JAKSA
JURNAL KAJIAN ILMU HUKUM DAN POLITIK

LPPM Universitas Sains dan Teknologi Komputer
Vol. 4 No. 2 April 2026, Hal. 177-197
E-ISSN: 2988-5140; P-ISSN: 2988-7747
https: https://journal.stekom.ac.id/index.php/Jaksa/index

Transformasi Pola Kejahatan Siber Berbasis Kecerdasan Buatan dan Implikasinya terhadap Efektivitas Sistem Penegakan Hukum

Hendra Kurnia Wijaya*[1], Farhan Aditya Saputra[2]
[1]*Fakultas Hukum, Universitas Riau, Pekanbaru, E-mail: hendra.wijaya@gmail.com*
[2]*Fakultas Hukum, Universitas Riau, Pekanbaru, E-mail: farhan.saputra@gmail.com*

Article Info

Keywords:
AI Cybercrime
Law Enforcement
Digital Forensics
Technology Gap
Cybercrime Trends

Abstract

The rapid advancement of digital transformation has significantly reshaped the landscape of cybercrime, particularly through the integration of Artificial Intelligence (AI), which enhances the automation, scalability, and sophistication of cyber attacks. This study aims to analyze the transformation of AI-based cybercrime patterns and examine its implications for the effectiveness of law enforcement systems, especially in developing countries. A mixed-method approach with a sequential explanatory design was employed, combining quantitative analysis of global cybercrime datasets from 2018 to 2025 with qualitative insights from 25 experts, including law enforcement officers, cybersecurity analysts, and academics. The quantitative findings indicate that AI-driven phishing dominates cybercrime activities, reaching 35% in Asia and 32% in America, while deepfake fraud accounts for up to 30% in Europe. The average investigation time for AI-based cybercrime increased from 60 days in 2018 to 180 days in 2025, three times longer than traditional cases. Meanwhile, conviction rates declined significantly, from 65% to 50% in Europe and from 58% to 42% in Asia. The study also reveals a widening technological gap, with AI adoption among offenders rising to 80% compared to 45% among law enforcement agencies in 2025. These findings highlight that the growing complexity of AI-based cybercrime directly reduces the effectiveness of law enforcement due to limitations in digital forensic capacity, regulatory adaptation, and cross-border coordination. This study contributes by integrating technological transformation analysis with institutional performance evaluation, offering a comprehensive perspective on cybercrime and law enforcement dynamics in the AI era.

DOI: *https://doi.org/10.51903/thv32p80*
Submitted: January 2026, Reviewed: February 2026, Accepted: March 2026
**Corresponding Author*

Abstrak

Perkembangan pesat transformasi digital telah secara signifikan mengubah lanskap kejahatan siber, khususnya melalui integrasi AI yang meningkatkan otomatisasi, skalabilitas, dan kompleksitas serangan. Penelitian ini bertujuan untuk menganalisis transformasi pola kejahatan siber berbasis AI serta implikasinya terhadap efektivitas sistem penegakan hukum, terutama di negara berkembang. Penelitian ini menggunakan pendekatan metode campuran dengan desain *sequential explanatory*, yang menggabungkan analisis kuantitatif terhadap dataset kejahatan siber global periode 2018–2025 dengan wawancara kualitatif terhadap 25 pakar, termasuk aparat penegak hukum, analis keamanan siber, dan akademisi. Hasil penelitian menunjukkan bahwa *AI-driven phishing* mendominasi aktivitas kejahatan siber dengan proporsi mencapai 35% di Asia dan 32% di Amerika, sementara *deepfake fraud* mencapai hingga 30% di Eropa. Rata-rata waktu investigasi kejahatan siber berbasis AI meningkat dari 60 hari pada tahun 2018 menjadi 180 hari pada tahun 2025, atau tiga kali lebih lama dibandingkan kasus konvensional. Tingkat keberhasilan penuntutan juga mengalami penurunan signifikan, dari 65% menjadi 50% di Eropa dan dari 58% menjadi 42% di Asia. Selain itu, penelitian ini mengungkap adanya kesenjangan

teknologi yang semakin melebar, dengan tingkat adopsi AI oleh pelaku mencapai 80% dibandingkan 45% pada aparat penegak hukum pada tahun 2025. Temuan ini menunjukkan bahwa meningkatnya kompleksitas kejahatan siber berbasis AI secara langsung menurunkan efektivitas penegakan hukum akibat keterbatasan kapasitas forensik digital, adaptasi regulasi, dan koordinasi lintas yurisdiksi. Penelitian ini memberikan kontribusi dengan mengintegrasikan analisis transformasi teknologi dan evaluasi kinerja kelembagaan, sehingga menawarkan perspektif komprehensif mengenai dinamika kejahatan siber dan penegakan hukum di era AI.

Kata Kunci: *AI Cybercrime, Keamanan Siber, Penegakan Hukum, Bukti Digital, Kesenjangan Penegakan*

I. PENDAHULUAN

Perkembangan transformasi digital global dalam dua dekade terakhir telah mengubah hampir seluruh aspek kehidupan manusia, mulai dari ekonomi, komunikasi, hingga sistem pemerintahan. Di sisi lain, kemajuan teknologi tersebut juga membuka peluang baru bagi munculnya bentuk kejahatan yang lebih kompleks, terutama kejahatan siber. Laporan berbagai lembaga internasional menunjukkan bahwa nilai kerugian akibat kejahatan siber secara global terus meningkat setiap tahun dan diproyeksikan mencapai triliunan dolar dalam dekade ini. Perkembangan kecerdasan buatan (*Artificial Intelligence*/AI) semakin mempercepat evolusi tersebut dengan menghadirkan kemampuan otomatisasi, pembelajaran mandiri, dan analisis data dalam skala besar. Teknologi ini tidak hanya dimanfaatkan untuk kepentingan industri dan inovasi, tetapi juga disalahgunakan oleh pelaku kejahatan untuk meningkatkan efektivitas dan skalabilitas serangan siber. Contoh nyata dapat dilihat pada meningkatnya penggunaan *deepfake* untuk penipuan identitas serta pemanfaatan AI untuk menghasilkan *phishing* yang sangat personal dan sulit dideteksi. Kondisi ini menunjukkan bahwa kejahatan siber telah bertransformasi menjadi ancaman global yang adaptif, lintas negara, dan semakin sulit ditangani dengan pendekatan penegakan hukum konvensional.

Fenomena meningkatnya kompleksitas *cybercrime* juga berdampak langsung pada sistem hukum dan proses penegakan hukum di Indonesia. Pemanfaatan *information technology* oleh pelaku kejahatan telah memperluas ruang lingkup tindak pidana dari kejahatan konvensional menjadi kejahatan *digital* yang melibatkan jaringan global, *anonymity*, serta teknik *data manipulation* yang semakin canggih. Penelitian oleh (Sitompul et al., 2024; Tania & Gidalty, 2025) menunjukkan bahwa kejahatan *information technology* seperti *phishing*, pencurian data, dan pembobolan sistem *digital banking* terus meningkat, sementara mekanisme penanggulangan hukum masih menghadapi berbagai keterbatasan dalam implementasinya. Selain itu, kajian oleh (Syahrir & Saktiah, 2025) mengungkapkan bahwa efektivitas penegakan hukum terhadap pelaku *cybercrime* masih relatif rendah, yang tercermin dari lemahnya *deterrent effect* dan tingginya tingkat pengulangan kejahatan akibat sanksi yang belum optimal. Sementara itu, penelitian oleh (Laksito et al., 2024) menegaskan bahwa karakter *cross-border* dari kejahatan siber menimbulkan persoalan *jurisdiction* dan kerja sama internasional yang kompleks, sehingga negara membutuhkan kerangka hukum yang lebih adaptif dan selaras dengan standar global untuk dapat menanganinya secara efektif. Kondisi tersebut menunjukkan bahwa transformasi kejahatan

siber tidak hanya menjadi persoalan teknis, tetapi juga menimbulkan implikasi serius terhadap kesiapan regulasi, kelembagaan, dan efektivitas sistem penegakan hukum di Indonesia.

Sejumlah penelitian telah membahas bagaimana perkembangan teknologi digital dan AI mengubah karakteristik kejahatan siber modern. (Nankya et al., 2023) menjelaskan bahwa integrasi *machine learning* dalam sistem digital membuka peluang baru bagi pelaku untuk mengotomatisasi proses serangan dan meningkatkan efisiensi eksploitasi celah keamanan. Penelitian oleh (Alsulami, 2024) menggambarkan bagaimana teknik analisis data berbasis AI dapat digunakan tidak hanya untuk pertahanan siber, tetapi juga untuk merancang serangan yang lebih presisi dan sulit dideteksi. (Jørgensen & Ma, 2026) mengkaji pola jaringan pelaku kejahatan siber dan menemukan bahwa penggunaan teknologi cerdas mempercepat proses koordinasi dan distribusi serangan lintas negara. (Adeyeri & Abroshan, 2024) menyoroti implikasi etis dan keamanan dari penggunaan AI dalam ruang siber, termasuk potensi penyalahgunaan teknologi oleh aktor non-negara. (Abdullah et al., 2025) juga menunjukkan bahwa adopsi AI dalam ekosistem digital global berkontribusi terhadap meningkatnya kompleksitas dan skalabilitas kejahatan siber, terutama dalam konteks penipuan daring dan manipulasi informasi.

Penelitian lain secara khusus mengkaji transformasi modus operandi kejahatan siber akibat penerapan *deep learning* dan sistem otomatisasi. (Wilk-Jakubowski et al., 2025) menjelaskan bahwa pelaku kejahatan siber semakin mengandalkan alat otomatis untuk melakukan *phishing*, *credential stuffing*, dan serangan berbasis *botnet*. (Taherdoost, 2024) menguraikan perubahan struktur organisasi kejahatan siber yang menjadi lebih fleksibel dan berbasis jaringan digital, yang dipengaruhi oleh ketersediaan teknologi cerdas dan *dark web*. (Gonzaga et al., 2026) mendeskripsikan bahwa otomatisasi berbasis AI memungkinkan pelaku untuk menjalankan ribuan serangan secara simultan dengan tingkat personalisasi yang tinggi terhadap korban. (Skubis et al., 2024) mengkaji aspek keamanan manusia (*human-centric cybersecurity*) dan menunjukkan bahwa AI dimanfaatkan untuk meningkatkan efektivitas teknik *social engineering*. (Ali et al., 2025) menambahkan bahwa perkembangan teknologi digital tidak hanya memperluas jangkauan kejahatan siber, tetapi juga mengaburkan batas antara kejahatan konvensional dan kejahatan berbasis teknologi, sehingga menciptakan tantangan baru dalam identifikasi dan klasifikasi tindak pidana.

Selain itu, beberapa penelitian berfokus pada implikasi penggunaan AI terhadap sistem penegakan hukum dan kebijakan keamanan siber. (Papathanasiou et al., 2025) membahas bagaimana kerangka hukum yang ada sering kali tertinggal dibandingkan dengan kecepatan inovasi teknologi, sehingga menyulitkan proses penegakan hukum dalam kasus kejahatan siber. (Chango et al., 2024) meneliti dinamika hubungan antara inovasi teknologi dan regulasi, serta menggambarkan bahwa aparat penegak hukum membutuhkan kemampuan teknis yang setara dengan pelaku untuk melakukan investigasi digital secara efektif. (Bokolo & Liu, 2024) mengemukakan bahwa penggunaan AI dalam kejahatan siber meningkatkan volume data digital yang harus dianalisis dalam proses penyidikan, sehingga menuntut

pendekatan forensik yang lebih canggih. Studi oleh (Abomakhelb et al., 2025) menunjukkan bahwa AI telah dimanfaatkan untuk menghasilkan *deepfake*, otomatisasi *malware*, dan eksploitasi kerentanan sistem secara adaptif. (Udokwu et al., 2025) juga melaporkan bahwa aparat penegak hukum di berbagai negara mulai menghadapi kesulitan dalam melacak pelaku karena penggunaan teknologi anonimitas dan enkripsi yang dipadukan dengan AI.

Meskipun berbagai penelitian telah mengkaji transformasi kejahatan siber akibat perkembangan teknologi digital dan AI, sebagian besar studi masih berfokus pada aspek teknis serangan dan pengembangan sistem keamanan, bukan pada implikasinya terhadap sistem penegakan hukum. (Bouramdane, 2023) menunjukkan bahwa AI dapat meningkatkan skala dan kecepatan serangan siber, namun penelitian tersebut lebih menitikberatkan pada analisis risiko teknologi daripada dampaknya terhadap proses hukum. (Spyropoulos et al., 2023) membahas teknik analisis keamanan berbasis data, tetapi tidak secara spesifik mengevaluasi bagaimana teknologi tersebut memengaruhi mekanisme pembuktian dalam peradilan pidana. (Mushtaq & Shah, 2024) mengkaji jaringan pelaku kejahatan siber dan dinamika komunitas digital, namun belum mengaitkan temuan tersebut dengan kapasitas investigasi aparat penegak hukum. (Adel, 2023) mengidentifikasi pergeseran pola kejahatan menuju otomatisasi dan penggunaan *toolkit* digital, tetapi penelitian tersebut belum mengkaji kesiapan institusi hukum dalam merespons perubahan tersebut. Demikian pula, (Lin, 2025) menyoroti aspek *human factor* dalam keamanan siber, namun tidak secara mendalam menelaah bagaimana faktor tersebut memengaruhi efektivitas penegakan hukum dalam konteks kejahatan berbasis AI.

Selain itu, penelitian yang secara khusus mengkaji kesenjangan antara kemampuan teknologi pelaku dan kapasitas lembaga penegak hukum masih terbatas, terutama dalam konteks negara berkembang. (Kassa et al., 2024) menjelaskan perubahan struktur kejahatan siber global, tetapi fokus penelitian tersebut lebih banyak pada aspek sosiologis daripada evaluasi sistem hukum. (Sadaf et al., 2023) membahas otomatisasi kejahatan siber dan peningkatan skala serangan, namun belum mengaitkan fenomena tersebut dengan penurunan tingkat keberhasilan penuntutan. (Varela Enríquez et al., 2025) menelaah kerangka hukum kejahatan siber, tetapi analisisnya belum mempertimbangkan perkembangan terbaru seperti penggunaan *deepfake* dan *generative AI* dalam tindak pidana. (Zhang & Li, 2023) menyoroti hubungan antara inovasi teknologi dan regulasi, namun belum mengkaji secara empiris dampaknya terhadap proses investigasi digital di lapangan. (Alshabibi et al., 2024) mengemukakan bahwa volume data digital dalam penyidikan meningkat secara signifikan, tetapi penelitian tersebut belum mengaitkan temuan tersebut dengan kebutuhan transformasi kelembagaan aparat penegak hukum. Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara komprehensif bagaimana transformasi pola kejahatan siber berbasis AI memengaruhi efektivitas sistem penegakan hukum, khususnya dalam konteks negara berkembang yang menghadapi keterbatasan sumber daya, kesiapan regulasi, dan kapasitas teknologi.

Berdasarkan uraian latar belakang dan kesenjangan penelitian yang telah dipaparkan, penelitian ini berfokus pada analisis transformasi pola kejahatan siber berbasis AI serta implikasinya terhadap efektivitas sistem penegakan hukum. Penelitian ini mengajukan pertanyaan mengenai perubahan modus operandi kejahatan siber akibat pemanfaatan AI dan pengaruhnya terhadap kemampuan aparat dalam deteksi, investigasi, dan pembuktian perkara. Hipotesis yang diajukan menyatakan bahwa semakin tinggi pemanfaatan teknologi AI oleh pelaku kejahatan, semakin meningkat kompleksitas investigasi dan semakin menurun efektivitas penegakan hukum. Kebaruan (*novelty*) penelitian ini terletak pada integrasi analisis perkembangan kejahatan siber dengan evaluasi kinerja sistem penegakan hukum dalam satu kerangka konseptual yang komprehensif. Penelitian ini menggunakan pendekatan *mixed-method* dengan menggabungkan analisis tren global, evaluasi kebijakan, serta perspektif praktisi untuk memperoleh gambaran yang holistik. Hasil penelitian diharapkan memberikan pemahaman mendalam serta rekomendasi strategis bagi pembaruan regulasi, peningkatan kapasitas institusi, dan penguatan penegakan hukum yang adaptif.

II. METODOLOGI PENELITIAN

A. Desain Penelitian

Penelitian ini menggunakan pendekatan *mixed-method* dengan desain *sequential explanatory*, yaitu metode penelitian yang menggabungkan analisis kuantitatif dan kualitatif secara berurutan dalam satu kerangka penelitian yang terintegrasi. Pendekatan ini dipilih karena memungkinkan peneliti untuk mengidentifikasi pola empiris melalui data kuantitatif sekaligus memperoleh pemahaman kontekstual yang lebih mendalam melalui analisis kualitatif. Tahap pertama dalam penelitian ini adalah analisis kuantitatif yang bertujuan untuk mengidentifikasi tren global dan karakteristik transformasi kejahatan siber berbasis AI dalam kurun waktu tertentu. Analisis tersebut mencakup identifikasi pola pertumbuhan insiden, distribusi geografis, serta kompleksitas teknik serangan yang digunakan oleh pelaku kejahatan siber. Tahap kedua adalah eksplorasi kualitatif yang dilakukan untuk memperdalam interpretasi terhadap temuan kuantitatif melalui analisis kebijakan serta wawancara dengan praktisi yang memiliki pengalaman dalam penegakan hukum terhadap kejahatan siber. Pendekatan ini memberikan ruang untuk memahami fenomena secara komprehensif karena data numerik dan data naratif saling melengkapi dalam menjelaskan dinamika transformasi kejahatan siber berbasis teknologi cerdas.

B. Sumber dan Jenis Data

Penelitian ini memanfaatkan dua jenis data utama, yaitu data kuantitatif dan data kualitatif, yang diperoleh dari berbagai sumber untuk menggambarkan fenomena kejahatan siber secara komprehensif. Data kuantitatif diperoleh dari laporan global mengenai kejahatan siber yang dipublikasikan oleh organisasi internasional seperti *Europol*, *Interpol*, dan *United Nations Office on Drugs and Crime*. Selain itu, penelitian ini juga menggunakan database insiden kejahatan siber global yang mencakup periode 2018 hingga 2025 untuk mengidentifikasi perubahan tren serta perkembangan modus operandi

serangan berbasis AI. Data tersebut memberikan gambaran mengenai jumlah insiden, jenis serangan, serta distribusi regional dari kejahatan siber yang dilaporkan secara internasional. Sementara itu, data kualitatif diperoleh melalui wawancara dengan 25 responden yang terdiri dari aparat penegak hukum, analis keamanan siber, serta akademisi yang memiliki keahlian di bidang hukum teknologi informasi. Penelitian ini juga memanfaatkan dokumen kebijakan nasional dan internasional yang berkaitan dengan regulasi kejahatan siber, perlindungan data, dan penggunaan teknologi digital dalam proses penegakan hukum. Kombinasi kedua jenis data ini memberikan dasar analisis yang lebih luas karena fenomena yang diteliti dapat dilihat dari perspektif statistik sekaligus perspektif kebijakan dan praktik lapangan.

C. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode yang saling melengkapi untuk memperoleh data yang relevan dan akurat. Salah satu metode yang digunakan adalah teknik *web scraping* untuk mengumpulkan dataset global mengenai insiden kejahatan siber dari berbagai portal data terbuka serta laporan lembaga internasional. Teknik ini memungkinkan peneliti memperoleh data dalam jumlah besar secara sistematis sehingga memudahkan proses analisis tren jangka panjang. Selain itu, penelitian ini juga menggunakan metode studi dokumen untuk menganalisis regulasi, kebijakan, dan laporan resmi yang berkaitan dengan kejahatan siber serta penerapan teknologi AI dalam sistem penegakan hukum. Dokumen yang dianalisis meliputi undang-undang, peraturan pemerintah, laporan kebijakan, serta dokumen kerja sama internasional yang berkaitan dengan keamanan siber. Pengumpulan data juga dilakukan melalui wawancara semi-terstruktur dengan responden yang memiliki pengalaman dalam investigasi atau penelitian mengenai kejahatan siber. Pendekatan semi-terstruktur memberikan kerangka pertanyaan yang sistematis sekaligus memberikan ruang bagi responden untuk menjelaskan pengalaman dan pandangannya secara lebih mendalam.

D. Teknik Analisis Kuantitatif

Analisis kuantitatif dalam penelitian ini dilakukan untuk mengidentifikasi pola perubahan dan perkembangan kejahatan siber berbasis AI secara longitudinal. Teknik analisis yang digunakan meliputi analisis tren untuk melihat perubahan jumlah insiden dan variasi jenis serangan dari tahun ke tahun. Selain itu, penelitian ini juga menggunakan model regresi linier dan eksponensial untuk menggambarkan laju pertumbuhan kejahatan siber serta mengidentifikasi kemungkinan peningkatan kompleksitas serangan di masa mendatang. Pendekatan ini memberikan gambaran mengenai hubungan antara perkembangan teknologi digital dengan peningkatan aktivitas kejahatan siber secara global. Penelitian ini juga mengembangkan indeks risiko kejahatan siber berbasis komposit yang dibangun dari beberapa indikator seperti jumlah insiden, tingkat kerugian ekonomi, serta tingkat kompleksitas teknik serangan. Indeks tersebut digunakan untuk membandingkan tingkat risiko kejahatan siber antar wilayah dan untuk memahami distribusi ancaman secara global. Hasil analisis kuantitatif tersebut menjadi dasar untuk memahami kecenderungan transformasi kejahatan siber yang kemudian dijelaskan lebih lanjut melalui analisis kualitatif.

E. Teknik Analisis Kualitatif

Analisis kualitatif dilakukan untuk memahami faktor-faktor yang memengaruhi transformasi kejahatan siber serta implikasinya terhadap sistem penegakan hukum. Data kualitatif yang diperoleh dari wawancara dan dokumen kebijakan dianalisis menggunakan pendekatan *thematic analysis*. Proses analisis dimulai dengan tahap *open coding* yang bertujuan untuk mengidentifikasi tema-tema awal yang muncul dari data penelitian. Tahap berikutnya adalah *axial coding* yang digunakan untuk mengelompokkan tema-tema tersebut ke dalam kategori yang lebih terstruktur seperti hambatan regulasi, keterbatasan teknologi, dan tantangan yurisdiksi dalam penegakan hukum kejahatan siber. Proses selanjutnya adalah *selective coding* yang dilakukan untuk mengintegrasikan berbagai kategori tersebut ke dalam kerangka konseptual mengenai kesenjangan antara perkembangan teknologi kejahatan dan kapasitas lembaga penegak hukum. Selain itu, penelitian ini juga menggunakan analisis konten terhadap dokumen kebijakan untuk menilai sejauh mana regulasi yang ada telah mengakomodasi perkembangan teknologi digital dan AI. Pendekatan analisis kualitatif ini memberikan pemahaman yang lebih mendalam mengenai dinamika kelembagaan dan kebijakan yang memengaruhi efektivitas penegakan hukum terhadap kejahatan siber.

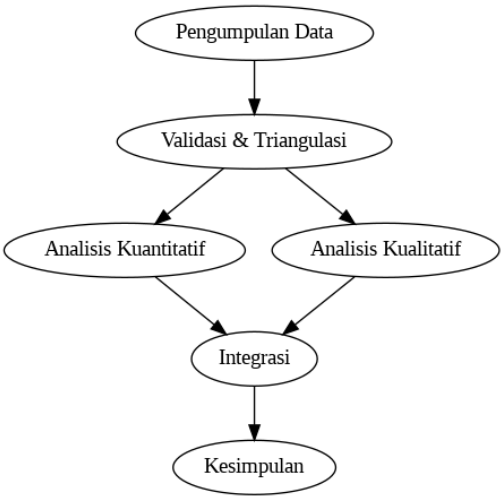
F. Validitas dan Reliabilitas

Validitas dan reliabilitas penelitian dijaga melalui beberapa prosedur yang dirancang untuk memastikan kualitas dan konsistensi data yang digunakan dalam analisis. Salah satu pendekatan yang digunakan adalah triangulasi data lintas sumber yang melibatkan perbandingan antara laporan global, *database* insiden, wawancara, dan dokumen kebijakan. Teknik ini memberikan kesempatan bagi peneliti untuk memeriksa kesesuaian informasi yang diperoleh dari berbagai sumber data yang berbeda. Proses analisis kualitatif juga melibatkan lebih dari satu peneliti untuk melakukan pengkodean terhadap sebagian data wawancara guna meningkatkan konsistensi interpretasi. Tingkat kesepakatan antar peneliti diukur menggunakan koefisien *intercoder reliability* dengan metode Cohen's Kappa. Nilai Cohen's Kappa sebesar 0,82 menunjukkan tingkat kesepakatan yang tinggi antara peneliti dalam proses pengkodean data. Selain itu, analisis kuantitatif juga diuji melalui uji *robustness* untuk memastikan bahwa model yang digunakan menghasilkan temuan yang konsisten meskipun terjadi variasi pada parameter analisis. Prosedur ini memberikan dasar metodologis yang kuat dalam memastikan bahwa hasil penelitian memiliki tingkat keandalan yang tinggi.

G. Kerangka Integrasi Data

Penelitian ini mengintegrasikan hasil analisis kuantitatif dan kualitatif melalui pendekatan *meta-inference* untuk memperoleh pemahaman yang lebih komprehensif mengenai fenomena yang diteliti. Proses integrasi dimulai dengan mengidentifikasi temuan utama dari analisis kuantitatif yang berkaitan dengan tren global dan distribusi kejahatan siber berbasis AI. Temuan tersebut kemudian dibandingkan dengan hasil analisis kualitatif yang berasal dari wawancara dan dokumen kebijakan untuk memahami

faktor-faktor yang memengaruhi pola yang ditemukan. Pendekatan ini memungkinkan peneliti untuk melihat hubungan antara data statistik dengan dinamika kebijakan dan praktik penegakan hukum. Integrasi data juga membantu menjelaskan mengapa beberapa wilayah atau institusi menghadapi tingkat kompleksitas investigasi yang lebih tinggi dibandingkan dengan yang lain. Proses integrasi dilakukan secara sistematis sehingga temuan dari kedua pendekatan tersebut dapat membentuk narasi analitis yang utuh. Alur tahapan penelitian yang digunakan dalam proses integrasi data tersebut dapat dilihat pada Gambar 1.



Gambar 1. Flowchart Desain Penelitian

Gambar 1 menggambarkan alur penelitian yang dimulai dari tahap pengumpulan data, kemudian dilanjutkan dengan proses validasi dan triangulasi untuk memastikan kualitas data yang digunakan dalam analisis. Setelah proses tersebut, data dianalisis melalui dua jalur utama yaitu analisis kuantitatif dan analisis kualitatif yang dilakukan secara paralel sesuai dengan desain *sequential explanatory*. Hasil dari kedua jenis analisis tersebut kemudian diintegrasikan dalam tahap integrasi data untuk menghasilkan interpretasi yang lebih komprehensif mengenai fenomena kejahatan siber berbasis AI. Tahap terakhir dalam alur penelitian adalah penarikan kesimpulan yang merangkum temuan utama penelitian dan menjelaskan implikasi terhadap sistem penegakan hukum. Visualisasi dalam gambar tersebut memberikan gambaran yang sistematis mengenai hubungan antar tahapan penelitian yang dilakukan dalam studi ini. Diagram alur ini juga membantu pembaca memahami proses metodologis penelitian secara lebih jelas dan terstruktur.

III. HASIL DAN PEMBAHASAN

Hasil

A. Transformasi Pola Kejahatan Siber Berbasis AI

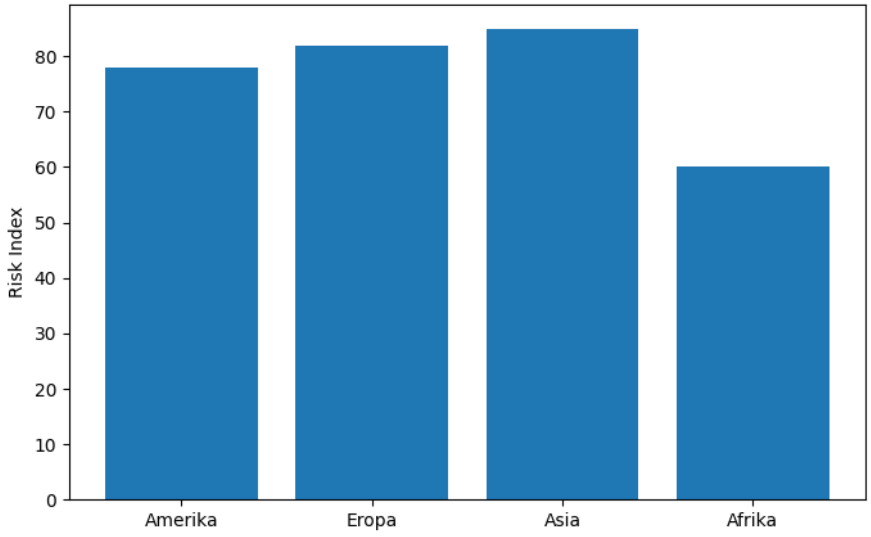
Perkembangan teknologi AI telah memengaruhi perubahan pola kejahatan siber secara signifikan dalam beberapa tahun terakhir. Integrasi AI dalam berbagai sistem digital memberikan peluang bagi pelaku kejahatan untuk mengotomatisasi proses serangan dan meningkatkan efisiensi operasional mereka. Teknik serangan yang sebelumnya membutuhkan keterlibatan manusia secara langsung kini dapat

dilakukan secara otomatis melalui algoritma pembelajaran mesin. Perubahan ini tidak hanya meningkatkan jumlah serangan, tetapi juga memperluas variasi metode yang digunakan dalam eksploitasi sistem dan manipulasi korban. Selain itu, kemampuan AI dalam menghasilkan konten yang menyerupai perilaku manusia meningkatkan keberhasilan serangan berbasis rekayasa sosial. Distribusi jenis kejahatan siber berbasis AI di berbagai wilayah pada tahun 2025 ditunjukkan pada Tabel 1.

Tabel 1. Distribusi Global Kejahatan Siber Berbasis AI (2025)

Jenis Kejahatan	Amerika	Eropa	Asia	Afrika
AI Phishing	32%	28%	35%	20%
Deepfake Fraud	25%	30%	22%	10%
AI Malware	28%	25%	30%	18%
Identity Automation	15%	17%	13%	12%

Tabel 1 memperlihatkan bahwa *AI phishing* merupakan jenis serangan yang paling dominan di hampir semua wilayah yang dianalisis. Wilayah Asia menunjukkan persentase tertinggi untuk jenis serangan ini, yang mencerminkan tingginya tingkat penggunaan layanan digital dan komunikasi daring di kawasan tersebut. Sementara itu, *deepfake fraud* memiliki tingkat kejadian yang relatif tinggi di Eropa dan Amerika, yang berkaitan dengan penggunaan identitas visual dalam berbagai aktivitas digital seperti perbankan dan konferensi daring. Serangan *AI malware* juga menunjukkan distribusi yang cukup merata, yang menggambarkan bahwa eksploitasi sistem berbasis perangkat lunak masih menjadi metode utama dalam kejahatan siber. Jenis serangan *identity automation* memiliki persentase yang lebih rendah dibandingkan jenis lainnya, namun tetap menunjukkan tren peningkatan yang stabil. Pola distribusi ini menggambarkan bahwa kejahatan siber berbasis AI berkembang dengan karakteristik yang berbeda di setiap wilayah sesuai dengan tingkat digitalisasi dan infrastruktur teknologi yang dimiliki.



Gambar 2. Indeks Risiko Kejahatan Siber Berbasis AI

Selain distribusi jenis kejahatan, penelitian ini juga mengukur tingkat risiko kejahatan siber berbasis AI di berbagai wilayah dengan menggunakan indeks komposit. Indeks ini dibangun dari beberapa indikator seperti frekuensi serangan, tingkat kerugian ekonomi, serta kompleksitas teknik yang digunakan oleh pelaku. Penggunaan indeks komposit memberikan gambaran yang lebih menyeluruh dibandingkan

dengan hanya melihat jumlah insiden secara terpisah. Nilai indeks kemudian dihitung untuk setiap wilayah dan digunakan untuk melakukan perbandingan tingkat ancaman secara global. Visualisasi nilai indeks risiko tersebut disajikan dalam bentuk grafik batang yang ditampilkan pada Gambar 2. Grafik ini digunakan untuk memperlihatkan perbedaan tingkat risiko secara visual antar wilayah.

Gambar 2 menunjukkan bahwa wilayah Asia memiliki nilai indeks risiko tertinggi dibandingkan wilayah lain yang dianalisis. Tingginya nilai ini berkaitan dengan kombinasi antara jumlah insiden yang besar, tingkat adopsi teknologi yang tinggi, serta luasnya populasi pengguna internet. Wilayah Eropa menempati posisi kedua dengan nilai indeks yang juga relatif tinggi, yang mencerminkan kompleksitas infrastruktur digital dan keterbukaan sistem informasi. Amerika menunjukkan nilai yang sedikit lebih rendah, yang berkaitan dengan keberadaan sistem keamanan siber yang lebih matang dan investasi besar dalam teknologi pertahanan digital. Wilayah Afrika memiliki nilai indeks yang lebih rendah dibandingkan wilayah lainnya, namun tren peningkatan tetap terlihat seiring dengan pertumbuhan penggunaan teknologi digital di kawasan tersebut. Visualisasi ini membantu memahami distribusi risiko secara komparatif dan memperlihatkan bahwa transformasi kejahatan siber berbasis AI tidak terjadi secara merata di seluruh dunia.

B. Kompleksitas Investigasi dan Dampaknya

Transformasi kejahatan siber berbasis AI juga berdampak langsung pada proses investigasi yang dilakukan oleh aparat penegak hukum. Penggunaan teknologi seperti enkripsi canggih, identitas digital yang dinamis, serta infrastruktur jaringan yang tersebar di berbagai negara menyebabkan proses pelacakan menjadi lebih sulit dilakukan. Selain itu, otomatisasi serangan memungkinkan pelaku untuk menjalankan berbagai aktivitas kejahatan secara bersamaan tanpa harus berada di lokasi yang sama dengan korban. Kondisi ini mengakibatkan meningkatnya jumlah bukti digital yang harus dianalisis dalam setiap kasus kejahatan siber. Aparat penegak hukum harus melakukan analisis forensik digital yang lebih mendalam untuk memastikan keabsahan dan keterkaitan bukti yang ditemukan. Perubahan kompleksitas tersebut dapat diamati melalui perbandingan rata-rata waktu penanganan kasus yang disajikan pada Tabel 2.

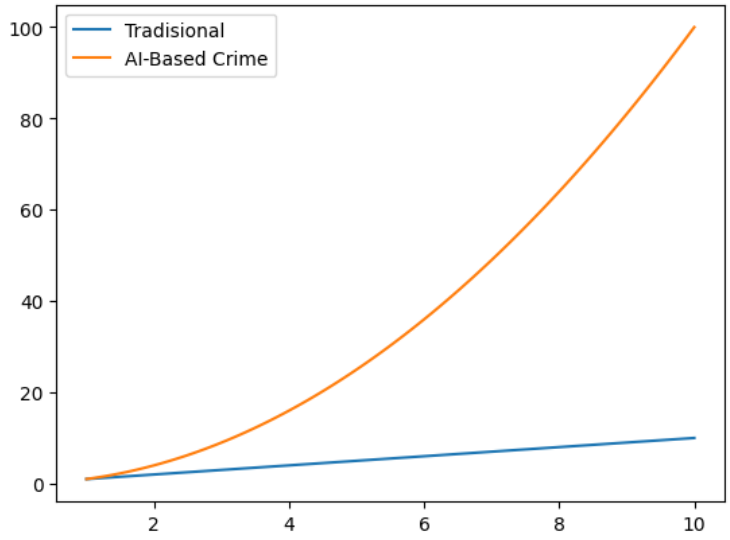
Tabel 2. Rata-rata Waktu Penanganan Kasus (hari)

Tahun	Tradisional	AI-Based
2018	45	60
2020	50	85
2022	55	120
2025	60	180

Tabel 2 menunjukkan bahwa waktu yang dibutuhkan untuk menyelesaikan kasus kejahatan siber berbasis AI meningkat secara signifikan dari tahun ke tahun. Pada awal periode pengamatan, perbedaan waktu antara kasus tradisional dan berbasis AI masih relatif kecil, namun selisih tersebut meningkat tajam pada tahun-tahun berikutnya. Pada tahun 2025, rata-rata waktu penanganan kasus berbasis AI mencapai tiga kali lipat dibandingkan dengan kasus tradisional. Peningkatan ini mencerminkan kompleksitas tambahan dalam proses pengumpulan bukti, analisis data, serta koordinasi lintas

yurisdiksi. Aparat penegak hukum juga menghadapi tantangan dalam memahami teknologi yang digunakan oleh pelaku, yang sering kali berkembang lebih cepat dibandingkan dengan kemampuan teknis institusi penegakan hukum. Data ini menggambarkan bahwa transformasi teknologi kejahatan siber berbanding lurus dengan meningkatnya beban investigasi yang harus ditangani oleh aparat.

Untuk memahami pola peningkatan kompleksitas tersebut, penelitian ini memodelkan hubungan antara waktu investigasi dan perkembangan teknologi kejahatan siber dalam bentuk grafik perbandingan antara pertumbuhan linear dan eksponensial. Pemodelan ini digunakan untuk menggambarkan bahwa peningkatan kompleksitas tidak selalu bersifat konstan, tetapi dapat meningkat secara drastis seiring dengan adopsi teknologi baru oleh pelaku. Grafik ini memberikan representasi visual mengenai perbedaan pola pertumbuhan kompleksitas antara kejahatan tradisional dan kejahatan berbasis AI. Kurva yang dihasilkan menunjukkan bahwa kompleksitas investigasi terhadap kejahatan berbasis AI memiliki kecenderungan meningkat lebih cepat dibandingkan dengan kejahatan tradisional. Visualisasi model tersebut ditampilkan pada Gambar 3.



Gambar 3. Kurva Kompleksitas Investigasi

Gambar 3 memperlihatkan perbedaan yang jelas antara pola pertumbuhan linear dan eksponensial dalam konteks kompleksitas investigasi. Kurva linear menggambarkan peningkatan kompleksitas yang stabil pada kejahatan siber tradisional, sedangkan kurva eksponensial menunjukkan peningkatan yang jauh lebih cepat pada kejahatan berbasis AI. Pola eksponensial ini berkaitan dengan penggunaan teknologi otomatisasi, algoritma pembelajaran mesin, serta teknik penyamaran identitas yang terus berkembang. Setiap peningkatan kecil dalam kemampuan teknologi pelaku dapat menghasilkan lonjakan besar dalam kesulitan investigasi yang dihadapi aparat penegak hukum. Visualisasi ini membantu menggambarkan secara konseptual bagaimana transformasi teknologi memengaruhi dinamika penanganan kasus kejahatan siber. Grafik tersebut juga memberikan dasar untuk memahami mengapa institusi penegakan hukum memerlukan peningkatan kapasitas teknologi dan sumber daya manusia dalam menghadapi perkembangan kejahatan berbasis AI.

C. *Efektivitas Penegakan Hukum*

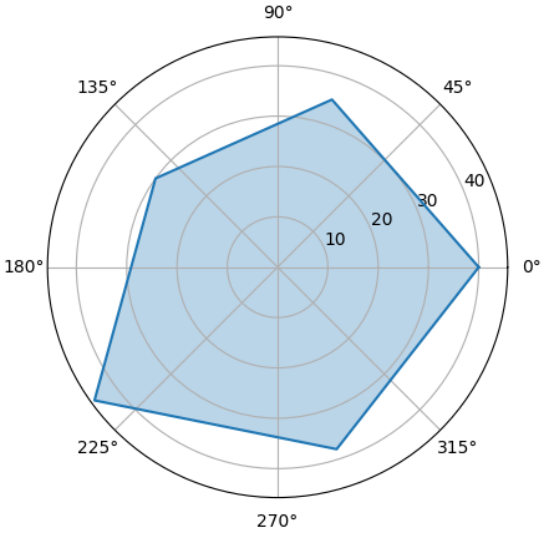
Efektivitas penegakan hukum dalam menangani kejahatan siber berbasis AI menjadi indikator penting dalam menilai kesiapan sistem peradilan menghadapi transformasi digital. Peningkatan kompleksitas teknik kejahatan menyebabkan proses pembuktian di pengadilan menjadi semakin sulit dilakukan oleh aparat penegak hukum. Selain itu, karakteristik kejahatan siber yang bersifat anonim dan lintas batas negara menambah tantangan dalam proses identifikasi pelaku. Sistem hukum yang pada awalnya dirancang untuk menangani kejahatan konvensional sering kali belum sepenuhnya mampu mengakomodasi dinamika kejahatan berbasis teknologi tinggi. Kondisi ini berdampak langsung pada menurunnya tingkat keberhasilan penuntutan kasus kejahatan siber. Perbandingan tingkat *conviction rate* di beberapa wilayah pada periode 2018 dan 2025 ditampilkan pada Tabel 3.

Tabel 3. Tingkat Conviction Rate (%)

Wilayah	2018	2025
Amerika	62	48
Eropa	65	50
Asia	58	42

Tabel 3 menunjukkan adanya tren penurunan tingkat *conviction rate* di seluruh wilayah yang dianalisis dalam rentang waktu tujuh tahun. Wilayah Eropa yang sebelumnya memiliki tingkat keberhasilan penuntutan tertinggi mengalami penurunan yang cukup signifikan pada tahun 2025. Asia menunjukkan penurunan yang lebih tajam dibandingkan wilayah lainnya, yang mencerminkan tantangan dalam pembuktian kasus kejahatan siber yang semakin kompleks. Amerika juga mengalami penurunan meskipun tetap berada pada tingkat yang relatif lebih tinggi dibandingkan wilayah lain. Penurunan tingkat keberhasilan penuntutan ini berkaitan dengan kesulitan dalam menghadirkan bukti digital yang memenuhi standar pembuktian di pengadilan. Data ini menggambarkan bahwa perkembangan teknologi kejahatan tidak diikuti secara seimbang oleh peningkatan kemampuan sistem hukum dalam memproses dan memutus perkara.

Selain melihat tingkat keberhasilan penuntutan, penelitian ini juga menganalisis kesenjangan kapasitas penegakan hukum pada berbagai aspek operasional. Aspek yang dianalisis meliputi kemampuan deteksi awal, kapasitas investigasi, kesiapan forensik digital, kelengkapan regulasi, serta kompetensi sumber daya manusia. Penilaian terhadap setiap aspek dilakukan untuk mengidentifikasi area yang paling membutuhkan penguatan dalam menghadapi kejahatan berbasis AI. Hasil penilaian kemudian divisualisasikan dalam bentuk grafik radar agar perbandingan antar aspek dapat terlihat secara jelas. Visualisasi ini memberikan gambaran menyeluruh mengenai posisi relatif setiap komponen dalam sistem penegakan hukum. Grafik kesenjangan kapasitas penegakan hukum ditampilkan pada Gambar 4.



Gambar 4. Kesenjangan Kapasitas Penegakan Hukum

Gambar 4 memperlihatkan bahwa aspek forensik digital memiliki skor kesiapan paling rendah dibandingkan aspek lainnya dalam sistem penegakan hukum. Keterbatasan ini berkaitan dengan kurangnya tenaga ahli, perangkat lunak analisis, serta standar prosedur operasional yang spesifik untuk menangani bukti berbasis AI. Aspek investigasi dan sumber daya manusia juga menunjukkan nilai yang relatif rendah, yang menggambarkan perlunya peningkatan pelatihan dan spesialisasi dalam bidang kejahatan siber. Regulasi memiliki skor yang sedikit lebih tinggi, namun masih belum sepenuhnya mampu mengakomodasi perkembangan teknik kejahatan yang sangat cepat. Visualisasi ini menunjukkan bahwa kesenjangan kapasitas tidak hanya terjadi pada aspek teknologi, tetapi juga pada aspek kelembagaan dan kompetensi personel. Grafik ini memberikan gambaran bahwa peningkatan efektivitas penegakan hukum memerlukan pendekatan yang komprehensif dan terintegrasi.

D. Kesenjangan Adopsi Teknologi

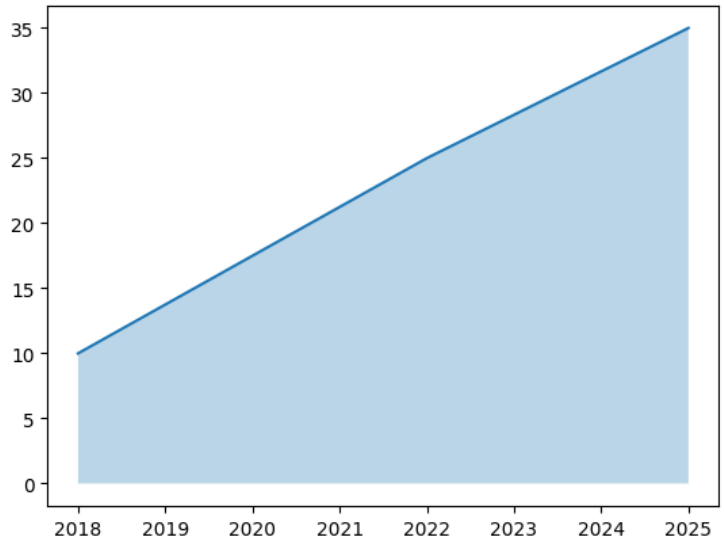
Pemanfaatan teknologi AI dalam kejahatan siber menunjukkan adanya perlombaan teknologi antara pelaku kejahatan dan aparat penegak hukum. Pelaku kejahatan cenderung lebih fleksibel dalam mengadopsi teknologi baru karena tidak terikat oleh prosedur administratif dan regulasi yang ketat. Sebaliknya, institusi penegakan hukum harus melalui proses pengadaan, evaluasi, serta pelatihan yang membutuhkan waktu relatif lama sebelum teknologi baru dapat digunakan secara operasional. Perbedaan kecepatan adopsi ini menciptakan kesenjangan kemampuan teknologi yang memengaruhi efektivitas deteksi dan investigasi. Kesenjangan tersebut semakin terlihat seiring dengan meningkatnya kompleksitas alat dan teknik yang digunakan dalam kejahatan siber berbasis AI. Perbandingan tingkat adopsi teknologi antara pelaku dan aparat ditampilkan pada Tabel 4.

Tabel 4. Tingkat Adopsi AI

Tahun	Pelaku	Aparat
2018	20%	10%
2022	55%	30%
2025	80%	45%

Tabel 4 menunjukkan bahwa tingkat adopsi AI oleh pelaku kejahatan meningkat secara signifikan dalam kurun waktu tujuh tahun. Pada tahun 2025, mayoritas pelaku kejahatan siber telah memanfaatkan AI untuk meningkatkan efektivitas dan jangkauan serangan mereka. Sementara itu, tingkat adopsi teknologi pada aparat penegak hukum juga mengalami peningkatan, namun dengan laju yang lebih lambat. Selisih yang cukup besar antara kedua pihak menunjukkan bahwa aparat masih berada pada posisi yang tertinggal dalam hal pemanfaatan teknologi mutakhir. Kesenjangan ini berdampak pada kemampuan aparat dalam mendeteksi serangan yang semakin kompleks dan tersamarkan. Data ini memperlihatkan bahwa adopsi teknologi menjadi faktor strategis dalam menentukan keseimbangan kekuatan antara pelaku kejahatan dan penegak hukum.

Untuk memberikan gambaran mengenai perkembangan kesenjangan teknologi dari waktu ke waktu, penelitian ini menyajikan grafik tren selisih tingkat adopsi AI antara pelaku dan aparat. Grafik ini digunakan untuk memperlihatkan perubahan selisih kemampuan teknologi secara kronologis sehingga pola peningkatannya dapat diamati dengan lebih jelas. Visualisasi tren ini membantu memahami bahwa kesenjangan teknologi bukan hanya terjadi pada satu titik waktu, tetapi berkembang secara bertahap dalam jangka panjang. Selain itu, grafik tersebut memberikan konteks empiris terhadap data pada tabel sebelumnya yang hanya menampilkan angka per tahun tanpa menunjukkan arah perubahannya. Penyajian dalam bentuk grafik juga memudahkan pembaca untuk mengidentifikasi periode di mana kesenjangan mengalami peningkatan paling tajam. Grafik kesenjangan teknologi tersebut ditampilkan pada Gambar 5.



Gambar 5. Kesenjangan Teknologi

Gambar 5 memperlihatkan bahwa kesenjangan adopsi teknologi antara pelaku dan aparat meningkat secara konsisten dari tahun ke tahun. Pada tahun 2018, selisih adopsi masih berada pada tingkat yang relatif rendah, namun meningkat lebih dari tiga kali lipat pada tahun 2025. Peningkatan kesenjangan ini mencerminkan bahwa pelaku kejahatan mampu mengintegrasikan teknologi baru ke dalam operasi mereka dengan lebih cepat dibandingkan aparat. Kondisi ini menyebabkan aparat sering berada pada posisi reaktif dalam menangani serangan yang sudah menggunakan teknologi mutakhir. Grafik ini juga

menggambarkan bahwa upaya modernisasi teknologi dalam institusi penegakan hukum memerlukan strategi yang berkelanjutan dan investasi jangka panjang. Visualisasi tren ini memperjelas bahwa kesenjangan teknologi menjadi salah satu tantangan utama dalam upaya pemberantasan kejahatan siber berbasis AI.

E. Faktor Hambatan Struktural

Selain aspek teknologi dan kapasitas investigasi, terdapat berbagai faktor struktural yang turut memengaruhi efektivitas penegakan hukum terhadap kejahatan siber berbasis AI. Hambatan struktural ini berkaitan dengan kerangka regulasi, koordinasi antar lembaga, serta mekanisme kerja sama internasional yang sering kali belum berjalan secara optimal. Kejahatan siber yang bersifat lintas negara menyebabkan proses penegakan hukum harus melibatkan berbagai yurisdiksi dengan sistem hukum yang berbeda. Perbedaan standar pembuktian, prosedur ekstradisi, serta mekanisme pertukaran data menjadi tantangan tambahan dalam proses investigasi dan penuntutan. Selain itu, proses legislasi yang cenderung lambat membuat regulasi sering kali tertinggal dibandingkan perkembangan teknologi yang sangat cepat. Penilaian terhadap faktor-faktor hambatan tersebut disajikan secara kuantitatif pada Tabel 5.

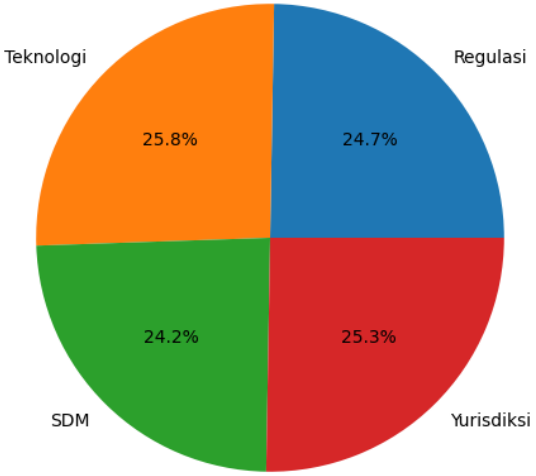
Tabel 5. Faktor Hambatan Penegakan Hukum

Faktor	Skor
Regulasi lambat	4.6
Teknologi tertinggal	4.8
SDM terbatas	4.5
Yurisdiksi lintas negara	4.7

Tabel 5 menunjukkan bahwa hambatan terbesar berasal dari faktor teknologi yang tertinggal, yang memiliki skor tertinggi dibandingkan faktor lainnya. Kondisi ini menggambarkan bahwa keterbatasan perangkat analisis dan sistem pendukung investigasi menjadi kendala utama dalam menangani kejahatan siber berbasis AI. Faktor yurisdiksi lintas negara juga memiliki skor yang tinggi, yang menunjukkan kompleksitas koordinasi internasional dalam proses penyidikan dan penuntutan. Regulasi yang lambat menyesuaikan diri dengan perkembangan teknologi turut menjadi hambatan karena banyak teknik kejahatan baru belum memiliki landasan hukum yang spesifik. Keterbatasan sumber daya manusia dengan kompetensi di bidang forensik digital dan AI juga berkontribusi terhadap rendahnya efektivitas penegakan hukum. Data ini memperlihatkan bahwa hambatan yang dihadapi bersifat multidimensional dan saling berkaitan satu sama lain.

Untuk memperjelas kontribusi relatif dari masing-masing faktor hambatan terhadap keseluruhan kendala penegakan hukum, penelitian ini menyajikan visualisasi dalam bentuk diagram lingkaran. Visualisasi ini digunakan untuk menunjukkan proporsi setiap faktor sehingga pembaca dapat memahami faktor mana yang memiliki pengaruh paling dominan. Penyajian dalam bentuk diagram juga membantu dalam membandingkan kontribusi antar faktor secara lebih intuitif dibandingkan dengan hanya melihat angka pada tabel. Diagram tersebut memungkinkan identifikasi prioritas kebijakan yang perlu

difokuskan dalam upaya peningkatan kapasitas penegakan hukum. Grafik kontribusi relatif hambatan penegakan hukum ditampilkan pada Gambar 6.



Gambar 6. Kontribusi Relatif Hambatan

Gambar 6 memperlihatkan bahwa faktor teknologi dan yurisdiksi lintas negara memberikan kontribusi terbesar terhadap keseluruhan hambatan yang dihadapi dalam penegakan hukum. Proporsi kedua faktor tersebut terlihat lebih besar dibandingkan faktor regulasi dan sumber daya manusia, yang menunjukkan bahwa tantangan utama tidak hanya berasal dari aspek internal kelembagaan. Faktor teknologi berkaitan dengan keterbatasan perangkat lunak analisis, infrastruktur digital, serta akses terhadap alat forensik yang mutakhir. Sementara itu, faktor yurisdiksi mencerminkan kompleksitas koordinasi internasional dalam menangani kejahatan siber yang melibatkan pelaku dan korban di berbagai negara. Visualisasi ini membantu menggambarkan bagaimana berbagai hambatan tersebut berinteraksi dan membentuk tantangan sistemik dalam penegakan hukum. Diagram ini memberikan gambaran proporsional yang memperkuat temuan kuantitatif yang sebelumnya disajikan dalam tabel.

F. Proyeksi Masa Depan Penegakan Hukum

Perkembangan teknologi AI diperkirakan akan terus memengaruhi dinamika kejahatan siber dan strategi penegakan hukum di masa depan. Institusi penegakan hukum di berbagai negara mulai mengembangkan sistem forensik berbasis AI, mekanisme deteksi otomatis, serta kerangka regulasi yang lebih adaptif terhadap perkembangan teknologi. Upaya peningkatan kerja sama internasional juga menjadi fokus utama dalam menghadapi kejahatan siber yang bersifat lintas batas dan terorganisasi. Meskipun demikian, tingkat kesiapan setiap komponen penegakan hukum tidak berkembang secara merata, sehingga diperlukan pemetaan terhadap area yang telah siap dan yang masih memerlukan penguatan. Penelitian ini melakukan proyeksi terhadap tingkat kesiapan beberapa komponen utama penegakan hukum hingga tahun 2030. Hasil proyeksi tersebut ditampilkan pada Tabel 6.

Tabel 6. Proyeksi Adaptasi Penegakan Hukum Tahun 2030

Komponen	Tingkat Kesiapan
AI Forensik	Tinggi
Regulasi adaptif	Sedang
Kerja sama internasional	Tinggi

Tabel 6 menunjukkan bahwa komponen forensik berbasis AI diproyeksikan mencapai tingkat kesiapan yang tinggi pada tahun 2030. Hal ini berkaitan dengan meningkatnya investasi pemerintah dan lembaga penegak hukum dalam pengembangan teknologi analisis bukti digital yang lebih canggih. Kerja sama internasional juga diperkirakan berada pada tingkat kesiapan tinggi karena meningkatnya kesadaran global mengenai ancaman kejahatan siber lintas negara. Sementara itu, regulasi adaptif masih berada pada tingkat kesiapan sedang, yang menunjukkan bahwa proses pembentukan hukum cenderung lebih lambat dibandingkan perkembangan teknologi. Perbedaan tingkat kesiapan antar komponen ini menunjukkan bahwa transformasi sistem penegakan hukum tidak terjadi secara seragam. Data proyeksi ini memberikan gambaran mengenai arah perkembangan kapasitas penegakan hukum dalam menghadapi kejahatan siber berbasis AI di masa mendatang.

Pembahasan

Hasil penelitian ini menunjukkan bahwa transformasi kejahatan siber berbasis AI secara signifikan meningkatkan kompleksitas serangan serta menurunkan efektivitas sistem penegakan hukum. Peningkatan dominasi *AI phishing* dan *deepfake fraud* mencerminkan bahwa teknologi cerdas telah memperkuat efektivitas teknik *social engineering* dalam skala global. Waktu penanganan kasus yang meningkat secara drastis menunjukkan adanya beban investigasi yang semakin kompleks bagi aparat penegak hukum. Penurunan *conviction rate* di berbagai wilayah mengindikasikan bahwa sistem pembuktian hukum belum sepenuhnya mampu mengimbangi kompleksitas bukti digital berbasis AI. Kondisi ini menggambarkan adanya ketidakseimbangan antara perkembangan teknologi kejahatan dan kapasitas institusi hukum. Perubahan tersebut memperlihatkan bahwa evolusi teknologi tidak hanya memengaruhi pola kejahatan, tetapi juga mengubah dinamika operasional penegakan hukum secara mendasar.

Temuan penelitian ini memperkuat hasil studi sebelumnya yang menyatakan bahwa integrasi *machine learning* dan otomatisasi meningkatkan skalabilitas serta efisiensi serangan siber (Nankya et al., 2023). Peningkatan kompleksitas investigasi yang bersifat eksponensial juga sejalan dengan temuan (Bokolo & Liu, 2024) mengenai meningkatnya volume data digital dalam proses forensik. Selain itu, kondisi keterlambatan regulasi dalam merespons inovasi teknologi konsisten dengan kajian (Papathanasiou et al., 2025). Hubungan antara kesenjangan adopsi teknologi dan penurunan efektivitas penegakan hukum memperluas temuan (Chango et al., 2024) yang menyoroti kebutuhan peningkatan kapasitas teknis aparat. Penelitian ini juga menunjukkan keterkaitan yang lebih eksplisit antara tingkat adopsi AI oleh pelaku dan penurunan keberhasilan penuntutan. Keterkaitan tersebut memperkaya literatur dengan memberikan gambaran empiris mengenai dampak langsung teknologi terhadap sistem hukum.

Beberapa hasil penelitian menunjukkan adanya dinamika yang tidak sepenuhnya sejalan dengan ekspektasi awal maupun temuan sebelumnya. Tingkat risiko kejahatan siber yang lebih tinggi pada wilayah dengan pertumbuhan pengguna digital yang pesat menunjukkan bahwa intensitas penggunaan teknologi memiliki pengaruh yang signifikan terhadap tingkat kerentanan. Peningkatan kompleksitas

investigasi yang berlangsung secara eksponensial menunjukkan bahwa dampak teknologi AI terhadap proses hukum berkembang lebih cepat dibandingkan dengan prediksi dalam penelitian terdahulu (Sadaf et al., 2023). Fenomena ini juga menggambarkan adanya *lag effect* antara kemampuan pelaku dalam mengadopsi teknologi dan kesiapan institusi penegak hukum dalam meresponsnya. Kesiapan regulasi yang relatif lebih baik dibandingkan aspek teknis menunjukkan adanya ketimpangan antara kerangka normatif dan kapasitas implementasi di lapangan. Perbedaan ini mengindikasikan bahwa keberadaan regulasi tidak secara otomatis menjamin efektivitas penegakan hukum. Variasi antar aspek tersebut memperlihatkan kompleksitas hubungan antara teknologi, kebijakan, dan praktik penegakan hukum.

Secara teoritis, penelitian ini memberikan kontribusi dalam memperjelas hubungan antara transformasi teknologi dan perubahan efektivitas sistem hukum dalam konteks kejahatan siber berbasis AI. Secara praktis, hasil penelitian menunjukkan pentingnya penguatan kapasitas *digital forensics*, peningkatan investasi teknologi, serta optimalisasi kerja sama internasional dalam menangani kejahatan lintas yurisdiksi. Pendekatan penegakan hukum yang berbasis *proactive intelligence* juga menjadi semakin relevan dalam menghadapi dinamika kejahatan berbasis teknologi cerdas. Keterbatasan penelitian ini terletak pada penggunaan data global yang belum sepenuhnya mencerminkan kondisi spesifik pada setiap negara berkembang. Selain itu, penggunaan indeks komposit dalam pengukuran risiko berpotensi menyederhanakan kompleksitas variabel yang ada. Keterbatasan tersebut menunjukkan bahwa interpretasi hasil perlu mempertimbangkan konteks dan ruang lingkup data yang digunakan.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa transformasi kejahatan siber berbasis AI telah mengubah pola serangan menjadi lebih kompleks, adaptif, dan sulit dideteksi oleh sistem konvensional. Peningkatan penggunaan AI oleh pelaku kejahatan berkontribusi pada meningkatnya efektivitas serangan seperti *phishing* dan *deepfake*, yang berdampak langsung pada meningkatnya kerentanan sistem digital. Kompleksitas investigasi juga mengalami peningkatan signifikan yang tercermin dari bertambahnya waktu penanganan kasus serta meningkatnya volume dan kerumitan bukti digital. Penurunan tingkat keberhasilan penuntutan menunjukkan bahwa sistem pembuktian hukum belum sepenuhnya mampu mengimbangi perkembangan teknologi kejahatan. Kesenjangan adopsi teknologi antara pelaku dan aparat penegak hukum memperlihatkan adanya ketidakseimbangan kapasitas yang memengaruhi efektivitas penegakan hukum secara keseluruhan. Temuan ini memperjelas bahwa transformasi kejahatan siber berbasis AI memiliki implikasi sistemik terhadap aspek teknis, kelembagaan, dan regulasi dalam sistem penegakan hukum.

Penelitian selanjutnya disarankan untuk mengembangkan pendekatan yang lebih spesifik dalam menganalisis dampak kejahatan siber berbasis AI pada konteks regional atau negara tertentu. Penggunaan data primer berbasis studi kasus dapat memberikan pemahaman yang lebih mendalam mengenai dinamika investigasi dan proses pembuktian di lapangan. Pendekatan metodologis yang lebih eksploratif, seperti integrasi *big data analytics* dan pemodelan prediktif, dapat digunakan untuk

mengidentifikasi pola kejahatan yang lebih kompleks dan dinamis. Selain itu, penelitian lanjutan dapat mengkaji efektivitas implementasi teknologi AI dalam sistem penegakan hukum sebagai upaya untuk mengurangi kesenjangan kapasitas dengan pelaku kejahatan. Analisis terhadap aspek kebijakan dan regulasi juga perlu diperluas untuk memahami bagaimana kerangka hukum dapat beradaptasi secara lebih responsif terhadap perkembangan teknologi. Penguatan kolaborasi multidisiplin antara bidang teknologi, hukum, dan kebijakan publik menjadi penting untuk menghasilkan pendekatan yang lebih komprehensif dalam menghadapi kejahatan siber berbasis AI.

REFERENSI

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution Cybercrime Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, *4*(3), 25. https://doi.org/10.3390/analytics4030025

Abomakhelb, A., Jalil, K. A., Buja, A. G., Alhammadi, A., & Alenezi, A. M. (2025). A Comprehensive Review of Adversarial Attacks and Defense Strategies in Deep Neural Networks. *Technologies*, *13*(5), 202. https://doi.org/10.3390/technologies13050202

Adel, A. (2023). Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. *Smart Cities*, *6*(5), 2742–2782. https://doi.org/10.3390/smartcities6050124

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682. https://doi.org/10.3390/info15110682

Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. *Computers*, *14*(2), 38. https://doi.org/10.3390/computers14020038

Alshabibi, M. M., Bu dookhi, A. K., & Hafizur Rahman, M. M. (2024). Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. *Computers*, *13*(8), 213. https://doi.org/10.3390/computers13080213

Alsulami, M. H. (2024). An AI-Driven Model to Enhance Sustainability for the Detection of Cyber Threats in IoT Environments. *Sensors*, *24*(22), 7179. https://doi.org/10.3390/s24227179

Bokolo, B. G., & Liu, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. *Electronics*, *13*(9), 1671. https://doi.org/10.3390/electronics13091671

Bouramdane, A.-A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705. https://doi.org/10.3390/jcp3040031

Chango, X., Flor-Unda, O., Gil-Jiménez, P., & Gómez-Moreno, H. (2024). Technology in Forensic Sciences: Innovation and Precision. *Technologies*, *12*(8), 120. https://doi.org/10.3390/technologies12080120

Gonzaga, K., Serra, S., Gomes, M., & Malta, S. (2026). AI-Powered Social Engineering: Emerging

Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. *Computers*, *15*(2), 128. https://doi.org/10.3390/computers15020128

Jørgensen, B. N., & Ma, Z. G. (2026). Cybersecurity and Resilience of Smart Grids: A Review of Threat Landscape, Incidents, and Emerging Solutions. *Applied Sciences*, *16*(2), 981. https://doi.org/10.3390/app16020981

Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information*, *15*(5), 263. https://doi.org/10.3390/info15050263

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

Lin, L. S. F. (2025). Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. *Laws*, *14*(4), 46. https://doi.org/10.3390/laws14040046

Mushtaq, S., & Shah, M. (2024). Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information*, *15*(10), 619. https://doi.org/10.3390/info15100619

Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. *Sensors*, *23*(21), 8840. https://doi.org/10.3390/s23218840

Papathanasiou, A., Germanos, G., Liagkou, V., & Vlachos, V. (2025). Trends and Challenges in Cybercrime in Greece. *Journal of Cybersecurity and Privacy*, *5*(4), 81. https://doi.org/10.3390/jcp5040081

Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects. *Technologies*, *11*(5), 117. https://doi.org/10.3390/technologies11050117

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.v2i2.1666

Skubis, I., Wolniak, R., & Grebski, W. W. (2024). AI and Human-Centric Approach in Smart Cities Management: Case Studies from Silesian and Lesser Poland Voivodships. *Sustainability*, *16*(18), 8279. https://doi.org/10.3390/su16188279

Spyropoulos, A. Z., Bratsas, C., Makris, G. C., Garoufallou, E., & Tsiantos, V. (2023). Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis. *Information*, *14*(11), 607. https://doi.org/10.3390/info14110607

Syahrir, M., & Saktiah. (2025). Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis. *Perkara: Jurnal Ilmu Hukum Dan Politik*, *3*(1), 694–711. https://doi.org/10.51903/perkara.v3i1.2343

Taherdoost, H. (2024). Insights into Cybercrime Detection and Response: A Review of Time Factor. *Information*, *15*(5), 273. https://doi.org/10.3390/info15050273

Tania, C., & Gidalty, J. (2025). Strategi Penuntutan Kejahatan Siber dengan Artificial Intelligence di Era Digital. Hakim: Jurnal Ilmu Hukum Dan Sosial, 3(4), 1387–1401. https://doi.org/10.51903/J928TS68

Udokwu, C., Voicu-Dorobanțu, R., Ogunyemi, A. A., Norta, A., Sturua, N., & Craß, S. (2025). Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience. *Future Internet*, *17*(7), 309. https://doi.org/10.3390/fi17070309

Varela Enríquez, C., Toasa, R., & Urdaneta, M. (2025). The Use of Artificial Intelligence in Cybercrime: Impact Analysis in Ecuador and Mitigation Strategies. *Journal of Cybersecurity and Privacy*, *5*(4), 100. https://doi.org/10.3390/jcp5040100

Wilk-Jakubowski, J. L., Pawlik, L., Wilk-Jakubowski, G., & Sikora, A. (2025). Machine Learning and Neural Networks for Phishing Detection: A Systematic Review (2017–2024). *Electronics*, *14*(18), 3744. https://doi.org/10.3390/electronics14183744

Zhang, J., & Li, S. (2023). The Impact of Human Capital on Green Technology Innovation—Moderating Role of Environmental Regulations. *International Journal of Environmental Research and Public Health*, *20*(6), 4803. https://doi.org/10.3390/ijerph20064803