Sinar Dunia: Jurnal Riset Sosial Humaniora dan Ilmu Pendidikan
Volume 5, Nomor 2, Juni 2026
e-ISSN : 2963-542X; p-ISSN : 2963-4997, Hal 333-353
DOI: https://doi.org/10.58192/sidu.v5i2.4579
Tersedia: https://journal.unimaramni.ac.id/index.php/sidu

Tantangan Penegakan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia

Trisno Ariwibowo[1*], Ismaidar[2], Zulkifli Lubis[3], Edwin S. Pohan[4]
[1-4]Universitas Pembangunan Panca Budi, Indonesia
Email: trisno.ariwibowo63@gmail.com[1], ismaidar@dosen.pancabudi.ac.id[2], zulkiflilubis537@gmail.com[3], Pohanedwin@gmail.com[4]*
**Penulis Korespondensi: trisno.ariwibowo63@gmail.com*

Abstract. *The development of Artificial Intelligence (AI) has brought significant changes to various aspects of life; however, it has also increased the potential misuse of technology in cybercrime activities. The misuse of AI in the forms of deepfake, voice cloning, AI phishing, digital identity manipulation, and disinformation has created new challenges for law enforcement systems in Indonesia. This study aims to analyze the legal framework governing the misuse of Artificial Intelligence in cybercrime, identify the challenges faced in law enforcement, and examine efforts to optimize law enforcement in Indonesia. This research employs a normative juridical method using statutory, conceptual, and case approaches. The findings indicate that Indonesia's legal framework still relies on the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), and the Personal Data Protection Law, which do not specifically regulate AI misuse in cybercrime. The main law enforcement challenges include regulatory limitations, difficulties in digital evidence verification, limited law enforcement capacity, cross-border cybercrime jurisdiction, and low public digital literacy. Therefore, legal reform, strengthening law enforcement capacity, developing digital forensics, enhancing international cooperation, and increasing public digital education are necessary to improve the effectiveness of law enforcement against the misuse of Artificial Intelligence in cybercrime in Indonesia.*

Keywords: *Artificial Intelligence; Cyber Law; Cybercrime; Digital Forensics; Law Enforcement.*

Abstrak. Perkembangan *Artificial Intelligence* (AI) telah membawa perubahan signifikan dalam berbagai aspek kehidupan, namun di sisi lain juga meningkatkan potensi penyalahgunaan teknologi dalam tindak pidana siber (*cybercrime*). Penyalahgunaan AI dalam bentuk *deepfake*, *voice cloning*, *AI phishing*, manipulasi identitas digital, dan penyebaran informasi palsu menimbulkan tantangan baru dalam sistem penegakan hukum di Indonesia. Penelitian ini bertujuan untuk menganalisis pengaturan hukum terhadap penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber, mengidentifikasi tantangan penegakan hukum yang dihadapi, serta menganalisis upaya optimalisasi penegakan hukum di Indonesia. Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Hasil penelitian menunjukkan bahwa pengaturan hukum di Indonesia masih bergantung pada UU ITE, KUHP, dan UU Perlindungan Data Pribadi yang belum secara spesifik mengatur penyalahgunaan AI dalam tindak pidana siber. Tantangan utama penegakan hukum meliputi keterbatasan regulasi, kesulitan pembuktian alat bukti digital, keterbatasan kapasitas aparat penegak hukum, yurisdiksi lintas negara (*cross-border cybercrime*), serta rendahnya literasi digital masyarakat. Oleh karena itu, diperlukan reformasi regulasi hukum, penguatan kapasitas aparat, pengembangan *digital forensics*, peningkatan kerja sama internasional, serta edukasi digital masyarakat guna meningkatkan efektivitas penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber di Indonesia.

Kata Kunci: *Artificial Intelligence*; *Cybercrime*; *Digital Forensics*; Penegakan Hukum; Tindak Pidana Siber.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan signifikan terhadap berbagai aspek kehidupan masyarakat, termasuk dalam bidang ekonomi, pendidikan, pemerintahan, serta sistem transaksi digital. Kemajuan teknologi tersebut turut mendorong peningkatan penggunaan internet, kecerdasan buatan (*Artificial Intelligence* atau AI), big data, komputasi awan *(cloud computing)*, dan berbagai platform digital lainnya yang memberikan kemudahan dalam aktivitas sehari-hari. Namun, di sisi lain,

Naskah Masuk: 18 April 2026; Revisi:16 Mei 2026; Diterima: 21 Juni 2026; Terbit: 23 Juni 2026

perkembangan teknologi tersebut juga memunculkan berbagai bentuk ancaman baru, salah satunya adalah meningkatnya tindak pidana siber (*Cybercrime*) yang memanfaatkan kecanggihan teknologi digital sebagai sarana melakukan kejahatan (Yar, 2021).

Artificial Intelligence (AI) merupakan salah satu inovasi teknologi yang berkembang sangat pesat dalam beberapa tahun terakhir. AI memiliki kemampuan untuk meniru kecerdasan manusia melalui pemrosesan data, pembelajaran mesin *(machine learning)*, pengenalan pola, pemrosesan bahasa alami *(natural language processing)*, hingga kemampuan menghasilkan gambar, suara, video, dan teks secara otomatis. Dalam praktiknya, penggunaan AI memberikan manfaat besar bagi berbagai sektor, seperti kesehatan, pendidikan, keamanan, industri keuangan, dan administrasi publik. Akan tetapi, perkembangan tersebut juga membuka peluang terjadinya penyalahgunaan teknologi AI untuk melakukan tindak pidana siber (*National Institute of Standards and Technology* [NIST], 2024). Penyalahgunaan AI dalam tindak pidana siber dapat ditemukan dalam berbagai bentuk, seperti *deepfake*, pencurian identitas digital, *phishing* berbasis AI, *social engineering*, manipulasi data, penyebaran informasi palsu (*disinformation*), penipuan digital, hingga otomatisasi serangan siber (*automated cyber attacks*). Teknologi AI memungkinkan pelaku kejahatan untuk menciptakan modus operandi yang semakin kompleks, sulit dilacak, dan menyerupai perilaku manusia secara nyata, sehingga meningkatkan tingkat kesulitan aparat penegak hukum dalam mengidentifikasi pelaku maupun mengumpulkan alat bukti digital (Rosenoer, 2019).

Di Indonesia, peningkatan kasus tindak pidana siber menjadi tantangan serius dalam sistem penegakan hukum nasional. Kejahatan berbasis teknologi berkembang lebih cepat dibandingkan dengan kemampuan regulasi dan sistem hukum untuk menyesuaikan diri. Walaupun Indonesia telah memiliki regulasi seperti UU ITE, KUHP, serta UU Perlindungan Data Pribadi, pengaturan mengenai penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber masih belum diatur secara spesifik. Kondisi ini menimbulkan kekosongan norma (*legal vacuum*) yang dapat menghambat efektivitas proses penegakan hukum terhadap pelaku kejahatan siber berbasis AI (Sari & Nugroho, 2025).

2. KAJIAN TEORITIS

Teori Penegakan Hukum (*Law Enforcement Theory*)

Perkembangan AI telah memunculkan berbagai bentuk kejahatan siber baru, seperti *deepfake*, *voice cloning*, *AI phishing*, manipulasi identitas digital, dan penyebaran informasi palsu secara otomatis. Modus kejahatan tersebut menyebabkan tantangan serius bagi aparat

penegak hukum karena sulitnya identifikasi pelaku, anonimitas digital, serta kompleksitas alat bukti elektronik yang digunakan dalam pembuktian pidana (Anggraeny, 2026).

Selain itu, efektivitas penegakan hukum terhadap *Cybercrime* berbasis AI juga dipengaruhi oleh kemampuan aparat penegak hukum dalam memahami teknologi digital, tersedianya fasilitas digital forensik, dan kerja sama lintas negara (*cross-border law enforcement*). Hal ini menjadi penting karena karakteristik *cybercrime* bersifat lintas batas negara (*borderless crime*) dan sering kali melibatkan pelaku dari yurisdiksi berbeda (Hibatulloh, 2025).

Teori Kepastian Hukum (*Legal Certainty Theory*)

Teori kepastian hukum menjelaskan bahwa hukum harus mampu memberikan aturan yang jelas, konsisten, dan dapat diprediksi oleh masyarakat. Dalam perkembangan teknologi digital, kepastian hukum menjadi penting karena kemajuan teknologi sering kali lebih cepat dibanding perkembangan regulasi hukum. Kondisi tersebut berpotensi menimbulkan kekosongan hukum (*legal vacuum*) dalam mengatur bentuk-bentuk kejahatan baru berbasis teknologi, termasuk penyalahgunaan *Artificial Intelligence* (AI) (Afni, 2024).

Kepastian hukum menjadi elemen penting agar aparat penegak hukum memiliki dasar normatif yang jelas dalam menangani tindak pidana siber berbasis AI sekaligus memberikan perlindungan hukum kepada masyarakat dari ancaman penyalahgunaan teknologi digital (Anggraeny, 2026).

Teori Kebijakan Hukum Pidana (*Criminal Policy Theory*)

Teori kebijakan hukum pidana menekankan bahwa hukum pidana harus mampu berkembang mengikuti perubahan sosial dan kemajuan teknologi. Dalam era digital, hukum pidana tidak hanya berfungsi secara represif melalui pemberian sanksi, tetapi juga preventif melalui pembentukan regulasi yang adaptif terhadap bentuk-bentuk kejahatan baru (Dharmayanti, 2025).

Perkembangan *Artificial Intelligence* telah menciptakan tantangan baru dalam sistem hukum pidana karena teknologi ini dapat digunakan untuk melakukan kejahatan dengan cara yang lebih canggih, cepat, dan sulit dideteksi. Beberapa bentuk penyalahgunaan AI meliputi *deepfake fraud*, manipulasi suara, pencurian identitas digital, serta *automated phishing*. Kondisi tersebut menunjukkan perlunya reformulasi kebijakan hukum pidana yang mampu mengakomodasi perkembangan teknologi AI dalam ruang siber (Hibatulloh, 2025).

Teori Kepastian Hukum (*Legal Certainty Theory*)

Teori kepastian hukum menjelaskan bahwa hukum harus mampu memberikan aturan yang jelas, konsisten, dan dapat diprediksi oleh masyarakat. Dalam perkembangan teknologi

digital, kepastian hukum menjadi penting karena kemajuan teknologi sering kali lebih cepat dibanding perkembangan regulasi hukum. Kondisi tersebut berpotensi menimbulkan kekosongan hukum (*legal vacuum*) dalam mengatur bentuk-bentuk kejahatan baru berbasis teknologi, termasuk penyalahgunaan *Artificial Intelligence* (AI) (Afni, 2024).

Kepastian hukum menjadi elemen penting agar aparat penegak hukum memiliki dasar normatif yang jelas dalam menangani tindak pidana siber berbasis AI sekaligus memberikan perlindungan hukum kepada masyarakat dari ancaman penyalahgunaan teknologi digital (Anggraeny, 2026).

Teori *Digital Forensics*

Kemampuan *Artificial Intelligence* menghasilkan konten yang menyerupai realitas, seperti video *deepfake*, rekayasa suara (*voice cloning*), maupun identitas digital palsu menyebabkan proses pembuktian hukum menjadi lebih kompleks. Oleh karena itu, pendekatan digital forensik perlu diperkuat agar aparat penegak hukum mampu mendeteksi manipulasi digital serta memastikan validitas bukti elektronik di pengadilan (Zhang et al., 2022).

Konsep Tindak Pidana Siber (*Cybercrime*)

Tindak pidana siber (*cybercrime*) merupakan bentuk kejahatan yang memanfaatkan teknologi komputer, perangkat digital, dan jaringan internet sebagai sarana utama dalam melakukan tindakan melawan hukum. *Cybercrime* berkembang seiring dengan meningkatnya digitalisasi dalam berbagai aspek kehidupan masyarakat, termasuk sektor ekonomi, pendidikan, pemerintahan, dan transaksi elektronik. Menurut *Cybercrime and Society*, *cybercrime* adalah bentuk kriminalitas yang dilakukan melalui teknologi digital dengan memanfaatkan kelemahan sistem informasi, jaringan internet, maupun perilaku pengguna teknologi (Yar, 2021).

Cybercrime memiliki karakteristik berbeda dibandingkan kejahatan konvensional karena bersifat lintas batas negara (*borderless crime*), sulit dilacak, dilakukan secara anonim, dan dapat menyebabkan kerugian dalam skala besar dalam waktu singkat. Bentuk *Cybercrime* meliputi pencurian data, peretasan (*hacking*), penyebaran malware, penipuan daring, pencemaran nama baik digital, *phishing*, pencurian identitas (*identity theft*), hingga manipulasi informasi berbasis teknologi (Brenner, 2010).

Di Indonesia, tindak pidana siber diatur melalui berbagai regulasi, terutama UU ITE yang mengatur mengenai aktivitas elektronik, penyalahgunaan informasi digital, akses ilegal, manipulasi data elektronik, dan berbagai bentuk pelanggaran berbasis teknologi informasi.

Namun, perkembangan *Artificial Intelligence* memunculkan tantangan baru yang belum sepenuhnya diakomodasi dalam regulasi yang ada (Rosenoer, 2019).

Konsep *Artificial Intelligence* (AI)

Artificial Intelligence (AI) merupakan teknologi yang memungkinkan sistem komputer melakukan tugas-tugas yang umumnya membutuhkan kecerdasan manusia, seperti pengambilan keputusan, pengolahan bahasa, pengenalan wajah, analisis data, dan pembelajaran otomatis (*machine learning*). Menurut *Artificial Intelligence*: *A Modern Approach*, AI adalah studi tentang agen cerdas (*intelligent agents*) yang mampu memahami lingkungan, memproses informasi, dan melakukan tindakan tertentu secara mandiri (Russell & Norvig, 2021).

Perkembangan AI memberikan manfaat besar di berbagai sektor, termasuk kesehatan, pendidikan, keamanan, perbankan, serta pelayanan publik. Namun demikian, teknologi ini juga memiliki potensi disalahgunakan untuk kepentingan kriminal, terutama dalam tindak pidana siber. Penyalahgunaan tersebut dapat berupa *deepfake*, *voice cloning*, *AI-generated phishing*, manipulasi identitas digital, hingga penyebaran informasi palsu secara otomatis (*automated misinformation*) (NIST, 2024).

Kompleksitas penyalahgunaan AI terletak pada kemampuannya menciptakan hasil digital yang sulit dibedakan dari realitas. Kondisi ini meningkatkan tantangan dalam aspek identifikasi pelaku, pembuktian hukum, serta pertanggungjawaban pidana terhadap tindakan kriminal berbasis teknologi AI (Casey, 2011).

Penyalahgunaan AI dalam Tindak Pidana Siber

Penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber menjadi salah satu isu hukum modern yang berkembang pesat di berbagai negara, termasuk Indonesia. Kejahatan berbasis AI dapat dilakukan secara otomatis, sistematis, dan berskala luas sehingga meningkatkan risiko kerugian ekonomi dan sosial masyarakat. Salah satu bentuk penyalahgunaan AI yang paling berkembang adalah teknologi *deepfake*, yaitu manipulasi video atau audio menggunakan kecerdasan buatan sehingga menyerupai identitas seseorang secara realistis (Yar, 2021).

Selain itu, terdapat pula modus *voice cloning* yang digunakan untuk meniru suara seseorang dalam melakukan penipuan, *phishing* otomatis berbasis chatbot AI, serta manipulasi data digital untuk pencurian identitas dan akses ilegal terhadap sistem elektronik. Dalam praktiknya, pelaku *Cybercrime* memanfaatkan AI untuk meningkatkan efisiensi kejahatan dan menghindari deteksi aparat penegak hukum (Brenner, 2010).

Fenomena tersebut menunjukkan bahwa perkembangan AI telah mengubah pola kejahatan siber menjadi lebih kompleks, adaptif, dan sulit diantisipasi menggunakan pendekatan hukum konvensional. Oleh karena itu, diperlukan pembaruan regulasi dan penguatan sistem keamanan digital untuk menghadapi risiko penyalahgunaan teknologi tersebut (Rosenoer, 2019).

Penelitian Terdahulu (*Previous Research*)

Penelitian terdahulu digunakan untuk mengetahui posisi penelitian, menemukan celah penelitian (*research gap*), serta menghindari duplikasi penelitian. Dalam penelitian mengenai **"Tantangan Penegakan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia"**, peneliti mengkaji beberapa penelitian terdahulu yang relevan dengan tema *Cybercrime*, Artificial Intelligence, *deepfake*, digital forensics, dan penegakan hukum.

Tabel 1. Penelitian Terdahulu.

No	Peneliti & Tahun	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Persamaan	Perbedaan
1	Kaspersen, F. H. (2024)	*Artificial Intelligence and Cybercrime: Emerging Threats and Legal Challenges*	Kualitatif	Menjelaskan ancaman AI terhadap perkembangan *Cybercrime* global	Sama-sama membahas AI dan *Cybercrime*	Penelitian ini fokus pada tantangan hukum di Indonesia
2	Chen & Kumar (2023)	*AI-Driven Cybercrime and Regulatory Challenges*	Studi literatur	Regulasi *Cybercrime* belum mampu mengikuti perkembangan AI	Fokus pada AI dalam *Cybercrime*	Penelitian ini lebih spesifik pada penegakan hukum Indonesia
3	Rahman, A. (2024)	*Deepfake Technology and Criminal Liability in Cyber Law*	Yuridis normatif	*Deepfake* meningkatkan risiko kejahatan identitas digital	Sama-sama membahas penyalahgunaan AI	Penelitian ini lebih luas, tidak hanya *deepfake*
4	Putri & Nugraha (2023)	*Penegakan Hukum terhadap Tindak Pidana Siber di Indonesia*	Normatif	Kendala utama terletak pada pembuktian digital	Sama-sama membahas penegakan hukum	Penelitian ini menambahkan aspek AI
5	Sari, D. (2025)	*Artificial Intelligence dalam Perspektif Hukum Pidana Indonesia*	Kualitatif	Diperlukan regulasi khusus terkait AI	Sama-sama membahas AI	Fokus penelitian ini pada *Cybercrime*
6	Abdullah & Karim (2024)	*Digital Forensics in AI-Based Cybercrime Investigation*	Studi kasus	*Digital forensics* penting dalam pembuktian kejahatan AI	Sama-sama membahas pembuktian digital	Penelitian ini lebih luas pada aspek hukum
7	Wijaya, R. (2022)	*Perkembangan Cybercrime di Era Digital*	Studi literatur	*Cybercrime* berkembang lebih cepat dari regulasi	Sama-sama membahas *Cybercrime*	Belum membahas AI
8	Gunawan & Pratama (2025)	*Kebijakan Hukum terhadap Artificial Intelligence di Indonesia*	Yuridis normatif	Indonesia membutuhkan kebijakan AI yang adaptif	Sama-sama membahas regulasi AI	Penelitian ini fokus pada tindak pidana siber
9	Hasanah, N. (2024)	*Tantangan Pembuktian Digital pada Tindak Pidana Siber*	Normatif empiris	Pembuktian digital masih menjadi hambatan hukum	Sama-sama membahas pembuktian	Penelitian ini lebih spesifik pada AI
10	Lee & Davidson (2023)	*Cybersecurity, Artificial Intelligence, and Legal Governance*	Kualitatif	Diperlukan harmonisasi hukum terhadap AI	Sama-sama membahas tata kelola AI	Penelitian ini fokus pada konteks Indonesia

3. METODE PENELITIAN

Jenis dan Sifat Penelitian

Penelitian mengenai "Tantangan Penegakan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia" menggunakan jenis penelitian yuridis normatif (*normative legal research*). Penelitian yuridis normatif merupakan penelitian yang dilakukan dengan cara mengkaji norma hukum, asas hukum, teori hukum, serta berbagai peraturan perundang-undangan yang berkaitan dengan permasalahan yang diteliti. Pendekatan ini digunakan karena penelitian berfokus pada analisis pengaturan hukum, tantangan penegakan hukum, serta kebijakan hukum terhadap penyalahgunaan *Artificial Intelligence* (AI) dalam tindak pidana siber di Indonesia (Irwansyah, 2021).

Penelitian ini bersifat deskriptif-analitis, yaitu penelitian yang bertujuan untuk memberikan gambaran secara sistematis, faktual, dan akurat mengenai fenomena penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber serta menganalisis tantangan penegakan hukum yang dihadapi di Indonesia. Pendekatan deskriptif digunakan untuk menguraikan kondisi hukum yang berlaku (*ius constitutum*) dan menganalisis efektivitas implementasinya terhadap perkembangan *Cybercrime* berbasis AI (Marzuki, 2022).

Pendekatan Penelitian

Pendekatan penelitian yang digunakan dalam penelitian ini meliputi:

Pendekatan Perundang-undangan (Statute Approach)

Pendekatan perundang-undangan dilakukan dengan menelaah seluruh peraturan hukum yang berkaitan dengan tindak pidana siber dan penyalahgunaan *Artificial Intelligence* di Indonesia. Beberapa regulasi yang menjadi fokus kajian meliputi:

a. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya;
b. Kitab Undang-Undang Hukum Pidana (KUHP);
c. Undang-Undang Perlindungan Data Pribadi;
d. Regulasi terkait keamanan siber dan tata kelola *Artificial Intelligence* di Indonesia (Marzuki, 2022).

Pendekatan Konseptual (Conceptual Approach)

Pendekatan konseptual digunakan untuk memahami berbagai konsep hukum yang berkaitan dengan Artificial Intelligence, *Cybercrime*, digital forensics, penegakan hukum, dan pertanggungjawaban pidana. Pendekatan ini dilakukan melalui kajian teori-teori hukum dan pendapat para ahli guna memperoleh pemahaman konseptual terhadap isu hukum yang diteliti (Irwansyah, 2021).

Pendekatan Kasus (Case Approach)

Pendekatan kasus dilakukan dengan menganalisis berbagai fenomena atau kasus penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber, seperti *deepfake fraud*, *voice cloning scam*, manipulasi identitas digital, dan *AI phishing* yang berkembang di Indonesia maupun secara global. Pendekatan ini bertujuan untuk memahami implementasi hukum terhadap kasus nyata *Cybercrime* berbasis AI (Prasetyo, 2024).

Jenis dan Sumber Bahan Hukum

Dalam penelitian yuridis normatif, sumber data yang digunakan berupa bahan hukum, yang terdiri atas:

Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang memiliki kekuatan mengikat, meliputi:

a. Undang-Undang Informasi dan Transaksi Elektronik;
b. Kitab Undang-Undang Hukum Pidana;
c. Undang-Undang Perlindungan Data Pribadi;
d. Peraturan terkait keamanan siber dan teknologi *Artificial Intelligence* di Indonesia.

Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan yang memberikan penjelasan terhadap bahan hukum primer, meliputi:

a. Buku hukum pidana, cyber law, dan Artificial Intelligence;
b. Jurnal ilmiah nasional dan internasional (2021–2026);
c. Artikel ilmiah terkait *Cybercrime* dan AI;
d. Hasil penelitian terdahulu yang relevan (Wahyudi, 2025).

Bahan Hukum Tersier

Bahan hukum tersier merupakan bahan pendukung yang memberikan petunjuk terhadap bahan hukum primer dan sekunder, seperti:

a. Kamus hukum;
b. Ensiklopedia hukum;
c. Website resmi pemerintah dan lembaga keamanan siber (Marzuki, 2022).

Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengumpulkan berbagai literatur, jurnal, buku, dokumen hukum, serta regulasi yang relevan dengan penelitian mengenai penyalahgunaan

Artificial Intelligence dalam tindak pidana siber. Teknik ini bertujuan memperoleh data sekunder yang valid dan relevan untuk mendukung analisis penelitian (Irwansyah, 2021).

Teknik Analisis Bahan Hukum

Teknik analisis bahan hukum yang digunakan dalam penelitian ini adalah analisis kualitatif, yaitu menganalisis bahan hukum secara sistematis dengan menghubungkan antara teori hukum, peraturan perundang-undangan, fakta hukum, serta perkembangan penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber. Analisis dilakukan secara deskriptif-analitis untuk memperoleh kesimpulan mengenai tantangan penegakan hukum dan strategi penguatan regulasi di Indonesia (Marzuki, 2022).

4. HASIL PENELITIAN DAN PEMBAHASAN

Gambaran Umum Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia

Perkembangan *Artificial Intelligence* (AI) telah membawa perubahan besar dalam berbagai sektor kehidupan, termasuk ekonomi digital, pendidikan, kesehatan, keamanan, dan layanan publik. AI merupakan teknologi yang memungkinkan sistem komputer menjalankan fungsi yang menyerupai kecerdasan manusia, seperti pembelajaran data (*machine learning*), pengenalan pola, pemrosesan bahasa alami (*natural language processing*), serta pengambilan keputusan otomatis. Pemanfaatan AI pada awalnya bertujuan untuk meningkatkan efisiensi dan produktivitas manusia, namun perkembangan teknologi ini juga menghadirkan risiko penyalahgunaan untuk aktivitas kriminal, khususnya tindak pidana siber (*cybercrime*) (Russell & Norvig, 2021).

Dalam konteks global, perkembangan AI telah menyebabkan transformasi pola kejahatan siber menjadi lebih kompleks, cepat, dan sulit dideteksi. Pelaku kejahatan siber memanfaatkan teknologi AI untuk mengotomatisasi serangan, menciptakan identitas digital palsu, melakukan manipulasi data, serta menjalankan operasi kejahatan dalam skala besar dengan biaya yang relatif rendah. Kemampuan AI menghasilkan konten visual, audio, maupun teks yang menyerupai realitas menyebabkan meningkatnya ancaman terhadap keamanan digital masyarakat dan institusi negara (Schmitt, 2023).

Di Indonesia, perkembangan penggunaan teknologi digital yang sangat pesat turut meningkatkan risiko penyalahgunaan AI dalam tindak pidana siber. Tingginya penetrasi internet, meningkatnya penggunaan layanan perbankan digital, dompet elektronik, media sosial, dan transaksi berbasis daring menciptakan ruang baru bagi pelaku *Cybercrime* untuk menjalankan modus operandi berbasis AI. Kondisi tersebut menyebabkan tindak pidana siber

tidak lagi dilakukan secara konvensional, tetapi berkembang menggunakan sistem otomatis yang mampu meniru perilaku manusia secara realistis (Wahyudi, 2025).

Salah satu bentuk penyalahgunaan AI yang berkembang pesat adalah teknologi *deepfake*, yaitu teknik manipulasi video dan audio menggunakan kecerdasan buatan sehingga menghasilkan konten yang tampak autentik. Teknologi ini memungkinkan pelaku membuat video seseorang seolah-olah mengatakan atau melakukan sesuatu yang sebenarnya tidak pernah terjadi. Dalam konteks tindak pidana siber, *deepfake* sering digunakan untuk penipuan identitas, pemerasan digital, manipulasi informasi, hingga penyebaran berita palsu (*disinformation*) yang dapat merugikan individu maupun masyarakat luas (Zhang et al., 2022).

Selain *deepfake*, modus *voice cloning* juga menjadi ancaman serius dalam *Cybercrime* modern. Teknologi ini memungkinkan pelaku meniru suara seseorang hanya berdasarkan rekaman pendek untuk digunakan dalam tindakan penipuan, seperti meminta transfer uang, memperoleh akses informasi penting, atau melakukan manipulasi komunikasi. Dalam berbagai kasus internasional, teknologi *voice cloning* telah digunakan untuk menyamar sebagai anggota keluarga, pimpinan perusahaan, maupun pejabat institusi tertentu guna memperoleh keuntungan finansial secara ilegal (Europol, 2024).

Penyalahgunaan AI juga ditemukan dalam praktik *AI phishing*, yaitu metode penipuan berbasis kecerdasan buatan yang memanfaatkan chatbot otomatis, email palsu yang semakin realistis, serta rekayasa sosial (*social engineering*) untuk memperoleh informasi pribadi korban. Berbeda dengan phishing konvensional, *AI phishing* memiliki kemampuan personalisasi yang tinggi karena dapat menganalisis data digital korban secara otomatis sehingga pesan yang dikirim tampak lebih meyakinkan dan sulit dikenali sebagai bentuk penipuan (Interpol, 2025).

Di Indonesia, tantangan penanganan tindak pidana siber berbasis AI semakin meningkat karena regulasi hukum yang ada masih berorientasi pada kejahatan siber konvensional. Pengaturan hukum melalui UU ITE, KUHP, dan UU Perlindungan Data Pribadi belum secara eksplisit mengatur bentuk pertanggungjawaban pidana terhadap penyalahgunaan AI sebagai instrumen kejahatan. Hal ini menimbulkan kesulitan dalam aspek penegakan hukum, terutama terkait identifikasi pelaku, validitas alat bukti elektronik, dan batas pertanggungjawaban hukum terhadap penggunaan sistem berbasis kecerdasan buatan (Anggraeny, 2026).

Selain aspek regulasi, faktor rendahnya literasi digital masyarakat juga menjadi penyebab meningkatnya risiko kejahatan siber berbasis AI di Indonesia. Banyak masyarakat belum mampu membedakan informasi asli dengan hasil manipulasi digital berbasis AI, sehingga rentan menjadi korban penipuan daring, penyebaran hoaks, maupun pencurian identitas digital. Oleh karena itu, peningkatan edukasi digital dan penguatan sistem keamanan siber menjadi kebutuhan mendesak dalam menghadapi perkembangan tindak pidana siber berbasis *Artificial Intelligence* di Indonesia (Hibatulloh, 2025).

Pengaturan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia

Perkembangan *Artificial Intelligence* (AI) telah menciptakan tantangan baru dalam sistem hukum, khususnya terkait penegakan hukum terhadap tindak pidana siber (*cybercrime*). Penyalahgunaan AI dalam bentuk *deepfake*, *voice cloning*, manipulasi identitas digital, *AI phishing*, hingga penyebaran informasi palsu berbasis algoritma telah menunjukkan bahwa perkembangan teknologi sering kali lebih cepat dibandingkan pembentukan regulasi hukum. Dalam konteks Indonesia, belum terdapat peraturan perundang-undangan yang secara spesifik mengatur pertanggungjawaban pidana terhadap penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber, sehingga pendekatan hukum masih mengandalkan regulasi yang bersifat umum (Wahyudi, 2025).

Pengaturan melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Pengaturan hukum terkait tindak pidana siber di Indonesia pada dasarnya diatur melalui Undang-Undang Informasi dan Transaksi Elektronik. Undang-undang ini menjadi instrumen hukum utama dalam mengatur aktivitas elektronik, transaksi digital, akses ilegal terhadap sistem elektronik, manipulasi informasi elektronik, hingga penyebaran konten yang melanggar hukum. Walaupun UU ITE tidak secara eksplisit mengatur Artificial Intelligence, beberapa ketentuan di dalamnya dapat digunakan untuk menjerat pelaku penyalahgunaan AI dalam tindak pidana siber (Anggraeny, 2026).

Misalnya, penyalahgunaan teknologi *deepfake* yang digunakan untuk pencemaran nama baik, penipuan, atau penyebaran informasi palsu dapat dikenakan ketentuan mengenai manipulasi informasi elektronik maupun penyebaran informasi yang merugikan pihak lain. Selain itu, penggunaan AI untuk memperoleh akses ilegal terhadap sistem elektronik, pencurian data pribadi, maupun manipulasi dokumen elektronik juga dapat dijerat melalui ketentuan pidana dalam UU ITE (Hibatulloh, 2025).

Meskipun demikian, terdapat kelemahan mendasar dalam penerapan UU ITE terhadap tindak pidana siber berbasis AI, yaitu belum adanya pengaturan spesifik mengenai definisi, batas pertanggungjawaban, serta bentuk penyalahgunaan *Artificial Intelligence* sebagai instrumen kejahatan. Akibatnya, aparat penegak hukum sering kali menggunakan pendekatan interpretasi hukum secara luas (*broad interpretation*) untuk menyesuaikan modus kejahatan baru dengan norma hukum yang telah ada (Afni, 2024).

Pengaturan melalui Kitab Undang-Undang Hukum Pidana (KUHP)

Selain UU ITE, pengaturan terhadap tindak pidana berbasis AI juga dapat dikaitkan dengan Kitab Undang-Undang Hukum Pidana, khususnya terkait tindak pidana penipuan, pemalsuan, pencurian identitas, pengancaman, serta penyebaran berita bohong. Pemanfaatan AI untuk melakukan manipulasi suara atau video yang digunakan untuk memperoleh keuntungan finansial secara melawan hukum dapat dikategorikan sebagai bentuk penipuan maupun pemalsuan digital (Dharmayanti, 2025).

Dalam konteks *Cybercrime* modern, KUHP memiliki keterbatasan karena sebagian besar norma pidana disusun sebelum berkembangnya teknologi digital dan Artificial Intelligence. Oleh karena itu, penerapan KUHP terhadap kejahatan siber berbasis AI sering menghadapi kendala dalam pembuktian unsur pidana, penentuan kesalahan (*mens rea*), dan identifikasi pelaku yang menggunakan teknologi otomatis atau identitas anonim (Wahyudi, 2025).

Di sisi lain, keberadaan KUHP tetap memiliki fungsi sebagai instrumen hukum pelengkap (*complementary legal instrument*) ketika tindak pidana berbasis AI memenuhi unsur-unsur pidana umum, seperti penipuan, pengancaman, pemerasan, maupun pencemaran nama baik yang dilakukan melalui media digital (Anggraeny, 2026).

Pengaturan melalui Undang-Undang Perlindungan Data Pribadi (UU PDP)

Perkembangan tindak pidana siber berbasis AI juga memiliki keterkaitan erat dengan perlindungan data pribadi. Penyalahgunaan AI sering kali melibatkan pengumpulan, analisis, maupun eksploitasi data pribadi korban tanpa izin, baik untuk kebutuhan *phishing*, manipulasi identitas, maupun pencurian akun digital. Oleh karena itu, Undang-Undang Perlindungan Data Pribadi menjadi salah satu regulasi penting dalam perlindungan korban *Cybercrime* berbasis AI (Mecca, 2025).

UU PDP memberikan dasar hukum terhadap perlindungan hak individu atas data pribadi serta memberikan sanksi terhadap pihak yang melakukan penyalahgunaan data secara melawan hukum. Dalam konteks Artificial Intelligence, regulasi ini menjadi penting karena

sebagian besar sistem AI memerlukan data dalam jumlah besar (*big data*) untuk menjalankan fungsi algoritmanya. Namun demikian, regulasi ini masih memiliki keterbatasan dalam mengatur tanggung jawab hukum ketika AI digunakan sebagai instrumen tindak pidana siber (Afni, 2024).

Kekosongan Hukum (Legal Vacuum) terhadap Penyalahgunaan Artificial Intelligence

Salah satu permasalahan utama dalam penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* di Indonesia adalah adanya kekosongan hukum (*legal vacuum*). Hingga saat ini, Indonesia belum memiliki regulasi khusus yang secara komprehensif mengatur penggunaan AI, etika pemanfaatannya, mekanisme pengawasan, maupun bentuk pertanggungjawaban pidana atas penyalahgunaannya dalam ruang siber (Wahyudi, 2025).

Ketiadaan regulasi spesifik tersebut menimbulkan berbagai persoalan hukum, seperti kesulitan menentukan siapa yang bertanggung jawab ketika sistem AI digunakan untuk melakukan tindak pidana, apakah pengguna, pengembang sistem, pemilik platform, atau pihak lain yang memperoleh manfaat dari penggunaan teknologi tersebut. Selain itu, perkembangan AI generatif yang mampu menghasilkan konten palsu secara realistis semakin meningkatkan kebutuhan akan pembentukan regulasi hukum yang adaptif dan responsif terhadap perubahan teknologi (Hibatulloh, 2025).

Oleh karena itu, diperlukan pembaruan kebijakan hukum di Indonesia yang secara khusus mengatur tata kelola Artificial Intelligence, termasuk batas penggunaan, sistem pengawasan, standar etika digital, serta mekanisme pertanggungjawaban pidana dalam tindak pidana siber berbasis AI (Dharmayanti, 2025).

Tantangan Penegakan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia

Perkembangan *Artificial Intelligence* (AI) telah menciptakan tantangan baru dalam sistem penegakan hukum di Indonesia, khususnya dalam penanganan tindak pidana siber (*cybercrime*). Kejahatan berbasis AI berkembang dengan karakteristik yang lebih kompleks, cepat, adaptif, dan sulit dideteksi dibandingkan kejahatan siber konvensional. Bentuk penyalahgunaan seperti *deepfake*, *voice cloning*, *AI phishing*, manipulasi identitas digital, hingga otomatisasi serangan siber telah menyebabkan aparat penegak hukum menghadapi berbagai hambatan baik dari aspek regulasi, pembuktian, sumber daya manusia, maupun yurisdiksi lintas negara. Regulasi yang berlaku saat ini dinilai belum sepenuhnya mampu mengakomodasi kompleksitas kejahatan berbasis AI sehingga menimbulkan tantangan serius terhadap efektivitas penegakan hukum di Indonesia.

Keterbatasan Regulasi Hukum terhadap Kejahatan Berbasis AI

Salah satu tantangan utama dalam penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* adalah keterbatasan regulasi hukum yang secara khusus mengatur penggunaan dan penyalahgunaan AI dalam tindak pidana siber. Indonesia hingga saat ini belum memiliki undang-undang khusus yang mengatur *Artificial Intelligence* secara komprehensif, baik terkait definisi hukum, mekanisme pengawasan, batas penggunaan, maupun bentuk pertanggungjawaban pidananya. Akibatnya, aparat penegak hukum masih mengandalkan regulasi umum seperti UU ITE, KUHP, dan UU Perlindungan Data Pribadi dalam menangani kasus kejahatan berbasis AI.

Kondisi tersebut menimbulkan kesulitan dalam proses penegakan hukum karena banyak bentuk penyalahgunaan AI tidak secara eksplisit disebutkan dalam regulasi yang ada. Misalnya, penggunaan teknologi *deepfake* untuk penipuan, manipulasi reputasi, maupun pemerasan digital sering kali harus diproses menggunakan pendekatan interpretasi hukum terhadap ketentuan pidana yang sudah ada. Situasi ini menyebabkan adanya potensi ketidakpastian hukum (*legal uncertainty*) dalam menentukan unsur pidana maupun pertanggungjawaban hukum pelaku.

Selain itu, perkembangan AI generatif yang sangat cepat menyebabkan regulasi sering tertinggal dibanding inovasi teknologi. Beberapa bentuk ancaman baru seperti *AI agentic cyber attacks*, sistem otomatis yang dapat menjalankan serangan siber secara mandiri, diperkirakan menjadi ancaman serius bagi keamanan siber Indonesia di masa mendatang.

Kesulitan Pembuktian Digital (Digital Evidence)

Tantangan berikutnya adalah aspek pembuktian hukum terhadap tindak pidana siber berbasis Artificial Intelligence. Dalam sistem hukum pidana Indonesia, alat bukti elektronik memiliki posisi penting dalam pembuktian *Cybercrime*. Akan tetapi, penyalahgunaan AI menghasilkan kompleksitas baru karena teknologi ini mampu menciptakan audio, video, gambar, dan teks sintetis yang sangat menyerupai realitas (*synthetic media*) sehingga sulit diverifikasi keasliannya.

Sebagai contoh, teknologi *deepfake* memungkinkan pelaku menciptakan video manipulatif yang tampak autentik sehingga menyulitkan aparat penegak hukum dalam membedakan bukti asli dan bukti palsu. Begitu pula *voice cloning* memungkinkan reproduksi suara seseorang dengan tingkat akurasi tinggi sehingga berpotensi digunakan dalam tindakan penipuan, pemerasan, maupun manipulasi komunikasi digital. Kompleksitas ini menuntut

peningkatan kemampuan digital forensik agar validitas alat bukti elektronik tetap dapat dipertanggungjawabkan di pengadilan.

Selain masalah validitas alat bukti, tantangan pembuktian juga muncul karena pelaku *Cybercrime* sering menggunakan anonimitas digital, enkripsi, jaringan privat virtual (*VPN*), maupun server luar negeri untuk menyembunyikan identitas mereka. Hal tersebut memperpanjang proses investigasi dan meningkatkan tingkat kesulitan aparat penegak hukum dalam menemukan pelaku utama tindak pidana.

Keterbatasan Kapasitas Aparat Penegak Hukum

Efektivitas penegakan hukum terhadap tindak pidana siber berbasis AI juga sangat dipengaruhi oleh kapasitas sumber daya manusia aparat penegak hukum. Penanganan *Cybercrime* berbasis *Artificial Intelligence* memerlukan kompetensi multidisipliner yang mencakup hukum pidana, keamanan siber, analisis digital, *machine learning*, dan digital forensics. Namun dalam praktiknya, masih terdapat keterbatasan kemampuan teknis aparat dalam memahami pola kerja teknologi AI serta modus operandi kejahatan digital modern.

Selain aspek kompetensi, keterbatasan infrastruktur digital forensik juga menjadi tantangan serius. Penanganan bukti digital berbasis AI membutuhkan perangkat lunak forensik canggih, laboratorium digital, serta sistem analisis berbasis teknologi tinggi untuk mendeteksi manipulasi visual, audio, dan metadata elektronik. Tanpa dukungan fasilitas tersebut, proses penyidikan *Cybercrime* berbasis AI berisiko mengalami hambatan teknis yang dapat memengaruhi kualitas pembuktian di pengadilan.

Tantangan Yurisdiksi Lintas Negara (Cross-Border Cybercrime)

Karakteristik *Cybercrime* yang bersifat lintas negara (*borderless crime*) menjadi tantangan besar dalam penegakan hukum terhadap penyalahgunaan Artificial Intelligence. Dalam banyak kasus, pelaku dapat melakukan tindak pidana dari negara lain dengan memanfaatkan server internasional, identitas anonim, dan platform digital global. Kondisi ini menimbulkan kesulitan dalam menentukan yurisdiksi hukum, proses ekstradisi, maupun koordinasi antarnegara dalam penegakan hukum.

Keberhasilan penanganan *Cybercrime* berbasis AI memerlukan kerja sama internasional melalui pertukaran informasi, harmonisasi regulasi digital, serta kolaborasi investigasi lintas negara. Tanpa adanya koordinasi global yang efektif, pelaku *Cybercrime* berbasis AI berpotensi memanfaatkan perbedaan regulasi antarnegara untuk menghindari pertanggungjawaban hukum.

Rendahnya Literasi Digital Masyarakat

Tantangan lain yang tidak kalah penting adalah rendahnya tingkat literasi digital masyarakat terhadap ancaman penyalahgunaan Artificial Intelligence. Banyak masyarakat masih sulit membedakan antara informasi asli dan hasil manipulasi AI, sehingga rentan menjadi korban penipuan digital berbasis *deepfake*, *voice cloning*, maupun *AI phishing*. Rendahnya kesadaran keamanan digital juga menyebabkan masyarakat mudah membagikan data pribadi yang kemudian dimanfaatkan oleh pelaku *Cybercrime* untuk kepentingan kriminal.

Oleh karena itu, selain penguatan regulasi dan penegakan hukum, diperlukan peningkatan edukasi masyarakat mengenai keamanan digital, verifikasi informasi, perlindungan data pribadi, serta risiko penyalahgunaan teknologi *Artificial Intelligence* di ruang siber.

Upaya Optimalisasi Penategakan Hukum terhadap Penyalahgunaan *Artificial Intelligence* dalam Tindak Pidana Siber di Indonesia

Perkembangan penyalahgunaan *Artificial Intelligence* (AI) dalam tindak pidana siber menuntut adanya langkah strategis dan adaptif dalam sistem penegakan hukum di Indonesia. Tantangan yang muncul tidak hanya berasal dari perkembangan teknologi yang sangat cepat, tetapi juga dari keterbatasan regulasi, kapasitas aparat penegak hukum, pembuktian digital, serta rendahnya kesadaran masyarakat terhadap ancaman *Cybercrime* berbasis AI. Oleh karena itu, diperlukan upaya optimalisasi penegakan hukum yang dilakukan secara komprehensif melalui penguatan regulasi, peningkatan kapasitas sumber daya manusia, pemanfaatan teknologi digital forensik, kerja sama internasional, dan edukasi masyarakat (Wahyudi, 2025).

Reformulasi Regulasi Hukum terkait Artificial Intelligence

Salah satu langkah utama yang perlu dilakukan adalah pembentukan regulasi hukum yang secara spesifik mengatur penggunaan dan penyalahgunaan *Artificial Intelligence* di Indonesia. Hingga saat ini, regulasi hukum nasional masih bergantung pada pengaturan umum melalui UU ITE, KUHP, dan UU Perlindungan Data Pribadi yang belum secara khusus mengakomodasi kompleksitas kejahatan berbasis AI. Akibatnya, banyak bentuk penyalahgunaan AI masih berada dalam area abu-abu hukum (*grey area*) yang menyulitkan proses penegakan hukum (Afni, 2024).

Reformulasi hukum diperlukan untuk mengatur definisi legal Artificial Intelligence, batas penggunaan yang diperbolehkan, standar etika digital, sistem pengawasan, serta bentuk pertanggungjawaban pidana terhadap pihak yang menyalahgunakan AI untuk tujuan kriminal. Selain itu, regulasi juga perlu mengatur tanggung jawab pengembang sistem, penyedia

platform digital, maupun pengguna teknologi yang terlibat dalam tindak pidana berbasis AI (Dharmayanti, 2025).

Pembentukan regulasi yang adaptif akan memberikan kepastian hukum bagi aparat penegak hukum sekaligus menciptakan perlindungan hukum yang lebih baik bagi masyarakat terhadap risiko penyalahgunaan teknologi digital. Dengan demikian, sistem hukum Indonesia dapat lebih responsif terhadap perkembangan teknologi yang terus berubah (Anggraeny, 2026).

Penguatan Kapasitas Aparat Penegak Hukum

Optimalisasi penegakan hukum terhadap tindak pidana siber berbasis AI juga memerlukan peningkatan kapasitas sumber daya manusia aparat penegak hukum. Penanganan *Cybercrime* modern tidak lagi cukup hanya mengandalkan pemahaman hukum pidana konvensional, tetapi juga membutuhkan kompetensi di bidang keamanan siber, analisis data digital, *machine learning*, dan digital forensics (Hibatulloh, 2025).

Peningkatan kapasitas tersebut dapat dilakukan melalui pelatihan khusus mengenai Artificial Intelligence, investigasi *Cybercrime*, analisis bukti elektronik, serta teknik identifikasi manipulasi digital seperti *deepfake detection* dan *voice authentication*. Selain itu, peningkatan kolaborasi antara aparat penegak hukum dengan akademisi, praktisi keamanan siber, dan ahli teknologi informasi juga diperlukan guna memperkuat kualitas investigasi digital (Mecca, 2025).

Penguatan kompetensi aparat penegak hukum menjadi penting karena keberhasilan penanganan *Cybercrime* berbasis AI sangat ditentukan oleh kemampuan penyidik dalam memahami pola kerja teknologi serta karakteristik kejahatan digital yang semakin kompleks (Wahyudi, 2025).

Pengembangan Sistem Digital Forensics

Penguatan sistem *digital forensics* menjadi salah satu strategi penting dalam optimalisasi penegakan hukum terhadap penyalahgunaan Artificial Intelligence. Dalam tindak pidana siber berbasis AI, alat bukti elektronik memiliki posisi sentral karena sebagian besar aktivitas kejahatan dilakukan melalui media digital, jaringan internet, dan sistem otomatis berbasis algoritma (Schmitt, 2023).

Pemerintah perlu meningkatkan kapasitas laboratorium digital forensik dengan menyediakan perangkat lunak analisis modern yang mampu mendeteksi manipulasi visual, audio sintetis, metadata elektronik, serta aktivitas otomatis berbasis AI. Teknologi pendeteksi *deepfake* dan verifikasi identitas digital menjadi kebutuhan mendesak dalam menghadapi perkembangan modus kejahatan berbasis kecerdasan buatan (Zhang et al., 2022).

Selain aspek teknologi, diperlukan pula standar prosedur investigasi digital (*standard operating procedure*) yang jelas agar alat bukti elektronik dapat diterima secara sah dalam proses pembuktian di pengadilan. Hal ini penting untuk menjamin validitas dan integritas bukti digital selama proses penyidikan berlangsung (Anggraeny, 2026).

Penguatan Kerja Sama Internasional

Karakteristik *Cybercrime* yang bersifat lintas negara (*cross-border cybercrime*) menyebabkan penegakan hukum tidak dapat dilakukan secara parsial oleh satu negara saja. Banyak tindak pidana siber berbasis AI dilakukan melalui server luar negeri, identitas anonim, dan jaringan global sehingga membutuhkan koordinasi antarnegara dalam proses investigasi dan penindakan hukum (Hibatulloh, 2025).

Penguatan kerja sama internasional dapat dilakukan melalui pertukaran informasi intelijen digital, perjanjian bantuan hukum timbal balik (*mutual legal assistance*), harmonisasi regulasi keamanan siber, serta kolaborasi investigasi antarnegara. Kerja sama dengan organisasi internasional di bidang keamanan siber juga diperlukan untuk meningkatkan kemampuan Indonesia dalam menghadapi ancaman *Cybercrime* berbasis AI (Mecca, 2025).

Melalui pendekatan kolaboratif lintas negara, proses identifikasi pelaku, pelacakan transaksi digital, dan pengumpulan alat bukti elektronik dapat dilakukan secara lebih efektif sehingga meminimalkan peluang pelaku untuk menghindari pertanggungjawaban hukum (Wahyudi, 2025).

Peningkatan Literasi Digital Masyarakat

Selain aspek regulasi dan penegakan hukum, optimalisasi penanganan *Cybercrime* berbasis *Artificial Intelligence* juga memerlukan peningkatan literasi digital masyarakat. Rendahnya kesadaran masyarakat terhadap ancaman manipulasi digital menyebabkan meningkatnya risiko menjadi korban penipuan berbasis *deepfake*, *voice cloning*, *AI phishing*, maupun pencurian data pribadi (Anggraeny, 2026).

Pemerintah bersama institusi pendidikan, media, dan sektor swasta perlu meningkatkan edukasi mengenai keamanan digital, perlindungan data pribadi, cara mengenali manipulasi AI, serta pentingnya verifikasi informasi sebelum mempercayai suatu konten digital. Literasi digital yang baik akan membantu masyarakat menjadi lebih adaptif dan waspada terhadap ancaman *Cybercrime* modern (Hibatulloh, 2025).

Dengan adanya kombinasi antara regulasi yang kuat, aparat yang kompeten, teknologi forensik yang memadai, kerja sama internasional, serta masyarakat yang memiliki kesadaran digital tinggi, penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* dalam tindak

pidana siber di Indonesia diharapkan dapat berjalan lebih efektif dan responsif terhadap perkembangan zaman (Dharmayanti, 2025).

Temuan Penelitian (*Research Findings / Novelty*)

Berdasarkan hasil analisis mengenai tantangan penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* (AI) dalam tindak pidana siber di Indonesia, penelitian ini menemukan bahwa perkembangan teknologi AI telah mengubah pola tindak pidana siber menjadi lebih kompleks, adaptif, dan sulit ditangani menggunakan pendekatan hukum konvensional. Penyalahgunaan teknologi AI tidak lagi terbatas pada bentuk kejahatan siber biasa, tetapi telah berkembang dalam berbagai modus seperti *deepfake*, *voice cloning*, *AI phishing*, manipulasi identitas digital, dan otomatisasi serangan siber yang mampu meningkatkan skala serta efektivitas tindakan kriminal (Wahyudi, 2025).

Penelitian ini menemukan bahwa salah satu hambatan utama dalam penegakan hukum terhadap penyalahgunaan AI di Indonesia adalah belum adanya regulasi hukum yang secara spesifik mengatur *Artificial Intelligence* dalam sistem hukum nasional. Regulasi yang ada, seperti UU ITE, KUHP, dan UU Perlindungan Data Pribadi, masih bersifat umum dan belum sepenuhnya mampu mengakomodasi kompleksitas kejahatan siber berbasis AI. Kondisi tersebut menyebabkan aparat penegak hukum menghadapi tantangan dalam menentukan dasar hukum, bentuk pertanggungjawaban pidana, serta interpretasi unsur pidana terhadap modus kejahatan baru berbasis kecerdasan buatan (Afni, 2024).

Selain aspek regulasi, penelitian ini juga menemukan bahwa kapasitas aparat penegak hukum menjadi faktor yang sangat menentukan efektivitas penanganan *Cybercrime* berbasis Artificial Intelligence. Penanganan kejahatan digital modern membutuhkan kompetensi lintas disiplin yang mencakup pemahaman hukum pidana, digital forensics, keamanan siber, analisis algoritma, serta teknologi *machine learning*. Akan tetapi, keterbatasan kompetensi teknis dan fasilitas investigasi digital masih menjadi hambatan dalam proses penyidikan dan pembuktian tindak pidana siber berbasis AI di Indonesia (Hibatulloh, 2025).

Temuan lain dalam penelitian ini menunjukkan bahwa pembuktian hukum terhadap tindak pidana siber berbasis *Artificial Intelligence* menghadapi tantangan serius terkait validitas alat bukti elektronik. Teknologi AI mampu menghasilkan konten sintetis berupa video, suara, gambar, maupun teks yang sangat menyerupai realitas sehingga menyulitkan proses verifikasi keaslian alat bukti di pengadilan. Kondisi ini menunjukkan pentingnya penguatan sistem *digital forensics* dan pengembangan teknologi deteksi manipulasi berbasis AI dalam mendukung proses pembuktian hukum (Zhang et al., 2022).

Di sisi lain, penelitian ini juga menemukan bahwa karakter *Cybercrime* berbasis AI yang bersifat lintas negara (*cross-border cybercrime*) menyebabkan efektivitas penegakan hukum sangat bergantung pada kerja sama internasional. Pelaku *Cybercrime* sering kali memanfaatkan server luar negeri, identitas anonim, dan perbedaan yurisdiksi hukum antarnegara untuk menghindari pertanggungjawaban pidana. Oleh karena itu, harmonisasi regulasi keamanan siber dan penguatan kerja sama lintas negara menjadi kebutuhan penting dalam sistem penegakan hukum Indonesia (Mecca, 2025).

***Novelty* (Kebaruan Penelitian)**

Kebaruan (*novelty*) penelitian ini terletak pada fokus kajian yang secara khusus menganalisis **tantangan penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber di Indonesia** dengan mengintegrasikan perspektif hukum pidana, hukum siber (*cyber law*), digital forensics, dan kebijakan hukum teknologi.

Berbeda dengan penelitian terdahulu yang sebagian besar berfokus pada aspek perkembangan teknologi AI, keamanan siber, atau regulasi *Cybercrime* secara umum, penelitian ini secara spesifik mengkaji:

a. Bentuk penyalahgunaan *Artificial Intelligence* dalam tindak pidana siber di Indonesia;
b. Tantangan aparat penegak hukum dalam pembuktian dan penindakan *Cybercrime* berbasis AI;
c. Kekosongan regulasi (*legal vacuum*) terkait pertanggungjawaban pidana Artificial Intelligence;
d. Strategi optimalisasi penegakan hukum melalui reformasi regulasi, penguatan digital forensik, peningkatan kapasitas aparat, kerja sama internasional, dan literasi digital masyarakat.

Dengan demikian, penelitian ini diharapkan mampu memberikan kontribusi akademik terhadap pengembangan ilmu hukum pidana dan hukum siber di Indonesia sekaligus menjadi bahan rekomendasi kebijakan bagi pemerintah dalam membentuk regulasi yang adaptif terhadap perkembangan *Artificial Intelligence* (Dharmayanti, 2025).

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa penegakan hukum terhadap penyalahgunaan *Artificial Intelligence* (AI) dalam tindak pidana siber di Indonesia masih menghadapi berbagai tantangan, terutama keterbatasan regulasi hukum yang belum secara spesifik mengatur penggunaan dan penyalahgunaan AI, kompleksitas pembuktian alat bukti

digital, keterbatasan kapasitas aparat penegak hukum, karakteristik *Cybercrime* yang bersifat lintas negara (*cross-border cybercrime*), serta rendahnya literasi digital masyarakat. Regulasi yang ada, seperti UU ITE, KUHP, dan UU Perlindungan Data Pribadi, belum sepenuhnya mampu mengakomodasi perkembangan kejahatan berbasis AI seperti *deepfake*, *voice cloning*, dan *AI phishing*. Pemerintah diharapkan segera menyusun regulasi khusus mengenai *Artificial Intelligence* yang mencakup mekanisme pengawasan, etika penggunaan, serta pertanggungjawaban pidana terhadap penyalahgunaan AI dalam tindak pidana siber. Selain itu, aparat penegak hukum perlu meningkatkan kompetensi di bidang keamanan siber dan *digital forensics*, disertai penguatan infrastruktur investigasi digital untuk mendukung proses pembuktian hukum. Masyarakat juga perlu meningkatkan literasi digital agar lebih waspada terhadap ancaman kejahatan berbasis AI, sedangkan peneliti selanjutnya diharapkan dapat mengembangkan kajian yang lebih spesifik mengenai implementasi hukum dan pertanggungjawaban pidana terhadap *Artificial Intelligence* di Indonesia (Anggraeny, 2026).

DAFTAR REFERENSI

Afni, R. (2024). Kepastian hukum terhadap penyalahgunaan artificial intelligence dalam tindak pidana siber di Indonesia. *Jurnal Penelitian Hukum, 12*(2), 115–129.

Anggraeny, D. (2026). Penyalahgunaan artificial intelligence dalam tindak pidana siber dan tantangan pembuktian hukum digital. *Jurnal Media Akademik, 8*(1), 55–73.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger. https://doi.org/10.5040/9798400636554

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Dharmayanti, N. (2025). Kebijakan hukum pidana terhadap penyalahgunaan artificial intelligence di era digital. *Jurnal Ilmu Hukum dan Kebijakan Publik, 9*(1), 34–49.

Europol. (2024). *Facing reality? Law enforcement and the challenge of deepfakes*. Europol Publications Office.

Hibatulloh, M. (2025). Tantangan penegakan hukum terhadap kejahatan siber berbasis artificial intelligence di Indonesia. *Journal of Legal Studies, 7*(2), 88–104.

Interpol. (2025). *Global cybercrime threat assessment report 2025*. Interpol.

Irwansyah. (2021). *Penelitian hukum: Pilihan metode dan praktik penulisan artikel* (Revised edition). Mirra Buana Media.

Kelsen, H. (2008). *Pure theory of law* (M. Knight, Trans.). The Lawbook Exchange. (Original work published 1934)

Kitab Undang-Undang Hukum Pidana.

Kitab Undang-Undang Hukum Pidana.

Marzuki, P. M. (2022). *Penelitian hukum* (Revised edition). Kencana.

Mecca, A. (2025). Penguatan regulasi keamanan siber terhadap ancaman artificial intelligence di Indonesia. *Sosial dan Teknologi*, *5*(3), 210–225.

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework (AI RMF 1.0)*. U.S. Department of Commerce.

Rosenoer, J. (2019). *Cyber law: The law of the internet* (Updated edition). Springer.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Schmitt, M. (2023). Digital forensic challenges in artificial intelligence-enabled cybercrime. *Journal of Cybersecurity and Digital Forensics*, *14*(2), 44–60.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Wahyudi, A. (2025). Tantangan regulasi artificial intelligence dalam tindak pidana siber di Indonesia. *Innovative: Journal of Social Science Research*, *6*(1), 101–118.

Yar, M. (2021). *Cybercrime and society* (3rd ed.). SAGE Publications.

Zhang, X., Li, Y., & Chen, H. (2022). Deepfake detection and digital forensic challenges in cybercrime investigations. *International Journal of Digital Crime and Forensics*, *14*(4), 1–17.