keamanan infrastruktur digital atau mematuhi regulasi pelindungan privasi secara kaku.

Audit Algoritma dan Urgensi Transparansi dalam Penegakan Cyber Law

Tantangan lain yang sangat fundamental adalah fenomena black box dalam AI, di mana proses pengambilan keputusan oleh mesin tidak selalu dapat dijelaskan secara logika hukum manusia. Dalam penegakan hukum siber, transparansi atau explainability adalah syarat mutlak agar sebuah tindakan dapat dipertanggungjawabkan secara hukum. Jika sebuah serangan siber terjadi karena kegagalan AI, jaksa atau hakim akan kesulitan untuk menentukan letak kesalahan jika algoritma tersebut bersifat tertutup. Oleh karena itu, diperlukan adanya kewajiban bagi pengembang AI keamanan untuk melakukan audit algoritma secara berkala oleh pihak ketiga yang independen. Audit ini bertujuan untuk memastikan bahwa algoritma tidak memiliki bias yang merugikan kelompok tertentu dan tetap beroperasi dalam koridor etika hukum yang ditetapkan (Astuti & Pratama, 2020:94).

Urgensi transparansi ini juga berkaitan dengan hak bela diri bagi pihak yang terdampak oleh keputusan AI. Dalam ekosistem hukum siber yang adil, setiap individu atau entitas yang dirugikan oleh sistem otomatis harus memiliki akses terhadap penjelasan mengenai mengapa sistem tersebut mengambil keputusan tertentu. Implementasi konsep Explainable AI (XAI) menjadi solusi teknologi yang harus didorong oleh regulasi. Dengan XAI, setiap langkah logika yang diambil oleh mesin dalam mendeteksi ancaman dapat diterjemahkan ke dalam bahasa yang dipahami oleh praktisi hukum. Hal ini akan memudahkan proses pembuktian di pengadilan dan memastikan bahwa penggunaan AI dalam keamanan siber tidak mengabaikan prinsip-prinsip keadilan dasar dalam hukum.[12]

Perbandingan Regulasi Global: Pembelajaran dari EU AI Act untuk Indonesia

Sebagai bahan perbandingan internasional, perkembangan regulasi di Uni Eropa melalui European Union AI Act dapat menjadi acuan berharga bagi pengembangan Cyber Law di Indonesia. Uni Eropa mengklasifikasikan penggunaan AI berdasarkan tingkat

[12] Hidayati, I., & Nurhasanah, S. (2021). *Cyber Law* dan tantangan hukum di era digital: Perspektif hukum Indonesia. *Jurnal Hukum dan Pembangunan*, hlm. 123-139.

risiko, di mana sistem keamanan siber yang mengelola infrastruktur kritis dikategorikan sebagai "risiko tinggi". Untuk kategori ini, terdapat standar kepatuhan yang sangat ketat, termasuk keharusan adanya pengawasan manusia (human oversight) dan dokumentasi teknis yang komprehensif. Pendekatan berbasis risiko ini sangat relevan untuk diadopsi di Indonesia agar regulasi tidak bersifat memukul rata semua jenis AI, melainkan fokus pada perlindungan terhadap kepentingan publik yang paling rentan terhadap serangan siber.[13]

Harmonisasi global juga mendesak karena sifat kejahatan siber yang bersifat lintas batas. Ketika AI digunakan untuk melancarkan serangan dari satu yurisdiksi ke yurisdiksi lain, diperlukan perjanjian bantuan hukum timbal balik yang secara spesifik mencakup bukti-bukti berbasis data AI. Indonesia perlu lebih aktif dalam diplomasi siber internasional untuk merumuskan standar bersama mengenai apa yang dianggap sebagai penggunaan AI yang bertanggung jawab dalam pertahanan negara. Tanpa adanya kesepahaman global, penggunaan AI dalam keamanan siber berisiko memicu perlombaan senjata digital yang tidak terkendali, yang pada akhirnya justru akan melemahkan stabilitas keamanan siber global secara keseluruhan.[14]

Rekonstruksi Pasal UU ITE dalam Menghadapi Kejahatan Berbasis AI Generatif

Penggunaan AI generatif untuk menciptakan konten palsu yang menyesatkan atau manipulatif memerlukan tinjauan hukum yang lebih spesifik dalam kerangka Undang-Undang Informasi dan Transaksi Elektronik yang berlaku di Indonesia. Dalam konteks ini, Pasal 27A dan Pasal 28 UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE menjadi sangat relevan. Pasal tersebut mengatur mengenai larangan mendistribusikan informasi elektronik yang menyerang kehormatan orang lain atau menyebarkan berita bohong yang menyesatkan. Namun, tantangan pembuktian muncul ketika konten tersebut diproduksi secara otomatis oleh AI. Jaksa penuntut umum harus mampu membuktikan adanya niat jahat (*mens rea*) dari pengguna yang memerintahkan AI tersebut, bukan hanya sekadar melihat hasil keluarannya. Kompleksitas ini menunjukkan bahwa *Cyber Law* di Indonesia perlu mulai mengadopsi standar pembuktian digital yang mampu

[13] Sari, R. K., & Nugroho, A. S. (2023). Tantangan regulasi *Cyber Law* terhadap ancaman deepfake dan AI generatif. *Jurnal Keamanan Nasional*, hlm. 12-29

[14] Siregar, A., & Sitompul, H. (2018). *Keamanan siber: Tantangan dan solusi di era digital*. Jakarta: RajaGrafindo Persada.

menjangkau jejak perintah (*prompting*) yang diberikan manusia kepada mesin (Sari & Nugroho, 2023:28).[15]

Selain masalah konten, AI juga sering digunakan dalam tindak pidana akses ilegal yang diatur dalam Pasal 30 UU ITE. Serangan brute force yang menggunakan AI untuk menebak kata sandi secara cepat memaksa kita untuk mendefinisikan kembali apa yang dimaksud dengan "melampaui atau menjebol sistem pengamanan". Jika penjebolan dilakukan oleh sistem otonom yang bekerja tanpa instruksi langkah demi langkah dari manusia, maka perlu ada ketegasan hukum mengenai atribusi kesalahan. Secara teori hukum, penggunaan AI sebagai alat (*instrumentum*) kejahatan seharusnya memberatkan ancaman pidana bagi pelakunya karena tingkat bahaya dan skalanya yang jauh lebih luas dibandingkan serangan manual. Oleh karena itu, yurisprudensi di masa depan harus mulai mempertimbangkan faktor penggunaan teknologi kecerdasan buatan sebagai keadaan yang memperberat pidana (*aggravating circumstances*) dalam tindak pidana siber.

Urgensi Etika Profesi dan Standar Operasional Prosedur Penggunaan AI

Di luar aspek pidana, penambahan dimensi etika profesi dalam pembahasan *Cyber Law* menjadi hal yang tidak terelakkan. Para praktisi keamanan siber dan pengembang teknologi memiliki tanggung jawab moral yang besar untuk memastikan bahwa AI yang mereka ciptakan tidak disalahgunakan. Indonesia perlu mendorong adanya kode etik nasional bagi pengembang AI, yang selaras dengan prinsip-prinsip universal seperti keadilan, non-diskriminasi, dan transparansi. Dalam dunia korporasi, hal ini dapat diwujudkan melalui penyusunan Standar Operasional Prosedur (SOP) yang ketat mengenai penggunaan alat keamanan berbasis AI. SOP tersebut harus mencakup batasan akses data, mekanisme intervensi manual oleh manusia (*human-in-the-loop*), serta laporan transparansi rutin mengenai efektivitas algoritma yang digunakan.

Penegakan etika ini tidak hanya berfungsi sebagai pelengkap regulasi hukum, tetapi juga sebagai lapisan pertahanan pertama dalam mencegah kerugian hukum. Jika sebuah perusahaan dapat membuktikan bahwa mereka telah mengikuti standar etika dan prosedur audit yang ketat, hal ini dapat menjadi dasar pembelaan hukum jika terjadi kegagalan sistemik yang tidak terduga. Sebaliknya, pengabaian terhadap standar etika

[15] Sari, R. K., & Nugroho, A. S. (2023). Tantangan regulasi *Cyber Law* terhadap ancaman deepfake dan AI generatif. *Jurnal Keamanan Nasional*, hlm. 16-25

algoritma dapat dianggap sebagai bentuk kelalaian (*negligence*) yang dapat dituntut secara perdata maupun administratif. Dengan mengintegrasikan etika ke dalam kebijakan perusahaan dan regulasi nasional, implementasi AI dalam keamanan siber akan memiliki fondasi yang kuat, sehingga inovasi teknologi tetap berjalan beriringan dengan nilai-nilai kemanusiaan dan kepastian hukum yang adil.[16]

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil analisis yang telah dipaparkan, penelitian ini menyimpulkan bahwa Kecerdasan Buatan memegang peran yang sangat vital dalam memperkuat sistem keamanan siber melalui kemampuan deteksi proaktif dan respons otomatis terhadap ancaman digital yang semakin kompleks. Namun, integrasi teknologi ini dalam kerangka *Cyber Law* masih menghadapi hambatan besar yang bersifat fundamental. Tantangan hukum berupa kesenjangan regulasi yang belum adaptif, tingginya risiko pelanggaran privasi data, serta ketidakpastian dalam penetapan tanggung jawab hukum atas tindakan otonom AI menjadi isu utama yang memerlukan penyelesaian segera. Oleh karena itu, sangat krusial bagi pemerintah dan pembuat kebijakan untuk merumuskan regulasi yang komprehensif agar inovasi AI dapat berjalan selaras dengan perlindungan hak-hak masyarakat dan keamanan nasional.

Saran

Pemerintah perlu memperkuat kerja sama lintas sektor yang melibatkan akademisi, praktis teknologi, dan lembaga penegak hukum untuk membangun kerangka regulasi AI yang responsif terhadap perubahan zaman. Selain itu, kerja sama internasional harus ditingkatkan untuk mengharmonisasi standar keamanan siber global guna menutup celah bagi penyalahgunaan AI oleh aktor kriminal lintas negara. Masyarakat juga perlu diberikan edukasi dan peningkatan literasi digital agar lebih waspada terhadap potensi risiko teknologi baru ini, serta memahami hak-hak mereka atas perlindungan data di era kecerdasan buatan. Terakhir, pengembang teknologi AI diharapkan menerapkan prinsip

[16] Astuti, W. P., & Pratama, M. A. (2020). Penerapan kecerdasan buatan dalam sistem keamanan siber. *Jurnal Teknologi Informasi dan Komunikasi*, hlm. 85-98.

transparansi dan etika sejak tahap desain untuk meminimalisir kesalahan sistem yang dapat berdampak hukum di masa depan.

DAFTAR REFERENSI

Astuti, W. P., & Pratama, M. A. (2020). Penerapan kecerdasan buatan dalam sistem keamanan siber. *Jurnal Teknologi Informasi dan Komunikasi*, 12(2), 85-100.

Budiarto, R. (2019). Keamanan siber di era kecerdasan buatan. *Jurnal Hukum Teknologi*, 8(1), 45-59

Hidayati, I., & Nurhasanah, S. (2021). *Cyber Law* dan tantangan hukum di era digital: Perspektif hukum Indonesia. *Jurnal Hukum dan Pembangunan*, 32(4), 123-139.

Pratama, A. B., & Wijaya, K. (2022). Perlindungan data pribadi dalam penggunaan algoritma kecerdasan buatan di Indonesia. *Jurnal Hukum Lex Generalis*, 3(5), 342-358.

Ramadhan, F., & Putri, L. S. (2022). Tanggung jawab hukum penyedia layanan kecerdasan buatan dalam kasus kebocoran data siber. *Jurnal Riset Hukum*, 2(3), 211-225.

Sari, R. K., & Nugroho, A. S. (2023). Tantangan regulasi *Cyber Law* terhadap ancaman deepfake dan AI generatif. *Jurnal Keamanan Nasional*, 9(1), 12-29

Siregar, A., & Sitompul, H. (2018). *Keamanan siber: Tantangan dan solusi di era digital*. Jakarta: RajaGrafindo Persada.

Yuliana, D., & Rahmawati, S. (2020). Kecerdasan buatan dan dampaknya terhadap hukum siber: Analisis dan perspektif Indonesia. *Jurnal Ilmu Hukum*, 16(1), 34-48