Jurnal Dialogica

Volume 1 Issue 2 Tahun 2026

Kebijakan Formulasi Pidana Dalam Merespons Kejahatan Siber Berbasis Kecerdasan Buatan

Muhammad Alpian Fauzan[1], Askari Razak [2], Hardianto Djanggih [3]

Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Email Koresponden: Alpianfauzanumi@gmail.com

Abstrak

Perkembangan kecerdasan buatan telah mengubah pola kejahatan siber menjadi lebih kompleks, masif, dan sulit dideteksi. Salah satu bentuk penyalahgunaan teknologi tersebut adalah pemanfaatan deepfake yang berpotensi merugikan individu maupun kepentingan publik. Penelitian ini bertujuan untuk menganalisis respons hukum pidana terhadap penggunaan kecerdasan buatan sebagai sarana kejahatan siber serta merumuskan arah kebijakan formulasi pidana yang relevan dengan perkembangan teknologi digital. Penelitian ini menggunakan pendekatan normatif dengan analisis konseptual dan sistematis terhadap bahan hukum primer dan sekunder. Kebaruan penelitian ini terletak pada penekanan terhadap urgensi formulasi hukum pidana yang secara eksplisit mengakomodasi karakteristik kejahatan berbasis kecerdasan buatan, khususnya terkait pertanggungjawaban pidana dan pembuktian digital. Hasil penelitian ini menunjukkan bahwa pengaturan hukum pidana yang ada masih bersifat umum dan belum sepenuhnya mampu menjawab tantangan kejahatan siber berbasis kecerdasan buatan. Oleh karena itu, diperlukan kebijakan formulasi pidana yang adaptif, progresif, dan berorientasi pada perlindungan hukum di ruang digital.

Kata Kunci: *Kebijakan Pidana; Kejahatan Siber; Kecerdasan Buatan; Deepfake.*

Abstract

The rapid development of artificial intelligence has transformed cybercrime into more sophisticated, massive, and difficult-to-detect forms. One significant misuse of this technology is deepfake, which poses serious risks to individuals and public interests. This study aims to analyze the criminal law response to the use of artificial intelligence as a tool for cybercrime and to formulate an appropriate criminal policy framework in the digital era. This research employs a normative approach through conceptual and systematic analysis of primary and secondary legal materials. The novelty of this study lies in emphasizing the urgency of explicit criminal law formulation that accommodates the unique characteristics of artificial intelligence-based crimes, particularly regarding criminal liability and digital evidence. The findings indicate that existing criminal regulations remain general and insufficient to address the complexities of artificial intelligence-driven cybercrime. Therefore, an adaptive and progressive criminal policy formulation is necessary to ensure effective legal protection in the digital environment.

Keywords: *Criminal Policy; Cybercrime; Artificial Intelligence; Deepfake*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa transformasi besar dalam berbagai aspek kehidupan masyarakat, termasuk dalam bidang hukum. Digitalisasi yang semakin masif tidak hanya menghadirkan kemudahan dalam mengakses dan menyebarkan informasi, tetapi juga membuka ruang bagi lahirnya berbagai bentuk kejahatan baru yang berbasis teknologi. Kejahatan siber (*cyber crime*) menjadi salah satu konsekuensi dari kemajuan tersebut, dengan karakteristik yang lintas batas, sulit dilacak, serta terus berkembang seiring dengan inovasi teknologi digital.[1]

Namun, kemajuan ini tidak hanya membawa dampak positif. AI juga membuka celah baru lagi bagi munculnya *Cyber Crime,* yaitu kejahatan yang dilakukan dengan menggunakan komputer, jaringan internet, atau perangkat digital sebagai sarana atau objek utama. Di era digital ini, *Cyber Crime* tidak hanya semakin konpleks, tetapi juga semakin sulit dideteksi dan ditindak secara hukum, terutama ketika para pelakunya memanfaatkan teknologi AI untuk mengaburkan identitas, memalsukan data, atau bahkan menjalankan kejahatan secara otomatis.[2]

Salah satu fenomena yang makin marak adalah penggunaan AI dalam *Cyber Crime.* Contohnya penipuan video "*deep learning* dan "*fake"* (*deepfake),* pelaku meniru wajah dan suara kapolres jepara, AKBP wahyu Nugroho Setyawan, melalui video call buatan AI, dimana ada dua korban asal jakarta dan yogyakarta, masing-masing ditipu sebesar Rp100.000.000,-(seratus juta rupiah) dan Rp135.000.000, -(seratus tiga puluh juta rupiah) dengan modus menawarkan mobil lelang, kasus ini terungkap pada selasa 24 desember 2024. Ada juga kasus yang serupa Cyber Crime menggunakan AI, penipuan kartu kredit dan verifikasi wajah lewat AI, dimana dua pelaku membuat rekening palsu menggunakan data identitas orang lain dan memanipulasi verifikasi wajah dengan AI, sehingga Bank menjadi korban atas kejahatan tersebut dengan adanya ribuan rekening palsu berhasil dibuka oleh pelaku, peristiwa ini terjadi antara september 2024 sampai dengan januari 2025.[2]

UU ITE merupakan bagian utama dari UU yang mengatur kejahatan siber di indonesia. Tujuan UU No. 11 Tahun 2008 tentang ITE adalah untuk menyelaraskan hukum teknologi

informasi nasional dan internasional. Selain itu, UU No. 19 tahun 2016 Tentang perubahan atas UU No. 11 Tahun 2008 bertujuan untuk memastikan bahwa hak-hak dan kebebasan orang lain diakui dan dihormati, serta untuk memenuhi tuntutan yang wajar dengan tetap memperhatikan ketertiban umum dan masalah keamanan dinegara demokrasi. UU ini juga berusaha untuk memberikan kejelasn hukum, ketertiban umum, dan keadilan. Namun, meskipun UU ITE dirancang untuk menangani berbagai bentuk kejahatan digital, penyalahgunaan teknologi deepfake sebagai alat pemerasan masih menjadi tantangan yang belum sepenuhnya terakomodasi dalam kerangka regulasi.[3]

Dari perspektif hukum pidana, penggunaan kecerdasan buatan sebagai sarana kejahatan menimbulkan tantangan serius, terutama dalam aspek perumusan norma, pertanggungjawaban pidana dan pembuktian. Sistem hukum pidana yang berlaku saat ini pada umumnya masih berorientasi pada paradigma konvensional yang menekankan pada perbuatan fisik dan hubungan kausal langsung antara pelaku dan akibat. Sementara itu, kejahatan berbasis AI sering kali melibatkan proses otomatis, anonimitas digital, serta pemanfaatan sistem algoritma yang beroprasi secara mandiri.[4]

Berbagai penelitian menunjukkan bahwa pengaturan hukum pidana yang ada masih bersifat umum dan belum secara eksplisit mengakomodasi karakteristik kejahatan siber berbasis kecerdasan buatan. Akibatnya, penegakan hukum kerap menghadapi kesulitan dalam mengkonstruksikan delik pidana, membuktikan unsur kesalahan, serta menentukan subjek yang bertanggung jawab secara pidana. Kondisi ini berpotensi menimbulkan kekosongan hukum (*legal vacum*) yang dapat dimanfaatkan oleh pelaku kejahatan untuk menghindari jerat hukum.[5]

Kesenjangan penelitian terletak pada belum optimalnya kajian mengenai bagaimana kebijakan formulasi hukum pidana seharusnya dirancang untuk merespons karakteristik kejahatan siber berbasis kecerdasan buatan yang bersifat otomatis, anonim, dan lintas yurisdiksi. Oleh karena itu, penelitian ini penting untuk menegaskan urgensi pembaruan kebijakan formulasi hukum pidana agar tetap relevan, adaptif, dan mampu memberikan kepastian hukum serta perlindungan yang efektif di ruang digital.[6]

B. METODE

Penelitian ini merupakan penelitian hukum normatif dengan spesifikasi deskriptif-analitis yang bertujuan untuk memberikan gambaran sistematis dan mendalam mengenai isu yang dikaji. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach), guna menelaah norma hukum positif serta konstruksi pemikiran hukum yang relevan. Bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder, yang diperoleh melalui studi kepustakaan. Bahan hukum primer mencakup peraturan perundang-undangan yang berkaitan dengan kejahatan siber dan pemanfaatan kecerdasan buatan, sedangkan bahan hukum sekunder meliputi literatur ilmiah, jurnal, serta doktrin hukum yang mendukung analisis. Seluruh bahan hukum tersebut dianalisis secara kualitatif dengan metode penalaran hukum yang logis dan sistematis, untuk menghasilkan pemahaman yang komprehensif mengenai kebijakan formulasi hukum pidana dalam menghadapi perkembangan kejahatan siber berbasis kecerdasan buatan.

C. PEMBAHASAN

1. Karakteristik Kejahatan Siber Berbasis Kecerdasan Buatan

Kejahatan siber berbasis kecerdasan buatan merupakan bentuk kejahatan modern yang memiliki karakteristik berbeda secara fundamental dibandingkan dengan kejahatan siber konvensional. Perbedaan tersebut terletak pada penggunaan algoritma kecerdasan buatan yang mampu meniru perilaku manusia, mempelajari pola data, serta menghasilkan konten digital yang sulit dibedakan dari realitas.[7] Salah satu manifestasi paling menonjol dari kejahatan ini adalah pemanfaatan teknologi deepfake, yang memungkinkan manipulasi audio dan visual secara realistis sehingga berpotensi menimbulkan kerugian hukum, sosial, dan psikologis bagi korban.[8]

Karakteristik utama kejahatan siber berbasis kecerdasan buatan adalah anonimasi pelaku dan sifat lintas yurisdiksi. Teknologi digital memungkinkan pelaku melakukan kejahatan tanpa kehadiran fisik serta menyamarkan identitas melalui akun palsu dan sistem otomatis. Dalam konteks deepfake, pelaku dapat menciptakan identitas digital palsu yang meyerupai individu nyata hanya dengan memanfaatkan data visual dan

suara yang tersedia di ruang publik.[9]. Kondisi ini menyebabkan kejahatan dapat dilakukan melintas batas negara tanpa hambatan geografis, sehingga menyulitkan proses penegakan hukum pidana.[10]

Selain anonimitas, kejahatan siber berbasis kecerdasan buatan juga dicirikan oleh kemampuan otomatisasi dan skalabilitas kejahatan. Teknologi AI memungkinkan pelaku menjalankan kejahatan secara massal dan berulang dengan tingkat efisiensi yang tinggi. Algoritma pembelajaran mesin dapat digunakan untuk menghasilkan konten *deepfake* dalam jumlah besar, menyesuaikan pola manipulasi terhadap target korban, serta meningkatkan efektivitas kejahatan seperti penipuan digital dan pemerasan. Hal ini menjadikan kejahatan berbasis AI memiliki dampak yang jauh lebih luas dan sistemik dibandingkan kejahatan siber konvensional.[11]

Karakteristik berikutnya adalah kemampuan manipulasi identitas digital secara realistis. Teknologi deepfake mampu meniru wajah, suara, dan ekspresi seseorang dengan tingkat presisi yang tinggi, sehingga korban sering kali kesulitan membuktikan bahwa dirinya telah dirugikan. Manipulasi identitas ini banyak dimanfaatkan dalam tindak pidana penipuan, pencemaran nama baik, dan pemerasan berbasis seksual (sextortion), yang berdampak serius terhadap reputasi dan kondisi psikologis korban.[4]

2. Keterbatasan Formulasi Hukum Pidana Saat Ini

Formulasi hukum pidana yang berlaku saat ini masih menunjukkan berbagai keterbatasan dalam merespons kejahatan siber berbasis kecerdasan buatan. Salah satu keterbatasan utama adalah tidak adanya pengaturan eksplisit mengenai kecerdasan buatan sebagai sarana kejahatan. Norma pidana yang ada cenderung hanya mengatur akibat perbuatan tanpa memperhatikan karakteristik teknologi yang digunakan.[12]

Keterbatasan berikutnya berkaitan dengan konsep pertanggungjawaban pidana. Dalam kejahatan berbasis kecerdasan buatan, proses kejahatan sering kali melibatkan sistem otomatis yang bekerja berdasarkan algoritma. Kondisi ini menimbulkan persoalan mengenai siapa yang harus dimintai pertanggungjawaban pidana, apakah pembuat sistem , pengguna, atau pihak lain yang memperoleh manfaat dari

penggunaan teknologi tersebut[7]. Hukum pidana yang masih bertumpuh pada konsep kesalahan individual (mens rea) mengalami kesulitan dalam mengakomodasi kejahatan berbasis sistem otonom.

Selain itu, keterbatasan formulasi hukum pidana juga tampak pada aspek pembuktian. Kejahatan *deepfake* menghasilkan alat bukti digital yang sangat canggih dan mudah dimanipulasi, sehingga menyulitkan aparat penegak hukum untuk membuktikan keaslian atau kepalsuan suatu konten. Sistem pembuktian pidana yang masih berorientasi pada alat bukti konvensional belum sepenuhnya didukung dengan mekanisme forensik digital yang memadai. Akibatnya, proses penegakan hukum terhadap kejahatan siber berbasis AI sering kali menghadapi hambatan teknis dan yuridis yang signifikan.[13]

3. Arah Kebijakan Formulasi Hukum Pidana di Masa Mendatang

Arah kebijakan formulasi hukum pidana di masa mendatang harus bersifat antisipatif dan adaptif terhadap perkembangan teknologi kecerdasan buatan. Formulasi norma pidana perlu secara eksplisit mengakui kecerdasan buatan sebagai sarana kejahatan siber, khususnya dalam konteks manipulasi identitas digital dan otomatisasi kejahatan.[11]

Selain itu, diperlukan pembaruan konsep pertanggungjawaban pidana yang lebih fleksibel, seperti pertanggungjawaban berbasis kontrol atau berbasis risiko, agar hukum pidana tetap efektif menjerat pelaku yang memiliki kendali atau memperoleh manfaat dari penggunaan kecerdasan buatan[14]. Penguatan sistem pembuktian digital melalui integritas forensik digital juga menjadi elemen penting dalam kebijakan formulasi hukum pidana ke depan.[15]

kebijakan formulasi hukum pidana juga harus diarahkan pada penguatan sistem pembuktian pidana berbasis digital. Kejahatan *deepfake* menghasilkan alat bukti elektronik yang sangat kompleks dan mudah dimanipulasi, sehingga memerlukan standar pembuktian yang adaptif terhadap perkembangan teknologi. Oleh karena itu, hukum pidana di masa mendatang perlu mengintegrasikan mekanisme forensik digital dan keahlian teknologi sebagai bagian yang tidak terpisahkan dari sistem pembuktian

pidana. Langkah ini penting agar aparat penegak hukum memiliki dasar hukum yang kuat dalam menilai keaslian atau kepalsuan konten digital berbasis kecerdasan buatan.

Arah kebijakan selanjutnya adalah integrasi kebijakan penal dan non-penal dalam penanggulangan kejahatan siber berbasis kecerdasan buatan. Hukum pidana tidak dapat berdiri sendiri tanpa dukungan kebijakan lain, seperti peningkatan literasi digital masyarakat, penguatan kapasitas aparat penegak hukum, serta pengembangan teknologi deteksi *deepfake*. Oleh karena itu, formulasi hukum pidana di masa mendatang harus disinergikan dengan kebijakan teknologi dan kebijakan pendidikan digital sebagai upaya pencegahan yang komprehensif.

Lebih jauh, kebijakan formulasi hukum pidana juga perlu memperhatikan dimensi perlindungan hak asasi manusia dan kepentingan publik. Pengaturan terhadap kejahatan berbasis kecerdasan buatan harus dilakukan secara proporsional agar tidak menghambat inovasi teknologi dan kebebasan berekspresi secara berlebihan. Oleh karena itu, hukum pidana di masa mendatang harus dirancang dengan pendekatan yang seimbang antara kepentingan penegakan hukum, perlindungan korban, dan penghormatan terhadap hak-hak fundamental di ruang digital.

Berdasarkan uraian tersebut, dapat ditegaskan bahwa arah kebijakan formulasi hukum pidana di masa mendatang harus berorientasi pada pembaruan normatif yang progresif dan kontekstual, dengan menjadikan kecerdasan buatan sebagai bagian integral dari perumusan tindak pidana siber. Pendekatan ini tidak hanya bertujuan untuk menutup kekosongan hukum, tetapi juga untuk memastikan bahwa hukum pidana tetap relevan, efektif, dan mampu memberikan perlindungan hukum yang optimal di tengah pesatnya perkembangan teknologi digital.

D. KESIMPULAN

Perkembangan kejahatan siber berbasis kecerdasan buatan, khususnya melalui teknologi deepfake, menunjukkan bahwa hukum pidana saat ini belum sepenuhnya mampu merespons kompleksitas dan karakteristik kejahatan digital modern. Formulasi hukum pidana masih berorientasi pada pradigma konvensional menyebabkan keterbatasan

dalam pengaturan norma, pertanggungjawaban pidan, dan pembuktian terhadap kejahatan berbasis teknologi otonom. Oleh karena itu, kebijakan formulasi hukum pidana di masa mendatang perlu diarahkan pada pembaruan normatif yang adaptif dan antisipatif dengan mengakui kecerdasan buatan sebagai sarana kejahatan siber, mengembangkan konsep pertanggungjawaban pidana yang relevan dengan sistem otomatis, serta memperkuat mekanisme pembuktian digital. Pendekatan tersebut harus disinergikan dengan kebijakan non-penal guna menjamin perlindungan hukum, kepastian hukum, dan keadilan di ruang digital tanpa menghambat perkembangan teknologi yang bertanggung jawab.

E. REFERENSI

[1] F. Richardo, M. Wanggai, M. S. Hartono, N. Putu, and E. Parwati, "Analisis Normatif terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber di Indonesia," 2026.

[2] M. Novrianto, "Kebijakan Hukum Pidana Terhadap Cyber Crime Berbasis Artificial Intelligence di Indonesia," vol. 7, no. 2, 2025.

[3] W. Z. Devi, "Implikasi Hukum terhadap Penyalahgunaan Teknologi Deepkfake untuk Pemerasan (Sextortion) dalam Perspektif Hukum Teknologi Informasi di Indonesia," vol. 3, 2026.

[4] D. Melalui, A. Inteligence, and A. I. Dari, "URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI ARTFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA Rendi," pp. 5–12, 2024.

[5] D. N. Marsudianto and E. I. Israhadi, "Uncertainty of Locus Delicti and Tempus Delicti as an Obstacle to Law Enforcement against Cybercrime," vol. 3, no. 2, pp. 114–121, 2025.

[6] A. Pertanggungjawaban and D. Hukum, "Jurnal Al Wasith: Jurnal Studi Hukum Islam || vol. 10 no. 1 (2025) €," vol. 10, no. 1, pp. 62–79, 2025.

[7] N. Mutiara, S. Hutapea, D. Kartika, C. Sitepu, and J. Damanik, "Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System," vol. 7,

no. 2, pp. 688–704, 2026, doi: 10.46924/jihk.v7i2.330.

[8] A. F. Rahmawati and Y. T. Naili, “Penguatan Literasi Digital dan Kesadaran Hukum Pidana Bagi UMKM Sebagai Kaum Rentan Terhadap Kejahatan Siber Berbasis AI di Wilayah Banyumas,” vol. 4, no. 4, 2025, doi: 10.35960/pimas.v1i2.2037.

[9] T. F. Blauth, O. J. Gstrein, and A. Zwitter, “Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI,” vol. 10, no. June, 2022.

[10] M. O. Alzwae, A. Aljahani, and Z. G. Younus, “Assessing Legislative Gaps in Qatari Law Regarding AI-Driven Misinformation : Insights from the UAE Legal Framework,” vol. 33, no. 2, pp. 396–416, 2025.

[11] B. M. Akbar, R. Yulia, M. Romdoni, F. Hukum, U. Sultan, and A. Tirtayasa, “Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana,” vol. 4, 2026.

[12] V. Mahardhika, P. Astuti, and A. Mustafa, “Yustisia Jurnal Hukum Could Artificial Intelligence be the Subject of Criminal Law ?,” vol. 12, no. 1, pp. 1–12, 2023, doi: 10.20961/yustisia.v12i1.56065.

[13] O. Novera and Y. F. Z, “Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial,” vol. 10, no. 2, pp. 460–474, 2024.

[14] J. A. Hammouri, A. Abd, A. Almahasneh, K. M. Khwaileh, and M. M. Al-raggad, “The Criminal Liability of Artificial Intelligence Entities,” vol. 22, pp. 8785–8790, 2024.

[15] N. A. Rakha, *Cybercrime and the Law : Addressing the Challenges of Digital Forensics in Criminal Investigations*, vol. XVI, no. June 2024. 2023.