Jurnal Ilmu Hukum dan Sosial (HAKIM)
Vol. 3 No. 4 November 2025, Hal. 1387-000
E-ISSN: 2987-7539; P-ISSN: 2987-6737
https://journal.stekom.ac.id/index.php/Hakim

Strategi Penuntutan Kejahatan Siber dengan Artificial Intelligence di Era Digital

Cindy Tania*[1], Janwan Gidalty[2]
[1,2]*Fakultas Studi Akademik, Universitas Sains dan Teknologi Komputer, Semarang*
E-mail: cindytania@gmail.com
*Corresponding Author

Article Info

Keywords:
Artificial Intelligence
Cybercrime Prosecution
Legal Strategy

Abstract

The rapid escalation of cybercrime in Indonesia and worldwide highlights the urgent need for adaptive legal strategies that integrate emerging technologies. This study investigates how Artificial Intelligence (AI) can strengthen prosecution strategies against cybercrime, focusing on law enforcement readiness, implementation challenges, and the opportunities it presents. Using a qualitative approach supported by empirical data, the research combines doctrinal legal analysis, socio-legal perspectives, and case studies through in-depth interviews with prosecutors, investigators, and digital forensic experts, alongside secondary data from national and international reports. The results reveal that while awareness of AI's potential is relatively high, its actual use in legal practice remains limited, with only 30 percent of respondents having direct experience with AI tools. Statistical data also confirm a significant increase in cyberattacks from 215 million anomalies in 2022 to nearly 400 million in 2024, underscoring the urgency of adopting AI. Findings show that AI can enhance the identification of digital evidence, detect hidden patterns in cyberattacks, and improve the effectiveness of prosecution. However, concerns about algorithmic bias and the lack of legal frameworks persist. This study contributes to academic discourse by offering an applied framework for AI-based prosecution strategies in developing countries and by providing practical recommendations for prosecutors and policymakers to accelerate digital legal reforms. The novelty lies in bridging theoretical discussions with an operational model contextualized to Indonesia's legal environment.

DOI: https://doi.org/10.51903/j928ts68
Submitted: August 2025, Reviewed: September 2025, Accepted: October 2025
**Corresponding Author*

I. PENDAHULUAN

Perkembangan teknologi digital telah melahirkan perubahan fundamental dalam kehidupan manusia modern. Internet, media sosial, dan teknologi berbasis data kini menjadi bagian tak terpisahkan dari aktivitas sehari-hari, mulai dari interaksi sosial, pendidikan, hingga transaksi ekonomi (Schaufelbühl et al., 2024). Transformasi ini membawa banyak keuntungan, seperti percepatan komunikasi, efisiensi layanan publik, serta lahirnya model bisnis baru berbasis digital. Namun, di balik manfaat besar tersebut, terdapat pula sisi gelap berupa maraknya kejahatan siber (Tuazon et al., 2024). Jika pada masa lalu tindak pidana lebih banyak meninggalkan jejak fisik yang dapat ditelusuri aparat penegak hukum, saat ini pelaku kejahatan beroperasi dalam ruang maya dengan teknik penyamaran identitas,

penggunaan perangkat enkripsi, dan strategi serangan yang semakin canggih. Situasi ini menimbulkan tantangan serius bagi aparat penegak hukum, khususnya jaksa sebagai aktor utama dalam proses penuntutan (Hukom & Martinus, 2025). Penuntutan yang selama ini bertumpu pada bukti fisik dan keterangan saksi kini harus berhadapan dengan bukti digital yang sering kali sulit diverifikasi, sehingga diperlukan strategi yang jauh lebih adaptif.

Kehadiran AI membuka peluang baru bagi aparat hukum untuk menghadapi tantangan tersebut. AI memungkinkan analisis data dalam skala besar secara cepat dan akurat, mendeteksi pola aktivitas mencurigakan, hingga melakukan prediksi terhadap potensi tindak pidana siber (Chakraborty & Mitra, 2024). Teknologi ini mampu memproses berbagai bentuk bukti digital, mulai dari log aktivitas, metadata, hingga pola lalu lintas jaringan yang dapat mengungkap jejak pelaku kejahatan. Di satu sisi, AI berpotensi memperkuat efektivitas penuntutan dengan menyediakan analisis berbasis data yang lebih komprehensif. Namun, di sisi lain, pemanfaatannya menimbulkan dilema etis dan yuridis, seperti potensi bias algoritmik yang dapat memengaruhi keadilan, persoalan perlindungan data pribadi, serta ketidakpastian mengenai keabsahan bukti yang diproses melalui AI di hadapan pengadilan (Laksito et al., 2024). Pertanyaan penting yang kemudian muncul adalah bagaimana memanfaatkan AI secara optimal dalam penuntutan kejahatan siber tanpa mengorbankan prinsip-prinsip dasar hukum, seperti kepastian hukum, due process of law, dan keadilan substantif.

Kejahatan siber kini juga semakin kompleks karena bersifat lintas batas negara. Banyak kasus melibatkan aktor-aktor yang beroperasi di yurisdiksi berbeda, dengan kemampuan teknologi jauh lebih maju dibandingkan instrumen penegakan hukum tradisional (Hukom & Setiadi, 2025). Fenomena ini tidak hanya menghadirkan kesulitan teknis dalam pelacakan dan pengumpulan bukti, tetapi juga menimbulkan persoalan koordinasi antarnegara dan harmonisasi hukum internasional. Di tengah dinamika ini, urgensi penelitian mengenai strategi penuntutan yang inovatif semakin nyata (Yu et al., 2024). Tanpa inovasi hukum yang berbasis teknologi, aparat hukum berisiko tertinggal dari dinamika kejahatan yang terus berevolusi, sementara masyarakat menuntut perlindungan hukum yang lebih kuat dan efektif.

Laporan (Interpol, 2024) menyebutkan bahwa pada tahun 2023 terdapat lebih dari 493 juta serangan siber di seluruh dunia, dengan kerugian ekonomi mencapai USD 8,1 triliun. Angka ini menempatkan kejahatan siber sebagai salah satu ancaman terbesar bagi stabilitas ekonomi global, sejajar dengan kejahatan narkotika dan terorisme internasional. Di berbagai negara, serangan ransomware melumpuhkan layanan publik, sementara kasus kebocoran data menimbulkan keresahan sosial dan krisis kepercayaan terhadap pemerintah maupun sektor swasta (Radu, 2025). Dengan cakupan ancaman yang demikian luas, penuntutan yang lamban dan tidak adaptif hanya akan memperburuk keadaan, sebab pelaku kejahatan dapat terus mengeksploitasi celah hukum dan teknologi (Hansel & Silomon, 2024).

Situasi di Indonesia juga tidak kalah mengkhawatirkan. (Badan Siber dan Sandi Negara (BSSN), 2024) melaporkan adanya lebih dari 361 juta anomali serangan siber sepanjang tahun 2023. Jenis serangan yang dominan mencakup phishing, ransomware, serta kebocoran data pribadi yang menimpa lembaga publik maupun swasta. Salah satu kasus besar adalah kebocoran data yang melibatkan informasi jutaan warga, yang kemudian diperjualbelikan di forum daring internasional (Scott, 2024). Peristiwa ini menimbulkan keresahan publik dan memunculkan pertanyaan mengenai kapasitas negara dalam melindungi hak-hak digital masyarakat. Kondisi tersebut mempertegas bahwa strategi penuntutan yang hanya mengandalkan cara-cara tradisional sudah tidak memadai, dan adopsi AI dalam sistem hukum menjadi kebutuhan yang mendesak (Rawat et al., 2022). Dengan kata lain, tanpa transformasi hukum berbasis teknologi, Indonesia berisiko menjadi sasaran empuk kejahatan siber yang semakin meningkat.

Namun, kesiapan aparat penegak hukum untuk merespons tantangan ini masih menghadapi kendala serius. Penelitian oleh (Sitompul et al., 2024) menyoroti bahwa kompleksitas kejahatan teknologi informasi (cybercrime) dan keterbatasan kerangka hukum serta kapasitas SDM masih menjadi hambatan signifikan dalam penanganan kasus digital di Indonesia. Mayoritas aparat masih terbentur oleh keterbatasan infrastruktur teknologi, rendahnya literasi digital hukum, serta belum adanya pedoman baku mengenai penggunaan AI dalam konteks pembuktian hukum (Faqir, 2023). (Rajendra & Thuraisingam, 2025) menegaskan bahwa kesenjangan antara ancaman yang terus meningkat dengan kapasitas institusional aparat hukum dapat mengakibatkan sistem peradilan kehilangan legitimasi di mata masyarakat. Data ini sekaligus menyingkap ironi bahwa meski kejahatan siber meningkat secara signifikan, respons hukum justru masih lambat dan parsial.

Berbagai literatur di Indonesia menunjukkan bahwa perhatian akademisi terhadap isu kejahatan siber umumnya terbatas pada aspek regulasi, keamanan data, dan pencegahan. Penelitian (Anwary, 2022) menyoroti pentingnya harmonisasi hukum nasional dengan instrumen hukum internasional untuk menghadapi kejahatan lintas batas. (Gojali, 2023) menekankan lemahnya pembuktian digital di pengadilan, di mana bukti elektronik sering kali tidak mampu menandingi kecanggihan metode penyamaran pelaku. Sementara itu, (Imran, 2023) lebih menitikberatkan pada literasi digital masyarakat sebagai strategi pencegahan. Meskipun kajian ini penting, semuanya masih berfokus pada aspek normatif dan preventif, sehingga aspek strategis penuntutan yang berbasis teknologi, khususnya AI, belum banyak dibahas. Kekosongan inilah yang memperlihatkan perlunya kajian lebih mengenai pemanfaatan AI untuk memperkuat proses penuntutan.

Di tingkat global, diskursus mengenai pemanfaatan AI dalam hukum berkembang lebih variatif. (Züger & Asghari, 2023) menegaskan bahwa AI dapat memperkuat kemampuan aparat hukum dalam mendeteksi pola kriminal melalui analisis big data, terutama pada kasus dengan volume bukti digital yang masif. (Greenstein, 2022) mengingatkan adanya risiko bias algoritmik yang dapat mengganggu prinsip keadilan prosedural. (Benefo et al., 2022) bahkan menunjukkan bagaimana AI digunakan di

beberapa yurisdiksi untuk memprediksi risiko residivisme, meskipun praktik ini menuai kontroversi etis. Dengan demikian, literatur global sudah bergerak dari sekadar pembahasan konseptual menuju pemanfaatan praktis, meskipun masih disertai perdebatan mengenai legitimasi dan etika.

Sejumlah studi juga menyoroti dilema penggunaan AI dalam hukum dari aspek etis dan teknis. (Kumar & Suthar, 2024) menekankan persoalan privasi dan keamanan data yang muncul dari pemanfaatan AI. (Sætra et al., 2022) melihat peluang pemanfaatan AI untuk menganalisis bukti digital dan mendeteksi pola kejahatan secara lebih cepat. (Zafar, 2024) menyoroti peran AI dalam penyusunan bukti yang lebih sistematis, sehingga dapat memperkuat argumentasi penuntutan. Namun, sebagian besar literatur masih bersifat deskriptif dan konseptual, belum menawarkan model operasional yang bisa langsung diadopsi aparat hukum dalam praktik penuntutan sehari-hari. Hal ini menunjukkan adanya jarak antara pemikiran teoretis dengan kebutuhan aplikatif di lapangan.

Oleh sebab itu, pemanfaatan AI di bidang hukum bukan hal yang mustahil, tetapi implementasinya sangat bergantung pada kesiapan regulasi dan sumber daya. Misalnya, di Amerika Serikat, AI digunakan untuk menganalisis kemungkinan pengulangan tindak pidana oleh terdakwa, tetapi mendapat kritik karena dianggap memperkuat bias rasial (Malek, 2022). Di Eropa, pendekatan yang lebih hati-hati diterapkan dengan menekankan aspek transparansi algoritme. Sementara di beberapa negara Asia, penggunaan AI lebih diarahkan untuk analisis forensik digital dalam kasus-kasus kejahatan ekonomi. Perbedaan ini menunjukkan bahwa setiap negara membutuhkan model yang sesuai dengan konteks sosial, hukum, dan budaya masing-masing (Karthikeyan et al., 2024).

Penelitian di Indonesia sejauh ini masih terbatas pada perdebatan normatif tentang legalitas penggunaan AI dalam proses hukum. Belum banyak kajian yang secara langsung merumuskan strategi penuntutan berbasis AI, sehingga aparat hukum tidak memiliki pedoman praktis untuk mengadopsinya. Padahal, mengingat tren global yang semakin mengarah pada pemanfaatan teknologi, Indonesia perlu bergerak cepat untuk mengembangkan kerangka kerja hukum yang lebih adaptif. Hal ini menjadi semakin penting mengingat kejahatan siber di Indonesia meningkat secara drastis, sementara kesiapan aparat hukum masih rendah.

Berdasarkan uraian konteks, perkembangan kejahatan siber, serta kesenjangan penelitian yang telah dipaparkan sebelumnya, diperlukan perumusan masalah yang mampu memberikan arah analisis yang lebih terfokus. Ketiadaan strategi penuntutan berbasis Artificial Intelligence dalam literatur hukum Indonesia menunjukkan adanya kebutuhan untuk mengidentifikasi bagaimana teknologi tersebut dapat diintegrasikan secara tepat dalam proses pembuktian dan penuntutan. Atas dasar itu, penelitian ini merumuskan tiga pertanyaan pokok, yakni: (1) bagaimana pemahaman dan penerapan AI oleh jaksa dalam proses penuntutan kejahatan siber di Indonesia; (2) faktor-faktor normatif dan empiris apa saja yang memengaruhi efektivitas penggunaan AI dalam penguatan bukti digital; dan (3) bagaimana strategi penuntutan berbasis AI dapat dirancang secara operasional agar selaras dengan kerangka

hukum nasional serta kebutuhan kelembagaan Kejaksaan RI. Rumusan masalah ini menjadi pijakan penting bagi penyusunan tujuan penelitian yang akan dijelaskan pada bagian berikutnya.

Tujuan utama penelitian ini adalah merumuskan strategi penuntutan kejahatan siber dengan memanfaatkan teknologi AI. Fokusnya adalah bagaimana algoritme dapat digunakan untuk mendukung penyusunan bukti, memprediksi pola kejahatan, serta meningkatkan efektivitas proses hukum. Kontribusi penelitian ini terletak pada kebaruan gagasan yang belum banyak disentuh dalam literatur hukum Indonesia, yakni strategi penuntutan berbasis AI yang kontekstual dengan realitas nasional. Secara akademis, penelitian ini diharapkan memperkaya khazanah literatur mengenai hukum digital di negara berkembang. Sementara secara praktis, penelitian ini dapat menjadi masukan penting bagi Kejaksaan Republik Indonesia dalam merumuskan kebijakan penuntutan yang lebih adaptif terhadap dinamika kejahatan siber. Dengan demikian, penelitian ini memiliki relevansi ganda: memberikan kontribusi teoritis dalam diskursus akademik, sekaligus menawarkan solusi praktis untuk memperkuat legitimasi dan efektivitas sistem hukum di era digital.

II. METODOLOGI

A. Desain Penelitian

Penelitian ini menggunakan pendekatan studi kasus dengan fokus pada penuntutan kasus kejahatan siber yang relevan di Indonesia. Studi kasus dipilih karena mampu memberikan pemahaman terhadap konteks sosial, hukum, dan teknologi yang melingkupi kejahatan siber. Selain itu, metode ini memungkinkan peneliti mengeksplorasi proses, hambatan, serta peluang penggunaan AI dalam penuntutan secara detail. Untuk memperkuat hasil analisis, penelitian juga memanfaatkan metode doctrinal legal research dengan mengkaji peraturan perundang-undangan yang berlaku, serta socio-legal research dengan menelaah praktik penegakan hukum yang ada di lapangan. Kombinasi ketiganya diharapkan menghasilkan temuan yang lebih komprehensif.

B. Sumber Data

Data primer diperoleh melalui wawancara dengan aparat penegak hukum, terutama jaksa yang pernah menangani kasus kejahatan siber yang berada wilayah Kejaksaan tingkat I dan II di Pulau Jawa, serta pakar hukum teknologi informasi dan forensik digital. Informan dipilih dengan metode purposive sampling, yakni berdasarkan pengalaman dan kompetensi mereka dalam bidang hukum siber. Wawancara dilakukan secara semi-terstruktur agar peneliti dapat menggali pengalaman praktis sekaligus mendapatkan ruang untuk eksplorasi topik baru yang muncul. Data sekunder diperoleh dari studi literatur yang mencakup peraturan perundang-undangan, dokumen kebijakan, laporan resmi dari lembaga seperti BSSN, Interpol, dan Kejaksaan Agung, serta publikasi akademik yang relevan. Untuk memperkaya analisis, penelitian juga menggunakan data statistik serangan siber dari laporan nasional dan internasional.

C. Teknik Pengumpulan Data

Proses pengumpulan data dilakukan dalam beberapa tahapan. Pertama, peneliti mengidentifikasi dan mengumpulkan dokumen hukum yang relevan, seperti Undang-Undang ITE, Kitab Undang-Undang Hukum Pidana, serta regulasi terkait perlindungan data pribadi. Kedua, dilakukan wawancara dengan aparat kejaksaan, penyidik, dan pakar hukum teknologi. Wawancara direkam dengan persetujuan informan dan ditranskrip secara verbatim untuk keperluan analisis. Ketiga, peneliti mengakses database serangan siber dari BSSN serta laporan tahunan lembaga internasional. Semua data yang diperoleh kemudian diverifikasi untuk menjamin keandalan dan validitasnya.

D. Prosedur Analisis Data

Analisis data dilakukan dengan menggunakan pendekatan tematik. Transkrip wawancara, dokumen hukum, serta data statistik dianalisis secara kualitatif untuk menemukan pola, kategori, dan tema yang relevan dengan tujuan penelitian. Analisis ini dilakukan dalam tiga tahap. Pertama, tahap reduksi data, di mana informasi yang tidak relevan dieliminasi untuk menjaga fokus penelitian. Kedua, tahap kategorisasi, yaitu mengelompokkan data berdasarkan tema-tema seperti tantangan penuntutan, peluang penggunaan AI, hambatan regulasi, serta praktik internasional. Ketiga, tahap interpretasi, di mana data yang telah dikategorikan dihubungkan dengan kerangka teori dan tujuan penelitian. Untuk memperkuat temuan, analisis kualitatif didukung dengan data kuantitatif berupa statistik serangan siber yang menggambarkan urgensi penerapan AI dalam penuntutan.

E. Validitas dan Reliabilitas

Untuk menjamin keabsahan data, penelitian ini menggunakan teknik triangulasi. Triangulasi sumber dilakukan dengan membandingkan data hasil wawancara, dokumen hukum, dan laporan statistik. Triangulasi metode digunakan dengan memadukan analisis doktrinal, sosio-legal, dan studi kasus. Selain itu, peneliti juga melakukan member checking dengan meminta konfirmasi dari sebagian informan mengenai hasil interpretasi wawancara. Proses ini dimaksudkan untuk memastikan bahwa temuan penelitian benar-benar merefleksikan pengalaman dan pandangan informan, bukan hasil interpretasi sepihak peneliti.

F. Kerangka Metode

Sebagai kerangka penelitian, metode ini menggabungkan tiga pendekatan utama. Pertama, analisis normatif untuk menelaah sejauh mana hukum positif mendukung atau membatasi pemanfaatan AI dalam penuntutan. Kedua, analisis empiris melalui wawancara dan data statistik untuk melihat kondisi faktual di lapangan. Ketiga, analisis komparatif dengan membandingkan praktik penggunaan AI di negara lain, seperti Amerika Serikat dan Eropa, untuk memperoleh pembelajaran yang relevan bagi konteks Indonesia. Melalui kombinasi ini, penelitian diharapkan mampu memberikan gambaran menyeluruh tentang strategi penuntutan kejahatan siber berbasis AI.

G. Alur Penelitian

Alur penelitian dimulai dengan identifikasi masalah melalui studi literatur dan analisis data statistik serangan siber. Tahap berikutnya adalah pengumpulan data primer melalui wawancara dengan aparat hukum dan pakar. Setelah data terkumpul, dilakukan analisis tematik yang menghubungkan temuan empiris dengan teori dan regulasi yang ada. Hasil analisis kemudian digunakan untuk merumuskan model strategi penuntutan berbasis AI yang kontekstual dengan kebutuhan Indonesia. Alur ini ditutup dengan penyusunan rekomendasi bagi pembuat kebijakan dan aparat penegak hukum.

III. HASIL DAN DISKUSI

Hasil

Penelitian ini menghasilkan temuan yang menggambarkan kondisi aktual kesiapan aparat penegak hukum, tantangan dalam penggunaan AI, serta peluang strategi yang dapat dikembangkan untuk memperkuat penuntutan kejahatan siber di Indonesia. Wawancara dengan aparat kejaksaan, penyidik, dan pakar forensik digital menunjukkan bahwa pemanfaatan AI masih berada pada tahap awal. Dari 20 informan (10 jaksa, 6 penyidik, 4 ahli forensik) hanya 6 orang yang pernah menggunakan teknologi analisis berbasis AI, sementara sebagian besar masih mengandalkan metode manual seperti analisis dokumen digital secara tradisional dan koordinasi antarinstansi. Temuan ini juga menunjukkan bahwa pemahaman aparat terhadap teknologi berbasis *artificial intelligence* masih bersifat konseptual dan belum terintegrasi dalam prosedur kerja teknis sehari-hari.

Hasil ini memperlihatkan adanya kesenjangan antara kesadaran akan potensi AI dan kemampuan praktis dalam mengimplementasikannya. Meski demikian, para informan mengakui bahwa AI memiliki peran penting dalam memperkuat bukti digital, khususnya dalam kasus phishing, ransomware, dan kebocoran data. AI mampu mendeteksi pola serangan melalui log activity dan metadata yang sulit ditelusuri secara manual. Namun, sebagian besar aparat mengungkapkan kekhawatiran mengenai belum adanya dasar hukum yang jelas terkait validitas bukti digital hasil analisis AI di pengadilan. Variasi pandangan tersebut mencerminkan perbedaan tingkat kesiapan individu dan institusi dalam merespons perkembangan teknologi analisis digital. Untuk memperjelas gambaran hasil penelitian, Tabel 1 menampilkan ringkasan data hasil wawancara mengenai kesiapan aparat kejaksaan dalam memanfaatkan AI.

Tabel 1. Kesiapan Aparat Hukum dalam Pemanfaatan AI

Kategori Kesiapan	Jumlah Responden	Persentase
Pernah menggunakan AI	6	30%
Mengetahui AI tetapi belum menerapkan	8	40%
Belum mengetahui potensi AI	6	30%

Sumber: Data primer hasil wawancara peneliti, (2025)

Tabel 1 memperlihatkan bahwa sebagian besar aparat hukum masih berada pada tahap mengetahui, tetapi belum mengimplementasikan AI secara langsung. Hanya 30 persen yang sudah memiliki pengalaman menggunakan teknologi ini. Kondisi tersebut menegaskan perlunya dukungan

infrastruktur, regulasi, dan peningkatan literasi digital di kalangan aparat hukum. Perbedaan ini berkaitan dengan akses terhadap pelatihan teknis, dukungan organisasi, serta ketersediaan sumber daya manusia yang memiliki kompetensi di bidang forensik digital dan *machine learning*.

Untuk memberikan gambaran lebih luas mengenai eskalasi kejahatan siber di Indonesia, diperlukan pembandingan antara temuan lapangan dan data resmi dari lembaga negara. Data sekunder berfungsi untuk menunjukkan konteks makro yang melatarbelakangi meningkatnya kompleksitas kejahatan siber. Informasi ini juga membantu memperlihatkan pola ancaman yang berkembang dari tahun ke tahun. Pendekatan komparatif ini digunakan untuk memperkuat pemahaman mengenai dinamika serangan siber secara nasional. Tabel 2 menampilkan data sekunder dari BSSN sebagai pembanding.

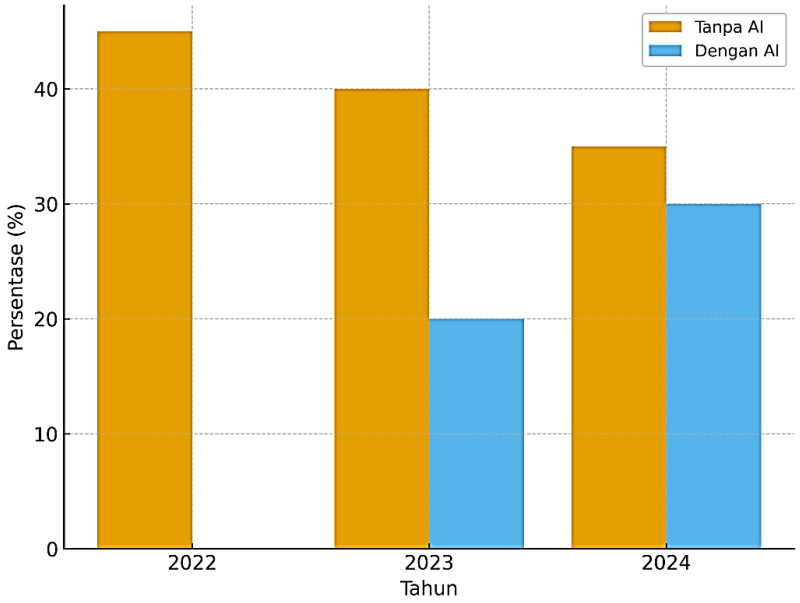
Tabel 2. Tren Kasus Kejahatan Siber di Indonesia (2022–2024)

Tahun	Jumlah Anomali Serangan Siber	Kasus Dominan
2022	215 juta	Phishing, Malware, Website Defacement
2023	361 juta	Phishing, Ransomware, Kebocoran Data
2024	398 juta	Ransomware, Data Breach, Social Engineering

Sumber: Laporan BSSN (2024), data diolah peneliti

Tabel 2 memperlihatkan adanya peningkatan jumlah anomali serangan siber dari tahun ke tahun dengan variasi jenis serangan yang semakin kompleks. Pada tahun 2022, serangan didominasi oleh *phishing*, *malware*, dan *website defacement* dengan jumlah anomali yang masih relatif lebih rendah dibandingkan tahun berikutnya. Tahun 2023 dan 2024 menunjukkan peningkatan signifikan baik dari sisi kuantitas maupun keragaman kasus, termasuk *ransomware*, *data breach*, dan *social engineering*. Perubahan pola ini mencerminkan adaptasi pelaku kejahatan siber terhadap sistem keamanan digital yang semakin berkembang.

Analisis tingkat keberhasilan penuntutan kasus siber diperlukan untuk memahami efektivitas praktik penegakan hukum dalam menghadapi kejahatan berbasis teknologi digital. Perbandingan lintas tahun dapat menunjukkan perubahan kinerja institusi penegak hukum seiring berkembangnya metode investigasi yang digunakan. Data ini juga memberikan konteks empiris mengenai dampak pemanfaatan teknologi analisis digital dalam proses pembuktian di pengadilan. Penggunaan teknologi berbasis *artificial intelligence* mulai dipertimbangkan sebagai salah satu faktor yang memengaruhi capaian penuntutan dalam kasus kejahatan siber. Gambar 1 menampilkan perbandingan tingkat keberhasilan penuntutan kasus siber (2022–2024).

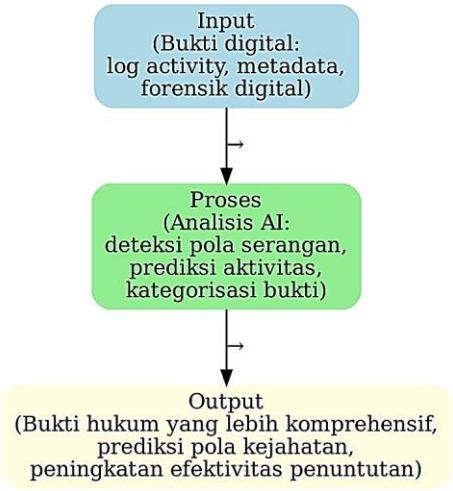


Gambar 1. Perbandingan Tingkat Keberhasilan Penuntutan Kasus Siber (2022–2024)

Sumber: Data diolah peneliti dari laporan Kejaksaan dan hasil wawancara (2025)

Gambar 1 menunjukkan tren peningkatan efektivitas penuntutan seiring mulai diperkenalkannya AI dalam proses analisis bukti digital. Pada 2024, meskipun penggunaannya masih terbatas, tingkat keberhasilan penuntutan berbasis AI sudah mendekati metode tradisional. Peningkatan ini berkaitan dengan kemampuan sistem analisis digital dalam mempercepat identifikasi dan pengelolaan bukti elektronik. Selain itu, integrasi teknologi berbasis *artificial intelligence* mulai memengaruhi pola kerja aparat dalam menyusun argumentasi pembuktian di persidangan.

Pemanfaatan AI dalam penuntutan kejahatan siber memerlukan pemahaman yang terstruktur mengenai alur kerja yang menghubungkan bukti digital dengan proses hukum. Hubungan antara data teknis dan kebutuhan pembuktian yuridis sering kali melibatkan tahapan yang kompleks dan saling terkait. Penyajian kerangka strategi membantu menjelaskan bagaimana teknologi dapat diintegrasikan secara sistematis dalam praktik penegakan hukum. Kerangka ini disusun untuk menggambarkan keterkaitan antara sumber data, proses analisis, dan hasil yang diharapkan dalam konteks penuntutan. Gambar 2 memvisualisasikan kerangka strategi pemanfaatan AI dalam penuntutan kejahatan siber.



Gambar 2. Kerangka Strategi Penuntutan Kejahatan Siber Berbasis AI

Sumber: Disusun oleh peneliti (2025)

Bagan ini memperlihatkan bahwa AI berfungsi sebagai jembatan antara kompleksitas bukti digital dengan kebutuhan pembuktian hukum yang sah, sehingga dapat memperkuat posisi jaksa dalam menyusun dakwaan dan menghadapi persidangan. Secara operasional, kerangka strategi pada Gambar 2 menunjukkan bahwa pemanfaatan AI dalam penuntutan kejahatan siber bergerak melalui tiga tahapan inti: (1) penguatan input bukti digital, (2) pemrosesan analitis berbasis algoritme, dan (3) penyusunan argumentasi hukum oleh jaksa. Setiap tahapan memiliki peran yang saling melengkapi dalam memastikan bahwa bukti digital dapat diolah secara akurat dan relevan secara hukum. Struktur bertahap ini membantu menjelaskan alur pemanfaatan teknologi berbasis *artificial intelligence* dalam mendukung proses penuntutan yang berbasis bukti digital.

Pada tahap pertama, AI digunakan untuk mengekstraksi artefak digital dari log aktivitas, metadata, pola lalu lintas jaringan, serta rekonstruksi serangan. Tahap ini memungkinkan identifikasi awal pola kejahatan yang selama ini tidak terlihat dengan metode manual. Pada tahap kedua, sistem AI melakukan pengelompokan pola serangan, analisis korelasi, serta deteksi anomali yang relevan dengan unsur pidana. Output analitis ini kemudian menjadi dasar bagi tahap ketiga, yaitu penyusunan konstruksi hukum oleh jaksa. Dalam tahap ini, jaksa memanfaatkan hasil analisis AI untuk mengonstruksi alur perbuatan pelaku, memetakan unsur tindak pidana, serta memperkuat pembuktian melalui bukti digital yang lebih sistematis. Dengan demikian, kerangka strategi tersebut tidak hanya menggambarkan hubungan konseptual antara teknologi dan penuntutan, tetapi juga menawarkan alur kerja konkret yang dapat diterapkan aparat penegak hukum untuk meningkatkan efektivitas penuntutan berbasis AI.

Diskusi

Temuan penelitian ini memperlihatkan adanya peluang besar sekaligus tantangan dalam pemanfaatan AI untuk penuntutan kejahatan siber di Indonesia. Dari sisi peluang, hasil penelitian menunjukkan bahwa AI mampu mempercepat analisis bukti digital, mendeteksi pola kejahatan yang tidak terlihat

oleh metode manual, dan meningkatkan efektivitas penuntutan. Hal ini konsisten dengan temuan (Oatley, 2022) yang menegaskan peran AI dalam memperkuat kapasitas aparat hukum melalui analisis big data. Namun, penelitian ini juga mengonfirmasi adanya hambatan signifikan, seperti bias algoritmik, keterbatasan regulasi, serta minimnya literasi digital aparat hukum. Kekhawatiran ini serupa dengan yang diidentifikasi oleh (Kusak, 2022), yang memperingatkan risiko AI dalam mengganggu prinsip due process of law. Di Indonesia, keterbatasan kesiapan aparat terlihat dari survei internal dan hasil wawancara, di mana hanya sebagian kecil aparat yang sudah menggunakan teknologi ini.

Selain itu, penerapan AI dalam penuntutan kejahatan siber juga menimbulkan potensi bias algoritmik yang dapat berdampak langsung terhadap prinsip keadilan substantif. Bias dapat muncul dari kualitas dataset pelatihan, ketidakseimbangan representasi data, maupun asumsi algoritme yang tidak transparan. Dalam konteks hukum pidana, bias ini berpotensi memengaruhi proses penilaian bukti digital, klasifikasi tingkat ancaman, atau identifikasi pola serangan sehingga menghasilkan kesimpulan yang tidak akurat. Secara normatif, kondisi tersebut berkaitan erat dengan prinsip due process of law serta asas equality before the law, karena setiap keputusan berbasis AI harus tetap menjamin objektivitas dan tidak mendiskriminasi pihak tertentu. Oleh karena itu, pemanfaatan AI dalam penuntutan harus disertai mekanisme pengawasan manusia (*human oversight*), verifikasi manual terhadap hasil analisis algoritme, serta penerapan prinsip *explainability* untuk memastikan bahwa penggunaan AI tidak mengganggu keadilan substantif maupun hak-hak terdakwa.

Perbandingan dengan penelitian sebelumnya menunjukkan perbedaan kontribusi. (Dai & Boroomand, 2022) fokus pada harmonisasi regulasi hukum internasional, sementara penelitian ini menitikberatkan aspek aplikatif strategi penuntutan berbasis AI. (Neiva et al., 2022) menyoroti kelemahan sistem pembuktian digital, yang diperkuat penelitian ini dengan data empiris mengenai keterbatasan aparat dalam menghadirkan bukti digital yang sah di pengadilan. Dengan demikian, penelitian ini tidak hanya melanjutkan diskursus yang ada, tetapi juga memperluasnya ke ranah praktis.

Implikasi dari penelitian ini cukup luas. Pertama, secara akademis penelitian ini memperkaya literatur tentang hukum digital di negara berkembang dengan memberikan perspektif aplikatif strategi berbasis AI. Kedua, secara praktis penelitian ini memberikan masukan bagi Kejaksaan Republik Indonesia untuk mulai mengintegrasikan teknologi AI dalam penyusunan strategi penuntutan, sekaligus mendorong pemerintah untuk memperbarui regulasi hukum acara pidana agar bukti hasil analisis AI diakui sah. Ketiga, secara strategis penelitian ini mendorong kolaborasi lintas sektor antara aparat hukum, lembaga keamanan siber, dan pengembang teknologi untuk menciptakan ekosistem hukum yang lebih adaptif.

Keterbatasan penelitian ini adalah jumlah responden wawancara yang masih terbatas, sehingga hasilnya belum mewakili seluruh aparat hukum di Indonesia. Selain itu, penelitian ini belum melakukan pengujian langsung terhadap algoritme AI dalam kasus riil, melainkan lebih banyak

mendasarkan pada persepsi dan pengalaman aparat hukum. Keterbatasan ini juga menekankan pentingnya pemahaman kontekstual mengenai pemanfaatan teknologi berbasis *artificial intelligence* di berbagai jenis kasus siber. Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk memperluas jumlah responden dari berbagai wilayah, melakukan simulasi empiris penggunaan algoritme AI dalam kasus konkret, serta mengeksplorasi regulasi yang paling sesuai agar pemanfaatan AI tidak menimbulkan persoalan baru terkait etika dan legitimasi hukum.

IV. KESIMPULAN

Penelitian ini menegaskan bahwa pemanfaatan Artificial Intelligence (AI) dalam penuntutan kejahatan siber merupakan kebutuhan mendesak seiring meningkatnya kompleksitas bukti digital dan tingginya volume serangan siber. Temuan menunjukkan bahwa penggunaan AI masih terbatas di kalangan aparat penegak hukum, namun teknologi ini memiliki potensi signifikan untuk mempercepat analisis bukti, mengungkap pola serangan, serta meningkatkan efektivitas pembuktian. Keterbatasan kapasitas teknis, ketiadaan standar hukum mengenai keabsahan analisis berbasis AI, dan potensi bias algoritmik merupakan tantangan utama yang perlu segera diatasi. Kondisi ini menunjukkan bahwa pemanfaatan teknologi berbasis *artificial intelligence* harus disertai pemahaman menyeluruh mengenai kapasitas teknis dan kerangka hukum yang berlaku.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan beberapa langkah strategis dan aplikatif. Pertama, Kejaksaan RI perlu menyusun pedoman teknis pemanfaatan AI dalam penuntutan, termasuk standar verifikasi bukti digital dan mekanisme human oversight. Kedua, diperlukan program penguatan kapasitas jaksa melalui pelatihan forensik digital, pemahaman algoritme dasar, serta penggunaan alat analisis berbasis AI. Ketiga, pembuat regulasi perlu memperbarui kerangka hukum acara pidana, UU ITE, dan kebijakan perlindungan data pribadi agar mengatur secara jelas legalitas bukti digital yang dihasilkan melalui AI. Keempat, diperlukan pengembangan ekosistem kolaboratif antara Kejaksaan, BSSN, aparat kepolisian, dan penyedia teknologi untuk menjamin interoperabilitas data dan keamanan sistem. Dengan penerapan kebijakan tersebut, pemanfaatan AI diharapkan tidak hanya meningkatkan efektivitas penuntutan kejahatan siber, tetapi juga memperkuat legitimasi hukum, menjamin keadilan substantif, dan menghadirkan sistem peradilan pidana yang lebih adaptif terhadap dinamika digital.

REFERENSI

Anwary, I. (2022). The Role of Public Administration in Combating Cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216–227. https://doi.org/10.5281/zenodo.4766577

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Keamanan Siber 2023*. Badan Siber dan Sandi Negara. https://educsirt.kemendikdasmen.go.id/portal/berita/197

Benefo, E. O., Tingler, A., White, M., Cover, J., Torres, L., Broussard, C., Shirmohammadi, A., Pradhan, A. K., & Patra, D. (2022). Ethical, Legal, Social, and Economic (ELSE) Implications of

Artificial Intelligence at a Global Level: A Scientometrics Approach. *AI and Ethics*, *2*(4), 667–682. https://doi.org/10.1007/s43681-021-00124-6

Chakraborty, C., & Mitra, S. (2024). Machine Learning and AI in Cyber Crime Detection. In *Advancements in Cyber Crime Investigations and Modern Data Analytics* (pp. 143–174). CRC Press (Taylor & Francis Group). https://doi.org/10.1201/9781003471103-8

Dai, D., & Boroomand, S. (2022). A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. *Archives of Computational Methods in Engineering*, *29*(2), 1291–1309. https://doi.org/10.1007/s11831-021-09628-0

Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, *17*(2), 77–94. https://doi.org/10.5281/zenodo.4766706

Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, *17*(1), 1–11. https://doi.org/10.5281/zenodo.4766600

Greenstein, S. (2022). Preserving the Rule of Law in the Era of Artificial Intelligence (AI). *Artificial Intelligence and Law*, *30*(3), 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hansel, M., & Silomon, J. (2024). Ransomware as a Threat to Peace and Security: Understanding and Avoiding Political Worst-Case Scenarios. *Journal of Cyber Policy*, *9*(2), 159–178. https://doi.org/10.1080/23738871.2024.2357092

Hukom, R., & Martinus. (2025). The Effectiveness of Artificial Intelligence in Judicial Decision-Making in Indonesia. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 1032–1051. https://doi.org/10.51903/hakim.v3i1.2298

Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *3*(1), 750–768. https://doi.org/10.51903/perkara.v3i1.2353

Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology*, *17*(1), 223–235. https://doi.org/10.5281/zenodo.4766614

Interpol. (2024). *Interpol Annual Report 2023*. International Criminal Police Organization. https://www.interpol.int/content/download/22267/file/interpolannualreport2023en.pdf

Karthikeyan, R., Yi, C., & Boudourides, M. (2024). Criminal Justice in the Age of AI: Addressing Bias in Predictive Algorithms Used by Courts. In *The Ethics Gap in the Engineering of the Future* (2nd ed., pp. 27–50). Emerald Publishing. https://doi.org/10.1108/978-1-83797-635-520241003

Kumar, D., & Suthar, N. (2024). Ethical and Legal Challenges of AI in Marketing: An Exploration of Solutions. *Journal of Information, Communication and Ethics in Society*, *22*(1), 124–144. https://doi.org/10.1108/jices-05-2023-0068

Kusak, M. (2022). Quality of Data Sets That Feed AI and Big Data Applications for Law Enforcement. *ERA Forum*, *23*(2), 209–219. https://doi.org/10.1007/s12027-022-00719-4

Laksito, J., Idris, M. F., & Waryanto, A. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 774–790. https://doi.org/10.51903/hakim.v2i4.2154

Malek, M. A. (2022). Criminal Courts' Artificial Intelligence: The Way It Reinforces Bias and Discrimination. *AI and Ethics*, *2*(1), 233–245. https://doi.org/10.1007/s43681-022-00137-9

Neiva, L., Granja, R., & Machado, H. (2022). Big Data Applied to Criminal Investigations: Expectations of Professionals of Police Cooperation in the European Union. *Policing and Society*, *32*(10), 1167–1179. https://doi.org/10.1080/10439463.2022.2029433

Oatley, G. C. (2022). Themes in Data Mining, Big Data, and Crime Analytics. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(2), 1432. https://doi.org/10.1002/widm.1432

Radu, R. (2025). Countering Ransomware: Government Responses in a Comparative Perspective. *17th International Conference on Cyber Conflict: The Next Step (CyCon)*, 91–108. https://ora.ox.ac.uk/objects/uuid%3A86ff65a2-c5bb-4cba-be6b-c2683d90a0f9

Rajendra, J. B., & Thuraisingam, A. S. (2025). The Role of Explainability and Human Intervention in AI Decisions: Jurisdictional and Regulatory Aspects. *Information & Communications Technology Law*, 1–32. https://doi.org/10.1080/13600834.2025.2537514

Rawat, R., Garg, B., Mahor, V., Telang, S., Pachlasiya, K., & Chouhan, M. (2022). Organ Trafficking on the Dark Web-the Data Security and Privacy Concern in Healthcare Systems. In *Internet of Healthcare Things: Machine Learning for Security and Privacy* (pp. 191–216). Wiley. https://doi.org/10.1002/9781119792468.ch9

Sætra, H. S., Coeckelbergh, M., & Danaher, J. (2022). The AI Ethicist's Dilemma: Fighting Big Tech by Supporting Big Tech. *AI and Ethics*, *2*(1), 15–27. https://doi.org/10.1007/s43681-021-00123-7

Schaufelbühl, S., Florquin, N., Werner, D., & Delémont, O. (2024). The Emergence of 3D-Printed Firearms: An Analysis of Media and Law Enforcement Reports. *Forensic Science International: Synergy*, *8*, 100464. https://doi.org/10.1016/j.fsisyn.2024.100464

Scott, B. (2024). "Everyone Freaks Out When the Leaks Are Made": Data Leaks, Investigative Journalism and Intelligence Practice. *Journal of Financial Crime*, *31*(3), 545–557. https://doi.org/10.1108/jfc-05-2023-0123

Sitompul, F., Petrus, A., Manik, P., Sinaga, C. D., Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(2), 222–228. https://doi.org/10.51903/jaksa.v2i2.1668

Tuazon, O. M., Wickenheiser, R. A., Ansell, R., Guerrini, C. J., Zwenne, G. J., & Custers, B. (2024). Law Enforcement Use of Genetic Genealogy Databases in Criminal Investigations: Nomenclature, Definition and Scope. *Forensic Science International: Synergy*, *8*, 100460. https://doi.org/10.1016/j.fsisyn.2024.100460

Yu, L., Cong, Q., & Li, S. (2024). Study on International Cooperation to Address Cross-Border Telecommunication Network Fraud Offence. *Journal of Politics and Law*, *17*(2), 51. https://doi.org/10.5539/jpl.v17n2p51

Zafar, A. (2024). Balancing the Scale: Navigating Ethical and Practical Challenges of Artificial Intelligence (AI) Integration in Legal Practices. *Discover Artificial Intelligence*, *4*(1), 27. https://doi.org/10.1007/s44163-024-00121-8

Züger, T., & Asghari, H. (2023). AI for the Public. How Public Interest Theory Shifts the Discourse on AI. *AI and Society*, *38*(2), 815–828. https://doi.org/10.1007/s00146-022-01480-5