JURNAL MEDIA AKADEMIK (JMA)
Vol.4, No.1 Januari 2026
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

DINAMIKA KEBIJAKAN PENEGAKAN HUKUM TERHADAP PEMANFAATAN KECERDASAN BUATAN DALAM KEJAHATAN SIBER DI INDONESIA

Oleh:

Gracia Rumondang Angelica Sihombing[1]
Bagus Hermanto[2]

Universitas Udayana
Alamat: JL. Raya Kampus Unud, Jimbaran, Kec. Kuta Sel., Kabupaten Badung, Bali (80361).
Korespondensi Penulis: graciaangelica716@gmail.com, bagus.hermanto@unud.ac.id

Abstract. *The development of artificial intelligence technology has significantly increased the complexity of cybercrime in Indonesia. This technology is not only utilized for positive purposes but also serves as a means to commit various forms of cybercrime with increasingly sophisticated patterns and modus operandi. This study aims to analyze the forms and patterns of artificial intelligence utilization in cybercrime, examine the obstacles faced by law enforcement officers, and assess the adequacy of existing legislation as a basis for law enforcement. The results indicate that the use of artificial intelligence in cybercrime creates difficulties in evidence collection and tracking perpetrators, while existing regulations do not specifically address the use of artificial intelligence as a tool for crime. Therefore, strengthening the regulatory framework and enhancing the capacity of law enforcement officers are necessary to ensure effective enforcement against artificial intelligence-based cybercrime in Indonesia.*
Keywords: *Artificial Intelligence, Cybercrime; Law Enforcement*

Abstrak. Perkembangan teknologi kecerdasan buatan telah membawa dampak signifikan terhadap meningkatnya kompleksitas kejahatan siber di Indonesia. Teknologi ini tidak hanya dimanfaatkan untuk kepentingan positif, tetapi juga digunakan sebagai sarana

Received December 08, 2025; Revised December 24, 2025; January 10, 2026
*Corresponding author: *graciaangelica716@gmail.com*

untuk melakukan berbagai bentuk kejahatan siber dengan pola dan modus operandi yang semakin canggih. Penelitian ini bertujuan untuk menganalisis bentuk dan pola pemanfaatan kecerdasan buatan dalam kejahatan siber, mengkaji hambatan yang dihadapi aparat penegak hukum, serta menilai kecukupan peraturan perundang-undangan yang berlaku sebagai dasar penegakan hukum. Hasil penelitian menunjukkan bahwa pemanfaatan kecerdasan buatan dalam kejahatan siber menimbulkan kesulitan dalam proses pembuktian dan penelusuran pelaku, sementara regulasi yang ada belum secara spesifik mengatur penggunaan kecerdasan buatan sebagai sarana kejahatan. Oleh karena itu, diperlukan penguatan kerangka regulasi dan peningkatan kapasitas aparat penegak hukum guna menjamin efektivitas penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan di Indonesia.

Kata Kunci: Kecerdasan Buatan, Kejahatan Siber, Penegakan Hukum

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang berlangsung sangat pesat, khususnya dalam bidang kecerdasan buatan (*artificial intelligence*), telah membawa dampak signifikan terhadap berbagai sektor kehidupan masyarakat. Seiring dengan proses globalisasi, kemajuan teknologi mempercepat pertukaran informasi antar negara dan tidak membatasi wilayah geografis sehingga mendorong keterhubungan sistem ekonomi, sosial, dan hukum dalam skala global. Pemanfaatan kecerdasan buatan tidak terbatas pada ruang lingkup nasional, melainkan berlangsung dalam lingkungan digital lintas yurisdiksi yang melibatkan berbagai pihak. Keadaan ini menimbulkan tantangan bagi negara, khususnya dalam hal pengawasan, pengendalian serta pelaksanaan penegakan hukum. Teknologi kecerdasan buatan dimanfaatkan secara luas untuk mendukung efektivitas dan efisiensi dalam pengolahan data, analisis informasi, serta pengambilan keputusan. Namun demikian, kemajuan tersebut juga menjadi tantangan berupa munculnya berbagai bentuk kejahatan siber yang memanfaatkan kecerdasan buatan sebagai sarana utama. Pemanfaatan teknologi ini dalam kejahatan siber, seperti pembuatan *deepfake*, kloning suara, pemalsuan identitas digital, hingga otomatisasi

serangan terhadap sistem elektronik, menunjukkan bahwa karakter kejahatan siber semakin berkembang dan menuntut pendekatan penegakan hukum yang lebih adaptif.[1]

Di Indonesia, perkembangan kejahatan siber berbasis kecerdasan buatan semakin mengemuka seiring dengan kebergantungan teknologi digital dalam aktivitas sehari-hari. Modus operandi kejahatan siber tidak lagi dilakukan secara sederhana, melainkan menggunakan algoritma cerdas yang mampu meniru perilaku manusia, memanipulasi informasi secara meyakinkan, serta melintasi batas-batas yurisdiksi negara.[2] Kondisi tersebut berpotensi menimbulkan dampak serius terhadap keamanan data pribadi, keandalan sistem elektronik, serta perlindungan hak asasi manusia. Oleh karena itu, kerangka kebijakan penegakan hukum siber yang melibatkan pemanfaatan kecerdasan buatan menjadi isu strategis yang memerlukan perhatian khusus, baik dari aspek pengaturan hukum, kapasitas aparatur penegak hukum, maupun kesadaran hukum masyarakat.[3]

Indonesia telah merumuskan kebijakan hukum terhadap pengaturan bidang siber, antara lain melalui UU ITE beserta perubahannya, yang mengatur larangan dan sanksi terhadap berbagai perbuatan melawan hukum di bidang teknologi informasi, seperti akses tanpa hak, manipulasi informasi elektronik, dan penipuan berbasis sistem elektronik.[4] Selain itu, UU PDP menjadi pijakan yuridis perlindungan data pribadi dari penyalahgunaan, yang kerap menjadi objek dalam kejahatan siber berbasis kecerdasan buatan.[5] Meskipun demikian, dilihat dari sudut pandang kebijakan publik, masih terlihat adanya perbedaan antara ketentuan hukum yang tertuang dalam peraturan perundang-undangan dan penerapannya, terutama dalam penanganan kejahatan siber yang melibatkan pemanfaatan kecerdasan buatan. Permasalahan yang muncul antara lain berkaitan dengan keterbatasan kemampuan aparat penegak hukum dalam memahami perkembangan teknologi, kurang optimalnya kerja sama antarinstansi terkait, serta belum

---

[1]Barda Nawawi Arief, *Tindak Pidana Mayantara (Cyber Crime)* (Jakarta: RajaGrafindo Persada, 2020), 42–45.
[2]Sigid Suseno, "Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *Jurnal Ilmu Hukum* 8, no. 1 (2021): 60–62.
[3]Agus Rahardjo, "Penegakan Hukum di Era Digital," *Jurnal Hukum Ius Quia Iustum* 27, no. 2 (2020): 205–208.
[4]Al Fatih, Sholahuddin, et.al. "Understanding Regulations Of Online Gambling In Indonesia: Is It Forbidden?." *Jurisdictie: Jurnal Hukum dan Syariah* 16, no. 1 (2025): 55-76.
[5]Hermanto, Bagus, I. Gede Yusa, and Ni Ketut Ardani. "Problems and Reform of Indonesia's Cyber Law: A Comparative Study with Other Countries." *Literasi Hukum* 9, no. 1 (2025): 45-58.

memadainya fasilitas dan infrastruktur yang mendukung penegakan hukum di bidang siber. Kebijakan hukum yang berlaku masih cenderung bersifat responsif terhadap kasus yang terjadi belum sepenuhnya mengantisipasi perkembangan penggunaan kecerdasan buatan dalam kejahatan siber. Kondisi tersebut menunjukkan pentingnya dilakukan evaluasi kebijakan secara berkesinambungan agar regulasi yang ada tidak hanya memberikan kepastian hukum, tetapi juga melindungi kepentingan masyarakat secara nyata. Dalam praktik penegakan hukum, aparat penegak hukum juga dihadapkan pada berbagai kendala dalam menangani kejahatan siber berbasis kecerdasan buatan. Kendala tersebut antara lain terbatasnya orang yang berkeahlian dalam bidang kecerdasan buatan dan forensik digital, keterbatasan sarana dan prasarana pendukung, serta sifat kejahatan siber yang bersifat lintas negara.[6] Di samping itu, dinamika teknologi kecerdasan buatan yang sangat cepat sering kali tidak sejalan dengan proses pembentukan dan pembaruan hukum, sehingga berpotensi menimbulkan kekosongan hukum (*rechtsvacuum*) dalam penanganan kejahatan siber berbasis teknologi mutakhir.

Beberapa penelitian terdahulu telah membahas penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan di Indonesia, meskipun kajiannya masih cenderung normatif dan terbatas pada isu tertentu. Wahyudi (2025) menyoroti kelemahan pengaturan dalam UU ITE yang belum mampu mengantisipasi perkembangan kejahatan siber berbasis AI, seperti *deepfake*, serta menekankan perlunya pembaruan regulasi, peningkatan kapasitas aparat penegak hukum, dan kerja sama lintas negara.[7] Selanjutnya, Prayoga dan Tuasikal (2025) memfokuskan kajian pada *deepfake* sebagai tindak pidana pencemaran nama baik, dengan temuan utama berupa lemahnya pembuktian forensik digital dan perlunya regulasi khusus serta peningkatan literasi digital masyarakat.[8] Sementara itu, Anggraeny (2025) mengkaji keterbatasan pengaturan pertanggungjawaban pidana dalam kejahatan siber berbasis AI, khususnya terkait perlindungan data pribadi dan data sintetis.[9]

---

[6]Widodo, "Tantangan Penegakan Hukum Kejahatan Siber," *Jurnal Legislasi Indonesia* 18, no. 3 (2021): 315.

[7] Wahyudi, *Penegakan Hukum terhadap Kejahatan Siber Berbasis Kecerdasan Buatan di Indonesia*, Jurnal Hukum dan Teknologi Informasi, Vol. 7 No. 2, 2025, hlm. 145–147.

[8] Dimas Prayoga dan Muhammad Tuasikal, *Deepfake sebagai Tindak Pidana Pencemaran Nama Baik dalam Perspektif Hukum Pidana Indonesia*, Jurnal Ilmu Hukum, Vol. 9 No. 1, 2025, hlm. 88–90.

[9] Anggraeny, *Pertanggungjawaban Pidana dalam Kejahatan Siber Berbasis Artificial Intelligence: Tantangan Perlindungan Data Pribadi dan Data Sintetis*, Jurnal Hukum Siber, Vol. 5 No. 3, 2025, hlm. 201–203.

Berbeda dengan penelitian-penelitian tersebut, kajian ini menganalisis pemanfaatan kecerdasan buatan dalam kejahatan siber secara lebih komprehensif, tidak hanya terbatas pada *deepfake*, tetapi juga mencakup bentuk lain seperti kloning suara dan serangan siber otomatis. Selain menelaah aspek hukum siber, penelitian ini juga mengintegrasikan perspektif kebijakan hukum publik untuk mengevaluasi implementasi regulasi dan merumuskan kebijakan yang lebih adaptif, sehingga diharapkan dapat memberikan gambaran mengenai bentuk dan pola pemanfaatan kecerdasan buatan dalam kejahatan siber, hambatan penegakan hukum, serta aspek kecukupan kebijakan hukum yang berlaku dalam melandasi kebutuhan futuristik akan perkembangan teknologi kecerdasan buatan. Kemudia penulis menemukan 3 rumusan masalah yaitu:

1. Bagaimana bentuk dan pola pemanfaatan kecerdasan buatan sebagai sarana kejahatan siber di Indonesia?
2. Apa saja hambatan yang dihadapi aparat penegak hukum dalam implementasi kebijakan penanganan kejahatan siber yang melibatkan pemanfaatan kecerdasan buatan selama ini?
3. Sejauh mana peraturan perundang-undangan yang berlaku telah memadai dalam konteks implementasi kebijakan Hukum Siber nasional atas penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan di Indonesia?

TUJUAN PENELITIAN

1. Menganalisis bentuk dan pola pemanfaatan kecerdasan buatan sebagai sarana kejahatan siber di Indonesia.
2. Mengidentifikasi hambatan yang dihadapi aparat penegak hukum dalam implementasi kebijakan penanganan kejahatan siber yang melibatkan pemanfaatan kecerdasan buatan.
3. Menilai kecukupan peraturan perundang-undangan yang berlaku dalam konteks implementasi kebijakan hukum siber nasional terhadap penegakan hukum kejahatan siber berbasis kecerdasan buatan di Indonesia.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk menganalisis penegakan hukum terhadap pemanfaatan kecerdasan buatan sebagai sarana

kejahatan siber di Indonesia.[10] Pemilihan metode normatif sejalan dengan pandangan Mathias Siems mengenai kerangka *macro–micro legal research*, di mana penelitian hukum normatif ditempatkan pada tingkat makro yang berfokus pada analisis struktur hukum secara menyeluruh, termasuk pengaturan hukum mengenai kecerdasan buatan dan kejahatan siber.[11] Pendekatan ini memungkinkan peneliti untuk mengidentifikasi adanya kesenjangan sistemik dalam regulasi, berbeda dengan penelitian mikro yang lebih menitikberatkan pada penerapan hukum dalam kasus tertentu. Selain itu, penelitian hukum normatif memiliki peran penting dalam melakukan sintesis hukum untuk memahami struktur dasar hukum melalui penafsiran dan pengembangan teori hukum, sehingga relevan untuk mengkaji kekosongan pengaturan kecerdasan buatan dalam UU ITE maupun UU PDP[12]. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan digunakan untuk menelaah ketentuan hukum yang mengatur kejahatan siber, antara lain UU ITE, UU PDP, serta ketentuan hukum pidana yang berkaitan. Pendekatan konseptual digunakan untuk mengkaji konsep kecerdasan buatan, kejahatan siber, dan penegakan hukum dalam perspektif hukum pidana dan hukum siber. Sementara itu, pendekatan analitis digunakan untuk menilai kecukupan pengaturan hukum yang berlaku serta mengidentifikasi hambatan dalam praktik penegakan hukum. Ketiga pendekatan tersebut selaras dengan pendekatan penelitian hukum, yang meliputi pendekatan perundang-undangan, konseptual, fakta hukum, kasus, dan komparatif, dengan penyesuaian sesuai dengan karakter penelitian hukum normatif, yang mana kesemuanya mengolah analisis bahan hukum dengan fokus perhatian dalam hal menjawab permasalahan penelitian mengenai bentuk dan pola pemanfaatan kecerdasan buatan dalam kejahatan siber, hambatan yang dihadapi aparat penegak hukum, serta tingkat kecukupan peraturan perundang-undangan yang berlaku di Indonesia.

---

[10] Hutchinson, Terry. "The doctrinal method: Incorporating interdisciplinary methods in reforming the law." *Erasmus L. Rev.* 8 (2015): 130.

[11] Siems, Mathias M. "Legal research in search of attention: A quantitative assessment." *King's Law Journal* 27.2 (2016): 170-187.

[12]Hermanto, Bagus, Nur, Asrul Ibrahim & Zulfa, Indana, "Dinamika Pengaturan Hukum Siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam Ius Constituendum", *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 14, no. 2 (2025): 315-335.

HASIL DAN PEMBAHASAN

Bentuk dan pola pemanfaatan kecerdasan buatan sebagai sarana kejahatan siber di Indonesia

Pemanfaatan kecerdasan buatan sebagai sarana kejahatan siber di Indonesia berkembang sejalan dengan pesatnya kebergantungan terhadap teknologi digital dalam kehidupan masyarakat. Kecerdasan buatan yang pada awalnya dirancang untuk mendukung efisiensi di berbagai bidang, seperti ekonomi, pemerintahan, dan komunikasi, kini juga dimanfaatkan pihak-pihak tertentu dalam rangka melakukan tindak pidana di ruang siber. Perkembangan ini menunjukkan adanya pergeseran karakter kejahatan siber, di mana teknologi modern digunakan untuk mempercepat proses kejahatan, memperluas jangkauan korban, serta menyempurnakan berbagai *modus operandi*.[13] Akibatnya, sistem hukum pidana yang selama ini lebih berorientasi pada kejahatan konvensional menghadapi tantangan baru dalam menyesuaikan diri dengan dinamika kejahatan berbasis teknologi.

Tabel 1. Pola Kejahatan Siber Berbasis Kecerdasan Buatan

No	Kejahatan Siber Berbasis AI	Deskripsi Pola Pemanfaatan
1.	Penipuan Digital	AI digunakan untuk menganalisis pola komunikasi, bahasa dan kebiasaan korban guna menyusun pesan penipuan yang personal dan meyakinkan.
2.	*Phising* dan *Social Engineering* Otomatisasi	Pemrosesan bahasa alami menghasilkan pesan palsu yang meniru lembaga resmi.
3.	Pemalsuan Identitas Digital (*Deepfake*)	Manipulasi audio dan video untuk meniru suara atau wajah individu.
4.	Disinformasi Berbasis AI	Produksi dan distribusi konten palsu secara otomatis dan terarah.
5.	Serangan Siber Otomatis (AI-*driven Cyber Attack*)	AI mengidentifikasi celah sistem dan menyesuaikan metode serangan.

[13]Ponkin, Igor V., and Alena I. Redkina. "Artificial intelligence from the point of view of law." *RUDN Journal of Law* 22.1 (2018): 91-109.

6.	Peretasan Sistem Elektronik Adaptif	*Machine learning* mempelajari pertahanan digital untuk meningkatkan efektivitas serangan.
7.	Penyebaran *Malware* Berbasis AI	Perangkat lunak berbahaya dikembangkan agar dapat menyesuaikan diri dengan lingkungan sistem.
8.	Otomatisasi Kejahatan Siber	Satu sistem AI menjalankan banyak tindakan kejahatan secara simultan.
9.	Anonimitas Digital Pelaku	AI digunakan untuk menyamarkan jejak dan identitas elektronik.
10.	Kejahatan Siber Lintas Negara	Operasi kejahatan dilakukan dari luar Indonesia.

Sumber: Diolah dari penulis. 2025

Salah satu bentuk pemanfaatan kecerdasan buatan dalam kejahatan siber di Indonesia dapat ditemukan dalam tindak pidana penipuan digital. Melalui penggunaan algoritma kecerdasan buatan, pelaku kejahatan mampu menganalisis pola komunikasi korban, gaya bahasa, serta kebiasaan interaksi di ruang digital. Hal tersebut memungkinkan pelaku menyusun pesan penipuan yang bersifat lebih personal dan meyakinkan.[14] Teknologi pemrosesan bahasa alami juga memungkinkan pembuatan pesan otomatis yang menyerupai komunikasi resmi dari lembaga perbankan, perusahaan jasa keuangan, maupun instansi pemerintah. Kondisi ini menyebabkan korban sering kali tidak menyadari bahwa komunikasi yang diterima merupakan bagian dari kejahatan, sehingga tingkat keberhasilan penipuan menjadi lebih tinggi dibandingkan dengan metode penipuan konvensional.[15]

Selain penipuan digital, kecerdasan buatan juga dimanfaatkan dalam kejahatan pemalsuan identitas melalui manipulasi konten audio dan visual. Teknologi *deepfake* memungkinkan pelaku untuk merekayasa suara atau video seseorang sehingga tampak seolah-olah individu tersebut benar-benar melakukan atau menyampaikan suatu

[14]Widodo Tresno Novianto, "Kejahatan Siber dalam Perspektif Hukum Pidana," *Jurnal Hukum Ius Quia Iustum* 23, no. 1 (2016).
[15]Alarie, Benjamin, Anthony Niblett, and Albert H. Yoon. "How artificial intelligence will affect the practice of law." *University of Toronto Law Journal* 68.supplement 1 (2018): 106-124.

pernyataan tertentu.[16] Dalam konteks Indonesia, praktik ini berpotensi digunakan untuk melakukan pemerasan, pencemaran nama baik, maupun membentuk opini publik yang menyesatkan. Dampak yang ditimbulkan tidak hanya merugikan individu yang menjadi korban, tetapi juga berpotensi menurunkan kepercayaan masyarakat terhadap keaslian informasi digital secara umum.

Pemanfaatan kecerdasan buatan juga terlihat dalam serangan siber yang bersifat teknis, seperti peretasan sistem elektronik dan penyebaran perangkat lunak berbahaya. Dengan dukungan teknologi pembelajaran mesin, serangan siber dapat dilakukan secara otomatis dan berulang tanpa keterlibatan manusia secara langsung. Sistem kecerdasan buatan mampu mengidentifikasi celah keamanan, mempelajari pola pertahanan digital suatu sistem, serta menyesuaikan metode serangan agar tetap efektif. Pola kejahatan seperti ini menyebabkan upaya pencegahan dan pendeteksian menjadi semakin sulit, sekaligus meningkatkan potensi kerugian yang dialami oleh korban, baik perorangan maupun institusi.

Di samping itu, kecerdasan buatan dimanfaatkan dalam penyebaran informasi palsu dan disinformasi di ruang digital. Dengan sistem otomatis, pelaku kejahatan dapat memproduksi dan menyebarkan konten palsu dalam jumlah besar dan waktu yang relatif singkat melalui berbagai platform digital. Algoritma kecerdasan buatan juga memungkinkan pelaku untuk menargetkan kelompok masyarakat tertentu berdasarkan preferensi atau pandangan yang dimiliki, sehingga dampak disinformasi menjadi lebih efektif. Dalam konteks sosial dan politik di Indonesia, praktik ini berpotensi memicu konflik sosial, menurunkan taraf *public trust*, bahkan resistensi terhadap kestabilan negara.

Berbagai bentuk pemanfaatan kecerdasan buatan tersebut menunjukkan bahwa kejahatan siber semakin terorganisasi dan sistematis. Pelaku kejahatan tidak lagi bertindak secara individual, melainkan memanfaatkan sistem dan jaringan digital yang kompleks. Kecerdasan buatan memungkinkan terjadinya otomatisasi kejahatan, di mana satu sistem dapat menjalankan berbagai tindakan kriminal secara bersamaan.[17] Pola ini menyebabkan skala kejahatan semakin luas dan jumlah korban meningkat, sementara

---

[16]Wahyudi Djafar, “Tantangan Regulasi Deepfake dalam Hukum Indonesia,” *Jurnal RechtsVinding* 9, no. 2 (2020).

[17]Hildebrandt, Mireille. "Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics." *University of Toronto Law Journal* 68.supplement 1 (2018): 12-35.

peluang pelaku untuk terdeteksi relatif lebih kecil akibat keterbatasan kemampuan penegakan hukum dalam mengimbangi perkembangan teknologi.

Pola pemanfaatan kecerdasan buatan dalam kejahatan siber di Indonesia juga ditandai dengan tingginya tingkat anonimitas pelaku. Melalui teknik penyamaran identitas digital dan penggunaan sistem otomatis, pelaku dapat menyembunyikan jejak elektronik yang ditinggalkan. Hal ini menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku dan membuktikan keterkaitan antara pelaku dengan perbuatan pidana yang dilakukan, mengingat sistem hukum pidana Indonesia masih sangat bergantung pada pembuktian identitas dan peran subjek hukum secara jelas.

Selain bersifat anonim, kejahatan siber berbasis kecerdasan buatan juga cenderung bersifat lintas batas negara. Pelaku dapat mengoperasikan sistem kejahatan dari luar wilayah Indonesia, sementara korban berada di dalam negeri. Pola kejahatan yang bersifat transnasional ini menimbulkan persoalan yurisdiksi serta menuntut adanya kerja sama antarnegara dalam proses penegakan hukum. Dalam praktiknya, perbedaan sistem hukum dan keterbatasan mekanisme kerja sama internasional seringkali menjadi kendala dalam menindak pelaku kejahatan siber secara efektif.

Hambatan yang dihadapi aparat penegak hukum dalam menangani kejahatan siber yang melibatkan pemanfaatan kecerdasan buatan

Penegakan hukum terhadap kejahatan siber yang melibatkan pemanfaatan kecerdasan buatan di Indonesia arasnya berasal dari persoalan implementasi kebijakan publik di bidang hukum dan teknologi informasi. Perkembangan kecerdasan buatan yang sangat pesat telah menciptakan bentuk dan pola kejahatan siber yang semakin kompleks, sementara kebijakan hukum yang ada belum sepenuhnya mampu mengakomodasi dinamika tersebut. Kondisi ini menunjukkan bahwa tantangan utama tidak hanya terletak pada ketiadaan norma hukum semata, tetapi juga pada kemampuan negara dalam melaksanakan kebijakan penegakan hukum secara efektif di tengah perubahan teknologi yang berlangsung cepat.

Dari perspektif kebijakan publik, problematik implementasi kebijakan dengan ditandai kegagapan kebijakan[18], ini dibuktikan dalam permasalahan utama yang dihadapi

[18] Hermanto, Bagus. "Deliberate legislative reforms to improve the legislation quality in developing countries: case of Indonesia." *The Theory and Practice of Legislation* 11.1 (2023): 1-31.

aparat penegak hukum berkaitan dengan kesenjangan antara tujuan kebijakan dan kapasitas pelaksana kebijakan di lapangan.[19] Secara normatif, negara memiliki kewajiban untuk memberikan perlindungan hukum kepada masyarakat dari berbagai bentuk kejahatan siber. Namun, dalam praktiknya, kebijakan penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan belum didukung oleh perangkat kebijakan yang bersifat teknis dan operasional. Akibatnya, aparat penegak hukum kerap menghadapi kesulitan dalam menerjemahkan ketentuan hukum yang bersifat umum ke dalam tindakan penegakan hukum yang konkret dan efektif.

Dalam konteks hukum siber, ketentuan peraturan perundang-undangan yang saat ini berlaku, seperti UU ITE dan KUHP, masih berorientasi pada pola kejahatan konvensional. Ketentuan tersebut pada umumnya menempatkan manusia sebagai pelaku utama tindak pidana, sementara dalam kejahatan siber berbasis kecerdasan buatan, perbuatan pidana sering kali dijalankan melalui sistem otomatis dan algoritma yang kompleks. Ketidaksesuaian ini menimbulkan kesulitan dalam menentukan konstruksi pertanggungjawaban pidana, khususnya dalam mengaitkan perbuatan melawan hukum dengan subjek hukum tertentu secara jelas.

Permasalahan pembuktian juga menjadi hambatan signifikan dalam penegakan hukum kejahatan siber berbasis kecerdasan buatan. Dari sudut pandang hukum pidana, pembuktian mensyaratkan adanya alat bukti yang sah dan keyakinan hakim terhadap kesalahan terdakwa. Namun, kejahatan yang dijalankan melalui sistem kecerdasan buatan sering kali meninggalkan jejak digital yang tidak mudah dilacak dan dipahami. Proses pembuktian dalam perkara semacam ini menuntut kemampuan analisis forensik digital yang tinggi, sementara kebijakan peningkatan kapasitas aparat penegak hukum di bidang teknologi informasi belum sepenuhnya berjalan secara merata dan berkelanjutan.

Keterbatasan sumber daya manusia aparat penegak hukum juga mencerminkan lemahnya implementasi kebijakan publik di bidang penegakan hukum siber. Penanganan kejahatan siber berbasis kecerdasan buatan memerlukan pemahaman yang memadai mengenai sistem digital, cara kerja algoritma, serta karakteristik teknologi kecerdasan buatan. Namun, tidak semua aparat penegak hukum memiliki latar belakang pendidikan atau pelatihan yang relevan dengan kebutuhan tersebut. Kondisi ini menyebabkan proses

---

[19]Natesan, Sarabjeet D., and Rahul R. Marathe. "Literature review of public policy implementation." *International Journal of Public Policy* 11.4-6 (2015): 219-241.

penyelidikan dan penyidikan sering kali berjalan lambat dan kurang optimal, terutama ketika berhadapan dengan modus kejahatan yang terus berkembang.

Keterbatasan sarana dan prasarana penunjang juga menjadi kendala dalam implementasi kebijakan penegakan hukum. Penanganan kejahatan siber berbasis kecerdasan buatan memerlukan perangkat teknologi khusus, seperti sistem forensik digital dan infrastruktur pendukung lainnya.[20] Dalam praktiknya, fasilitas tersebut belum tersedia secara merata di seluruh wilayah Indonesia. Ketimpangan ini berpengaruh terhadap kemampuan aparat penegak hukum dalam penanganan kejahatan siber, sehingga efektivitas penegakan hukum menjadi berbeda.

Dari perspektif kebijakan publik, pola kebijakan mendasarkan pada konteks sifat kejahatan siber berbasis kecerdasan buatan yang lintas batas negara juga menimbulkan tantangan tersendiri dalam tahap implementasi. Pelaku kejahatan dapat dengan mudah mengoperasikan sistem kejahatan dari luar wilayah Indonesia, sementara korban berada di dalam negeri. Kondisi ini menuntut adanya kerja sama internasional yang efektif sebagai bagian dari kebijakan penegakan hukum siber. Namun, dalam praktiknya, perbedaan sistem hukum, keterbatasan perjanjian kerja sama, serta prosedur birokrasi yang panjang seringkali menghambat proses penegakan hukum terhadap pelaku kejahatan siber transnasional.[21]

Tingginya tingkat anonimitas pelaku kejahatan siber berbasis kecerdasan buatan juga memperlihatkan keterbatasan kebijakan hukum dalam menjangkau pelaku secara efektif. Penggunaan identitas digital palsu dan sistem otomatis memungkinkan pelaku untuk menyamarkan jejak serta keberadaannya. Hal ini menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku dan membuktikan keterlibatannya dalam tindak pidana, sehingga meningkatkan risiko tidak terungkapnya perkara secara menyeluruh.

Selain itu, belum optimalnya koordinasi antarinstansi yang berwenang menunjukkan adanya persoalan tata kelola kebijakan publik di bidang hukum siber. Penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan melibatkan berbagai aktor, baik aparat penegak hukum maupun instansi yang memiliki kewenangan di bidang teknologi informasi dan perlindungan data. Tanpa koordinasi yang jelas dan

[20] Faqir, Raed SA. "Digital criminal investigations in the era of artificial intelligence: a comprehensive overview." *International Journal of Cyber Criminology* 17.2 (2023): 77-94.
[21] Robichau, Robbie Waters, and Laurence E. Lynn Jr. "The implementation of public policy: Still the missing link." *Policy studies journal* 37.1 (2009): 21-36.

kebijakan yang terintegrasi, upaya penegakan hukum cenderung berjalan secara sektoral dan kurang efektif. Berdasarkan uraian tersebut, dapat disimpulkan bahwa hambatan penegakan hukum siber berbasis kecerdasan buatan bukanlah segi problema aspek hukum positif, namun lebih berdasar lagi pada aras persoalan implementasi kebijakan publik.

Kecukupan peraturan perundang-undangan yang berlaku telah memadai dalam konteks implementasi kebijakan Hukum Siber nasional atas penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan di Indonesia

Perkembangan kecerdasan buatan (*artificial intelligence*) kaitannya dengan pemanfaatan teknologi ini pada dasarnya memberikan banyak manfaat, terutama dalam meningkatkan efisiensi dan mendorong inovasi di berbagai bidang. Namun demikian, di balik manfaat tersebut, kecerdasan buatan.[22] Situasi ini menimbulkan persoalan hukum, khususnya mengenai kebijakan yang berlaku saat ini telah mampu menjadi dasar yang memadai dalam penegakan hukum siber yang memanfaatkan kecerdasan buatan.

Secara normatif, Indonesia hingga saat ini belum memiliki regulasi khusus yang secara komprehensif mengatur kecerdasan buatan, baik dalam kedudukannya sebagai objek hukum maupun sebagai sarana berbuat tindak pidana. Penegakan hukum terhadap kejahatan siber yang melibatkan kecerdasan buatan masih mengandalkan peraturan yang bersifat umum. Meskipun UU ITE telah memuat berbagai larangan terkait perbuatan di ruang siber, seperti akses tanpa hak, manipulasi data elektronik, penipuan, dan penyebaran informasi palsu, pengaturan tersebut belum secara tegas mengatur penggunaan kecerdasan buatan sebagai alat utama dalam melakukan kejahatan siber. Hal ini menunjukkan bahwa pada tataran regulasi tertinggi atau kebijakan makro, pengaturan hukum yang ada masih belum sepenuhnya menyesuaikan diri dengan perkembangan teknologi.

Selain UU ITE, KUHP juga masih digunakan sebagai dasar hukum dalam menangani kejahatan siber. Beberapa ketentuan dalam KUHP, seperti tindak pidana penipuan, pemalsuan, dan pencemaran nama baik, dinilai masih relevan untuk diterapkan. Namun, KUHP disusun dengan asumsi bahwa pelaku tindak pidana adalah manusia yang melakukan perbuatan secara langsung. Asumsi tersebut menyebabkan KUHP kurang

---

[22] Anna, Ubaydullayeva. "Artificial intelligence and intellectual property: Navigating the complexities of cyber law." *International Journal of Law and Policy* 1 (2023): 1-8.

mampu menjangkau karakteristik kejahatan siber berbasis kecerdasan buatan yang dijalankan melalui sistem otomatis dan algoritma yang dapat bekerja secara mandiri. Dari sudut pandang hukum siber, kondisi ini menunjukkan adanya ketidaksesuaian antara hukum pidana konvensional dengan realitas kejahatan di ruang digital.

Keterbatasan pengaturan tersebut berdampak pada munculnya persoalan mendasar dalam penegakan hukum, terutama terkait pertanggungjawaban pidana. Sistem hukum pidana Indonesia menganut asas *geen straf zonder schuld* yang menekankan adanya unsur kesalahan berupa kesengajaan atau kealpaan dari subjek hukum manusia. Dalam kejahatan siber yang melibatkan kecerdasan buatan, penentuan pihak yang harus dimintai pertanggungjawaban pidana menjadi tidak sederhana, apakah pengguna sistem, pengembang teknologi, penyedia platform, atau pihak lain yang memperoleh keuntungan dari penggunaan kecerdasan buatan tersebut. Ketidakjelasan ini berpotensi menimbulkan ketidakpastian hukum dalam praktik penegakan hukum.

Selain masalah pertanggungjawaban pidana, kelemahan regulasi juga terlihat pada aspek pembuktian. Walaupun terdapat rumusan UU ITE, pengaturan tersebut belum disertai dengan ketentuan teknis yang memadai terkait pembuktian kejahatan siber yang melibatkan algoritma dan sistem pembelajaran mesin. Akibatnya, aparat penegak hukum sering mengalami kesulitan dalam membuktikan keterkaitan antara perbuatan pidana, sistem kecerdasan buatan yang digunakan, serta pihak yang bertanggung jawab. Kondisi ini mencerminkan belum optimalnya pengaturan pada tataran kebijakan mikro, yaitu aturan teknis yang seharusnya mendukung proses penegakan hukum di lapangan.

Ditinjau dari perspektif hukum dan kebijakan publik, permasalahan tersebut tidak hanya berkaitan dengan kekurangan norma hukum, tetapi juga dengan lemahnya aspek implementasi kebijakan. Regulasi yang ada masih cenderung bersifat reaktif dan belum sepenuhnya mampu mengantisipasi perkembangan teknologi yang sangat cepat. Padahal, hukum pidana seharusnya tidak hanya berfungsi sebagai sarana pemidanaan, tetapi juga sebagai instrumen kebijakan publik yang bersifat preventif dalam mencegah terjadinya kejahatan[23].

Kondisi ini semakin relevan apabila dikaitkan dengan kebijakan nasional di bidang kecerdasan buatan. Pemerintah Indonesia telah menetapkan Strategi Nasional

[23] Bhushan, Tripti. "Artificial Intelligence, Cyberspace and International Law." *Indonesian J. Int'l L.* 21 (2023): 281.

Kecerdasan Artifisial melalui Peraturan Presiden Nomor 88 Tahun 2021 yang menekankan pentingnya pengembangan dan pemanfaatan kecerdasan buatan secara bertanggung jawab dan beretika. Namun, kebijakan tersebut lebih difokuskan pada aspek pengembangan dan pemanfaatan teknologi di sektor-sektor strategis, sementara pengaturan mengenai penegakan hukum pidana terhadap penyalahgunaan kecerdasan buatan, khususnya dalam kejahatan siber, belum diatur secara rinci. Hal ini menunjukkan adanya kelemahan pada tingkat kebijakan meso, yaitu peraturan pelaksana yang seharusnya menghubungkan kebijakan nasional dengan praktik penegakan hukum.

Ketiadaan pengaturan yang terintegrasi antara kebijakan kecerdasan buatan dan sistem penegakan hukum pidana berdampak pada lemahnya kepastian hukum. Aparat penegak hukum masih harus melakukan penafsiran yang luas terhadap ketentuan dalam UU ITE dan KUHP untuk menjerat pelaku kejahatan siber berbasis kecerdasan buatan. Meskipun pendekatan ini dapat digunakan sebagai langkah sementara, namun berpotensi menimbulkan perbedaan penafsiran dan ketidakkonsistenan dalam penegakan hukum. Selain itu, kondisi tersebut juga berdampak pada perlindungan hukum bagi korban kejahatan siber yang belum sepenuhnya terpenuhi.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa peraturan perundang-undangan yang berlaku di Indonesia saat ini belum sepenuhnya memadai sebagai dasar penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan. Permasalahan ini tidak hanya terletak pada aspek normatif, tetapi juga pada belum terbangunnya keterpaduan kebijakan pada tingkat makro, meso, dan mikro. Oleh karena itu, diperlukan penguatan hukum siber yang tidak hanya berfokus pada pembentukan norma hukum baru, tetapi juga pada efektivitas implementasi kebijakan, agar penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan dapat berjalan secara lebih efektif dan memberikan kepastian hukum bagi masyarakat.

KESIMPULAN DAN SARAN

Kecerdasan buatan telah mengubah karakter dan pola kejahatan siber di Indonesia menjadi lebih kompleks, cepat, sistematis, anonim, dan berskala lintas negara, sehingga menimbulkan tantangan signifikan bagi aparat penegak hukum dalam hal identifikasi, pembuktian, dan penentuan pertanggungjawaban pidana, disertai pelbagai hambatan, yang belum sepenuhnya adaptif terhadap perkembangan teknologi. Dengan demikian,

penegakan hukum siber berbasis kecerdasan buatan membutuhkan penguatan kebijakan secara menyeluruh pada tingkatan makro, meso, dan mikro, peningkatan kompetensi aparat, penyediaan infrastruktur penunjang, serta penguatan kerja sama nasional dan internasional, agar implementasi hukum dapat berjalan efektif sekaligus menjamin kebijakan yang berkepastian hukum maupun menjangkau perlindungan seoptimal mungkin bagi masyarakat di era digital.

Perlunya penguatan regulasi dan kebijakan hukum siber yang mampu mengikuti perkembangan kecerdasan buatan, terutama terkait kejahatan siber yang dijalankan secara otomatis dan berskala luas. Selain itu, peningkatan kemampuan aparat penegak hukum melalui pelatihan khusus, penyediaan sarana forensik digital yang memadai, serta koordinasi yang lebih baik antarinstansi dan kerja sama internasional menjadi langkah mendasar dalam penguatan implementasinya. Dengan kombinasi pembaruan kebijakan serta meningkatkan kapasitas aparat, diharapkan penegakan hukum siber di Indonesia dapat lebih efektif, berkepastian hukum, maupun melindungi masyarakat terhadap resistensi kejahatan digital dengan pelbagai kompleksitasnya.

DAFTAR REFERENSI

Jurnal

Agus Rahardjo, “Penegakan Hukum di Era Digital,” *Jurnal Hukum Ius Quia Iustum* 27, no. 2 (2020): 205–208.

Al Fatih, Sholahuddin, et.al. "Understanding Regulations Of Online Gambling In Indonesia: Is It Forbidden?." *Jurisdictie: Jurnal Hukum dan Syariah* 16, no. 1 (2025): 55-76.

Alarie, Benjamin, Anthony Niblett, and Albert H. Yoon. "How artificial intelligence will affect the practice of law." *University of Toronto Law Journal* 68.supplement 1 (2018): 106-124.

Anggraeny, *Pertanggungjawaban Pidana dalam Kejahatan Siber Berbasis Artificial Intelligence: Tantangan Perlindungan Data Pribadi dan Data Sintetis*, Jurnal Hukum Siber, Vol. 5 No. 3, 2025, 201–203.

Bhushan, Tripti. "Artificial Intelligence, Cyberspace and International Law." *Indonesian J. Int'l L.* 21 (2023): 281.

Dimas Prayoga dan Muhammad Tuasikal, *Deepfake sebagai Tindak Pidana Pencemaran Nama Baik dalam Perspektif Hukum Pidana Indonesia*, Jurnal Ilmu Hukum, Vol. 9 No. 1, 2025, 88–90.

Hermanto, Bagus. "Deliberate legislative reforms to improve the legislation quality in developing countries: case of Indonesia." *The Theory and Practice of Legislation* 11.1 (2023): 1-31.

Hermanto, Bagus, I. Gede Yusa, and Ni Ketut Ardani. "Problems and Reform of Indonesia's Cyber Law: A Comparative Study with Other Countries." *Literasi Hukum* 9, no. 1 (2025): 45-58.

Hermanto, Bagus, Nur, Asrul Ibrahim & Zulfa, Indana, "Dinamika Pengaturan Hukum Siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam Ius Constituendum", *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 14, no. 2 (2025): 315-335.

Hildebrandt, Mireille. "Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics." *University of Toronto Law Journal* 68.supplement 1 (2018): 12-35.

Hutchinson, Terry. "The doctrinal method: Incorporating interdisciplinary methods in reforming the law." *Erasmus L. Rev.* 8 (2015): 130.

Natesan, Sarabjeet D., and Rahul R. Marathe. "Literature review of public policy implementation." *International Journal of Public Policy* 11.4-6 (2015): 219-241.

Ponkin, Igor V., and Alena I. Redkina. "Artificial intelligence from the point of view of law." *RUDN Journal of Law* 22.1 (2018): 91-109.

Siems, Mathias M. "Legal research in search of attention: A quantitative assessment." *King's Law Journal* 27.2 (2016): 170-187.

Sigid Suseno, "Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *Jurnal Ilmu Hukum* 8, no. 1 (2021): 60–62.

Wahyudi, *Penegakan Hukum terhadap Kejahatan Siber Berbasis Kecerdasan Buatan di Indonesia*, Jurnal Hukum dan Teknologi Informasi, Vol. 7 No. 2, 2025, hlm. 145–147.

Widodo, "Tantangan Penegakan Hukum Kejahatan Siber," *Jurnal Legislasi Indonesia* 18, no. 3 (2021): 315.

Widodo Tresno Novianto, "Kejahatan Siber dalam Perspektif Hukum Pidana," *Jurnal Hukum Ius Quia Iustum* 23, no. 1 (2016).

Buku

Barda Nawawi Arief, *Tindak Pidana Mayantara (Cyber Crime)* (Jakarta: RajaGrafindo Persada, 2020).

Peraturan Perundang-Undang

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952), dan terakhir dengan Undang-undang Nomor 1 Tahun 2024 (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).

Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 180, Tambahan Lembaran Negara Republik Indonesia Nomor 6787).