JURNAL KEPASTIAN HUKUM DAN KEADILAN
Volume 7 No. 2 Desember 2025
P-ISSN: 2721-0545, E-ISSN: 2722-3604
Open Access: https://jurnal.um-palembang.ac.id/KHDK
Fakultas Hukum Universitas Muhammadiyah Palembang

Kebijakan Hukum Pidana Terhadap *Cyber Crime* Berbasis *Artificial Intelligence* di Indonesia

M. Novrianto
Fakultas Hukum Universitas Muhammadiyah Palembang

Abstract

The rapid development of Artificial Intelligence (AI) technology has had a significant impact on the dynamics of cybercrime in Indonesia. AI is being exploited by perpetrators to commit crimes using increasingly sophisticated methods, such as deepfake fraud, biometric verification manipulation, and automated cyberattacks. This phenomenon poses a serious challenge to criminal law enforcement, given that existing regulations, particularly the Criminal Code (KUHP) and the ITE Law, do not specifically address the characteristics of AI-based crimes, including legal definitions, the scope of offenses, and criminal liability mechanisms. This study aims to analyze the existing criminal law regulations, identify regulatory weaknesses, and formulate responsive criminal law policies for AI-based cybercrime in Indonesia. The research method used is normative legal research with a statutory and conceptual approach, supported by primary, secondary, and tertiary legal materials. The results of the study indicate a legal vacuum regarding the definition of AI, the division of responsibility between AI creators, operators, and users, as well as the limited capacity of law enforcement officials and digital forensic infrastructure. Therefore, a reformulation of criminal law policy is needed, including the development of specific regulations for AI cybercrime, strengthening the technical capacity of law enforcement, establishing a dedicated unit for handling high-tech digital crimes, and integrating ethical technology principles into national policy. Adaptive and comprehensive policies are expected to ensure legal certainty, public protection, and effective cybercrime mitigation in the era of artificial intelligence.

Keywords: *Criminal Law Policy, Cybercrime, Artificial Intelligence.*

Abstrak

Perkembangan pesat teknologi *Artificial Intelligence* (AI) telah membawa dampak signifikan terhadap dinamika kejahatan siber di Indonesia. AI dimanfaatkan pelaku untuk melakukan tindak pidana dengan modus yang semakin canggih, seperti penipuan deepfake, manipulasi verifikasi biometrik, hingga serangan siber otomatis. Fenomena ini menimbulkan tantangan serius dalam penegakan hukum pidana, mengingat regulasi yang ada terutama KUHP dan UU ITE belum secara spesifik mengatur karakteristik kejahatan berbasis AI, termasuk definisi yuridis, ruang lingkup delik, dan mekanisme pertanggungjawaban pidana. Penelitian ini bertujuan menganalisis pengaturan hukum pidana yang berlaku, mengidentifikasi kelemahan regulasi, serta merumuskan kebijakan hukum pidana yang responsif terhadap *Cyber Crime* berbasis AI di Indonesia. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, didukung oleh bahan hukum primer, sekunder, dan tersier. Hasil kajian menunjukkan adanya kekosongan hukum terkait definisi AI, pembagian tanggung jawab antara pembuat, operator, dan pengguna AI, serta keterbatasan kapasitas aparat penegak hukum dan infrastruktur forensik digital. Oleh karena itu, diperlukan reformulasi kebijakan hukum pidana yang mencakup penyusunan regulasi khusus AI *Cyber Crime*, penguatan kapasitas teknis aparat, pembentukan unit khusus penanganan kejahatan digital berbasis teknologi tinggi, dan integrasi prinsip etika teknologi dalam kebijakan nasional. Kebijakan yang adaptif dan komprehensif diharapkan mampu menjamin kepastian hukum, perlindungan masyarakat, serta efektivitas penanggulangan kejahatan siber di era kecerdasan buatan.

Kata Kunci: Kebijakan Hukum Pidana, *Cyber Crime, Artificial Intelligence.*

Info Artikel

Masuk: 10 Agustus 2025, Diterima: 8 Oktober 2025, Terbit: 23 Desember 2025

Email Corresponding Author:
Nama Author : mnovriantonovrianto28@gmail.com

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan besar terhadap tatanan kehidupan masyarakat global, termasuk di Indonesia. Perubahan ini ditandai dengan meluasnya penggunaan internet, perangkat digital, serta sistem berbasis *Artificial Intelligence* (AI) dalam berbagai bidang kehidupan manusia mulai

dari pendidikan, bisnis, kesehatan, hingga pemerintahan dan interaksi sosial sehari-hari.

Namun, kemajuan ini tidak hanya membawa dampak positif. AI juga membuka celah baru 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 kompleks, 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[1].

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 lima juta rupiah) dengan modus menawarkan mobil lelang, Kasus ini terungkap pada Selasa 24 desember 2024.[2] 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.[3]

---

[1] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Prenada Media, 2010, hlm. 76.

[2] Penipuan Canggih, Gunakan AI Tiru Wajah dan Suara Kapolres Jepara Korban Rugi Ratusan Juta, 25 Desember 2024, diakses melalui: https://suarabaru.id/2024/12/25/penipuan-canggih-gunakan-ai-tiru-wajah-dan-suara-kapolres-jepara-korban-rugi-ratusan-juta pada tanggal 18 juni 2025.

[3] Modus Baru Penipuan Kartu Kredit dengan Aplikasi AI, 2 Pelaku Ditangkap, 07 Feb 2025, diakses melalui: https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap pada tanggal 18 juni 2025.

Dengan pesatnya kemajuan teknologi, pelaku kejahatan kini semakin mudah memanfaatkan AI untuk melancarkan aksinya. Teknologi seperti *deepfake* digunakan untuk menyebarkan disinformasi secara masif dan meyakinkan, algoritma pembelajaran mesin dimanfaatkan untuk mencuri data pribadi melalui teknik rekayasa sosial yang canggih, *botnet* berbasis AI mampu melancarkan serangan *Distributed Denial of Service (DDoS)*[4] secara otomatis dan terkoordinasi bahkan *malicious software (malware)* [5] yang digerakkan oleh AI dapat terus belajar dan beradaptasi agar lolos dari sistem deteksi keamanan. Jenis-jenis kejahatan ini tidak hanya mengancam privasi dan keamanan data individu, tetapi juga berpotensi mengganggu stabilitas nasional dan tatanan hukum.[6]

Indonesia sebagai negara hukum berdasarkan Pasal 1 ayat (3) Undang-Undang Dasar 1945, memiliki kewajiban untuk menjamin kepastian hukum dan keamanan masyarakat, termasuk dalam ranah digital. Namun, dalam praktiknya, penegakan hukum terhadap kejahatan siber berbasis AI menghadapi berbagai tantangan. Di antaranya adalah kerangka hukum yang belum responsif terhadap perkembangan AI, minimnya pemahaman aparat

[4] "Serangan *Distributed Denial of Service* (DDoS) adalah salah satu permasalahan besar dalam kemanan jaringan yang menyebabkan services yang ada pada jaringan menjadi tidak dapat diakses dalam jangka waktu tertentu". Lihat: Yeni Yanti, dkk., "Deteksi Serangan *Distributed Deniel of Service* Pada Jaringan Sensor Nirkabel Menggunakan *Support Vector Machine*, *G-Tech: Jurnal Teknologi Terapan,* Vol. 8 No. 4 oktober 2024, hlm. 2688. Diakses melalui: https://jurnal.untan.ac.id/index.php/jepin/article/view/28214/75676581121

[5] "*Malicious Software* atau yang biasa disebut *malware* yang merupakan suatu program jahat, Beragam tujuan yang dimiliki para pelaku ini beberapa diantaranya adalah untuk melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi". Lihat: Aldy Putra Aldya, "*Reverse Engineering* untuk Analisis *Malware Remote Access Trojan", JEPIN (Jurnal Edukasi dan Penelitian Informatika),* Vol. 5 No. 1, April 2019, hlm. 40. diakses melalui; https://ejournal.uniramalang.ac.id/g-tech/article/view/5428/3380

[6] Raihani Latifatunnisa, Made Wira Yudha, "Urgensi Pembaruan Regulasi Dalam Menanggulangi Penyalahgunaan Teknologi *Artificial Intelligence* Dan *Deepfake* Di Indonesia: Perspektif Perlindungan Hak Privasi", *Jurnal Hukum dan Kewarganegaraan,* Vol. 11 No. 1 tahun 2025, diakses melalui: https://ejournal.warunayama.org/index.php/causa/article/view/11617,

hukum terhadap teknologi baru, serta keterbatasan alat bukti digital dan sumber daya forensik digital.[7]

Saat ini, penanganan tindak pidana *cyber* di Indonesia merujuk pada beberapa reg ulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan semua perubahannya, serta Kitab Undang-Undang Hukum Pidana (KUHP), Namun, regulasi tersebut tidak secara eksplisit mengatur bentuk-bentuk kejahatan yang dilakukan dengan bantuan atau berbasis AI.[8]

Ketiadaan norma hukum yang spesifik membuat banyak kejahatan digital modern luput dari jerat hukum atau sulit dijerat dengan tepat. Selain itu, pembuktian dalam kasus *Cyber Crime* berbasis AI menjadi tantangan tersendiri. [9] Hal ini lah yang menjadi kegelisahan akademik penulis, bagaimana menetapkan tanggung jawab pidana apabila kejahatan dilakukan oleh AI dengan tingkat otonomi tinggi, selanjutnya apakah yang bertanggung jawab itu adalah *programmer*, operator, atau sistem itu sendiri.

Secara filosofis, hukum harus menjamin asas keadilan, kepastian, dan kemanfaatan sebagaimana dikemukakan Gustav Radbruch. Ketika hukum tidak mampu menjawab tantangan teknologi, maka ketiga nilai ini akan sulit diwujudkan. Apalagi jika AI digunakan untuk melakukan kejahatan yang sulit dilacak pelakunya, maka keadilan bagi korban pun menjadi semakin jauh dari harapan.

Secara yuridis, prinsip dasar dalam hukum pidana adalah adanya subjek hukum yang bertanggung jawab atas perbuatan pidana. Dalam konteks AI, terjadi kekaburan antara tindakan manusia dan tindakan mesin. Hal ini menjadi diskursus penting dalam kajian hukum kontemporer, bahwa

---

[7] Nurul Aini, Fauziah Lubis, "Tantangan Pembuktian Dalam Kasus Kejahatan Siber", *Jurnal Hukum,* Vol. 5 No. 02 tahun 2024 hlm. 56, diakses melalui https://journal.cattleyadf.org/index.php/Judge/article/view/566/433,

[8] Abdul Wahid dan Mohammad Labib, *Kejahatan Siber (Cyber Crime)*, Refika Aditama, 2005, hlm. 114.

[9] Yusep Mulyana, "Sosialisasi Implikasi Hukum Penggunaan Artificial Intellegence Dalam Tindak Pidana Cyber Crime Di Kabupaten Garu", *Besiru Jurnal Pengabdian Masyarakat,* Vol. 1 No. 11 tahun 2024, diakses melalui https://manggalajournal.org/index.php/BESIRU/article/view/508/661,

pergeseran teknologi menuntut reformulasi terhadap prinsip-prinsip hukum tradisional[10].

Sementara itu, dari sudut pandang internasional, sejumlah negara dan organisasi mulai menyusun kerangka hukum yang mengatur penggunaan AI dalam konteks pidana. Uni Eropa, misalnya, telah menyusun *Artificial Intelligence Act* sebagai langkah preventif terhadap potensi penyalahgunaan AI[11]. Di Indonesia, diskusi mengenai regulasi AI masih bersifat normatif dan belum terimplementasi dalam kebijakan konkret yang mengatur aspek pidana.

Data dari Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa sepanjang tahun 2023, terdapat lebih dari 300 juta serangan siber yang terdeteksi di Indonesia[12]. Sebagian besar dari serangan tersebut diduga menggunakan teknologi otomatisasi dan AI. Sayangnya, dari sekian banyak kasus, hanya sebagian kecil yang berhasil ditindak secara hukum. Ini menunjukkan adanya jurang antara dinamika kejahatan digital dan kemampuan negara dalam meresponsnya melalui instrumen hukum.

Kajian ini menjadi semakin penting ketika kita memahami bahwa hukum tidak hanya sebagai alat kontrol sosial *(social control),* tetapi juga sebagai instrumen perlindungan hak-hak dasar warga negara. Tanpa kejelasan hukum terhadap kejahatan berbasis AI, masyarakat berada dalam ketidakpastian hukum, dan negara kehilangan kendali atas keamanan digital nasional.

Berdasarkan uraian tersebut diatas, maka rumusan masalah penelitian ini, yaitu:

---

[10] Annie Long Ashton, *et.al*, "Penegakan Hukum Terhadap Peran Artificial Intelligence di Indonesia", *Jurnal Analogi Hukum*, Vol. 6 Issue 3 tahun 2024, diakses melalui : https://ejournal.warmadewa.ac.id/index.php/analogihukum/article/view/11551/6465,

[11] *European Commission*, *Proposal for a Regulation of The European Parliament and Of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, 2021. Diakses melalui : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206, pada tanggal 18 juni 2025.

[12] BSSN, *Laporan Tahunan Statistik Keamanan Siber Indonesia*, 2023. Diakses melalui: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-023.pdf, pada tanggal 18 juni 2025.

1. Bagaimana Pengaturan Hukum Pidana terhadap Tindak Pidana *Cyber Crime* berbasis *Artificial Intelligence* di Indonesia?
2. Bagaimana Kebijakan Hukum Pidana dalam Menanggulangi *Cyber Crime* berbasis *Artificial Intelligence* di Indonesia yang Akan Datang?

B. METODE

Metode penelitian yang digunakan adalah penelitian hukum normatif, yaitu penelitian yang bertujuan menemukan kebenaran berdasarkan logika keilmuan hukum melalui penelaahan norma, asas, dan doktrin hukum. Penelitian ini memanfaatkan pendekatan konseptual dan pendekatan perundang-undangan untuk memahami konsep serta regulasi yang berkaitan dengan penegakan hukum pidana terhadap *Cyber Crime* berbasis AI di Indonesia. Sumber bahan penelitian terdiri dari bahan hukum primer seperti Pancasila, UUD 1945, KUHP, dan UU ITE; bahan hukum sekunder berupa publikasi dan kajian hukum; serta bahan hukum tersier seperti kamus dan ensiklopedia. Pengumpulan bahan dilakukan melalui studi kepustakaan dan penelusuran dokumen, kemudian diolah melalui proses sistematisasi berdasarkan tataran teknis, teleologis, dan sistematisasi eksternal.

Teknik pengolahan dilakukan melalui inventarisasi dan penyusunan sistematis peraturan perundang-undangan yang relevan, sedangkan teknik analisis menggunakan analisis kualitatif dengan mengaitkan bahan yang dihimpun dengan teori hukum dan penerapan dalam peraturan perundang-undangan. Kesimpulan penelitian ditarik dengan metode berpikir deduktif, yaitu berangkat dari pemahaman umum mengenai konsep dan kerangka hukum kemudian merumuskan kesimpulan khusus terkait kebijakan hukum pidana dalam menanggulangi *Cyber Crime* berbasis AI di Indonesia.

C. HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Pidana terhadap Tindak Pidana *Cyber Crime* Berbasis *Artificial Intelligence* di Indonesia

Secara normatif, instrumen hukum pidana yang berlaku di Indonesia untuk menindak *Cyber Crime* masih mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-

Undang Nomor 1 Tahun 2024. Regulasi ini telah memberikan dasar hukum untuk menindak kejahatan yang menggunakan komputer dan jaringan internet.

Meski instrumen ini memberikan dasar hukum terhadap tindak pidana *cyber*, namun terdapat kelemahan mendasar dan belum menyentuh secara spesifik karakteristik kejahatan yang dilakukan melalui atau dengan bantuan AI, yaitu:

a. Kekosongan definisi dan norma

1) Definisi AI belum tersedia.

Ketiadaan definisi yuridis yang jelas tentang apa yang dimaksud dengan AI menjadi hambatan utama dalam merumuskan hukum yang efektif, terutama dalam hukum pidana. Tanpa batasan yang jelas, sulit bagi penegak hukum untuk menerapkan norma-norma yang ada.

Menurut penulis ada beberapa aspek yang menjelaskan mengapa ketiadaan definisi yuridis ini menjadi masalah: *Pertama,* Unsur Delik *(Corpus Delicti).* Dalam hukum pidana, unsur delik adalah fakta-fakta yang harus dibuktikan untuk menunjukkan bahwa suatu kejahatan telah terjadi. Tanpa definisi AI yang jelas, sulit untuk menentukan kapan suatu tindakan yang melibatkan AI dapat dianggap sebagai "tindakan kriminal". Ketiadaan definisi yang jelas membuat penentuan subjek hukum, objek hukum, dan perbuatan yang dilarang menjadi kabur. *Kedua,* Niat Jahat *(Mens Rea).* Mens rea adalah unsur psikologis dalam suatu tindak pidana, yang mengacu pada niat atau keadaan mental pelaku. Konsep ini menjadi sangat problematis dalam konteks AI karena: AI tidak memiliki kesadaran, niat, atau kehendak. AI beroperasi berdasarkan algoritma dan data yang diberikan. Bagaimana kita bisa membuktikan bahwa sebuah program memiliki niat jahat untuk melakukan sesuatu?. Hukum pidana tradisional mengasumsikan bahwa pelaku adalah manusia yang memiliki akal budi dan kehendak bebas. Asumsi ini tidak berlaku pada AI. Akibatnya, penegak hukum harus mencari "niat jahat" pada pencipta AI, *programmer,* atau pengguna, yang mungkin tidak memiliki niat jahat secara langsung.

Ketiga, Standar Pembuktian. Standar pembuktian adalah tingkat keyakinan yang diperlukan bagi hakim untuk memutuskan suatu perkara. Dalam kasus yang melibatkan AI, standar ini menjadi sulit diterapkan karena: Banyak model AI, Kausalitas yang tidak jelas.

Untuk mengatasi masalah ini menurut penulis, diperlukan kolaborasi yang erat antara ahli hukum, pembuat kebijakan, dan ahli teknologi. Karena beberapa negara dan organisasi internasional sudah mulai merancang kerangka hukum yang mencoba mendefinisikan AI berdasarkan fungsinya, risikonya, atau tingkat otonominya.[13] Pendekatan ini mungkin lebih pragmatis dari pada mencoba memberikan satu definisi tunggal yang mencakup semua jenis AI.

2) AI sebagai "alat" atau "subjek" hukum.

Dalam ranah hukum pidana tradisional, subjek hukum yang dapat dimintai pertanggungjawaban pada prinsipnya adalah manusia *(natuurlijk persoon)* sebagai pelaku yang memiliki kesadaran dan kehendak *(mens rea)* dalam melakukan suatu perbuatan. Konsep ini sejalan dengan *asas nulla poena sine culpa,* yang mengandaikan adanya kesalahan yang dapat diatribusikan pada subjek hukum tersebut. Namun, dengan semakin otonomnya sistem AI yang mampu mengambil keputusan, melakukan prediksi, bahkan melakukan tindakan kompleks tanpa intervensi langsung manusia muncul pergeseran paradigma tentang bagaimana hukum harus memandang dan menanggapi akibat yang ditimbulkan oleh AI.

Pergeseran ini menimbulkan perdebatan mendasar: apakah AI yang beroperasi secara *self-learning* atau *autonomous* dapat dianggap sebagai subjek hukum yang berdiri sendiri *(electronic person),* ataukah tetap harus dipandang sebagai "alat" *(tool)* dari manusia atau badan hukum yang mengoperasikannya. Di satu sisi, atribusi tanggung jawab penuh kepada manusia atau korporasi berpotensi mengabaikan kompleksitas pengambilan

[13] Eka Nanda Ravizki dan Lintang Yudhantaka, "*Artificial Intelligence* Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia", *Notaire Journal of notarial law,* Vol. 5 No. 3 Oktober 2022, hlm. 353. Diakses melalui https://e-journal.unair.ac.id/NTR/article/view/39063

keputusan AI yang dapat bersifat *black box* dan tidak sepenuhnya dapat diprediksi. Di sisi lain, pemberian status subjek hukum pada AI menimbulkan tantangan filosofis, yuridis, dan praktis, mengingat AI tidak memiliki kesadaran moral, perasaan bersalah, atau kemampuan untuk menjalani hukuman dalam arti tradisional.

Dilema inilah yang mendorong perlunya rekonstruksi kerangka hukum pidana agar mampu merespons perkembangan teknologi, termasuk melalui pengaturan mekanisme pertanggungjawaban pidana yang adaptif, proporsional, dan tetap menjamin kepastian hukum serta perlindungan terhadap korban.

b. Keterbatasan cakupan delik

Pasal-pasal yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 pada dasarnya masih berfokus pada bentuk-bentuk *conventional Cyber Crime,* seperti akses ilegal *(illegal access),* intersepsi tanpa hak *(illegal interception),* manipulasi data *(data interference),* dan penyebaran konten yang dilarang. Rumusan delik yang ada belum secara eksplisit mengantisipasi perkembangan modus kejahatan siber berbasisAI*(AI-generated crime),* seperti *synthetic identity fraud* yakni penciptaan identitas palsu yang kompleks dan realistis menggunakan teknologi *machine learning* atau pemanfaatan AI untuk melakukan adaptive *Distributed Denial of Service (DDoS) attacks* yang mampu menyesuaikan pola serangan secara dinamis guna menghindari deteksi sistem keamanan.

Keterbatasan ini menimbulkan kesenjangan regulasi karena karakteristik *AI-generated crime* sering kali tidak dapat dipetakan langsung pada unsur-unsur tindak pidana yang sudah ada dalam UU ITE. Akibatnya, aparat penegak hukum dihadapkan pada tantangan dalam pembuktian, khususnya terkait mens rea dan pertanggungjawaban pidana ketika pelaku memanfaatkan sistem AI yang bekerja secara otonom. Hal ini mengindikasikan bahwa pembaruan regulasi diperlukan agar hukum pidana

nasional mampu mengakomodasi fenomena kejahatan siber generasi baru, yang bersifat adaptif, otonom, dan *self-learning*.

Dari sudut pandang penulis, hal ini menunjukkan bahwa Pengaturan hukum pidana yang ada masih belum memadai secara substansi dan teknis dalam menjawab kompleksitas *Cyber Crime* berbasis AI. Kekosongan hukum muncul karena sistem hukum Indonesia belum mengantisipasi perkembangan teknologi digital yang sangat cepat, khususnya dalam hal subjek hukum, pertanggungjawaban pidana, dan model pencegahan kejahatan digital yang menggunakan AI sebagai alat atau actor.

Oleh karena itu, menurut penulis, diperlukan reformulasi kebijakan hukum pidana yang meliputi Penyusunan regulasi baru atau revisi UU ITE yang secara eksplisit mengatur tindak pidana dengan keterlibatan AI. Penguatan kapasitas aparat penegak hukum dalam memahami teknologi AI dan cara kerjanya dalam *Cyber Crime*. Dengan langkah-langkah tersebut, kebijakan hukum pidana diharapkan dapat lebih adaptif, komprehensif, dan efektif dalam menghadapi ancaman baru dari *Cyber Crime* berbasis AI di era transformasi digital.

2. Kebijakan Hukum Pidana dalam Menanggulangi *Cyber Crime* Berbasis *Artificial Intelligence* di Indonesia yang Akan Datang

Regulasi hukum pidana mengenai penanggulangan *Cyber Crime* khususunya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi instrumen utama yang sangat penting. Namun, meskipun undang-undang sudah ada, tetapi pelaksanaannya belum mampu mengakomodir permasalahan yang ada. Beberapa keterbatasan dalam hukum positif dalam rangka penanggulangan *Cyber Crime* berbasis AI diantaranya ialah:

a. Ketiadaan regulasi khususnya *AI Cyber Crime*
b. Definisi dan ruang lingkup *Cyber Crime* dalam UU ITE cenderung bersifat umum, sehingga belum mampu mencakup kejahatan berbasis AI
c. Kurangnya kapasitas kemampuan aparat penegak hukum khususnya berkaitan dengan identifikasi dan penanganan *Cyber Crime* berbasis kecerdasan buatan.

Pembaharuan kebijakan hukum mengenai penanggulangan kejahatan siber dengan basis AI saat ini sangat mendesak. Hal ini tentunya disebabkan karena adanya kekosongan hukum di mana belum ada regulasi yang mengatur secara detail dan rinci mengenai permasalahan *Cyber Crime* berbasis AI di Indonesia. Kekosongan hukum yang mengatur mengenai AI di Indonesia ini khususnya yang berkaitan dengan kedudukan tanggung jawab AI dalam industri hukum di Indonesia. Kekosongan hukum dalam bidang AI inilah yang menyebabkan banyak praktisi hukum masih memanfaatkan pengaturan yang berkaitan dengan regulasi bidang teknologi untuk menanggapi permasalahan di bidang kecerdasan buatan, salah satunya melalui UU ITE.[14]

Berdasarkan permasalahan kekosongan hukum di bidang AI, perlu antisipasi dari segala kemungkinan yang bisa muncul akibat kurangnya regulasi di bidang AI. Dalam regulasi baru ini nantinya diharapkan ada pertimbangan yang rinci dan jelas berkaitan dengan kedudukan AI dalam pertanggungjawaban hukum. Secara eksplisit, AI memang dapat melakukan perbuatan hukum layaknya subjek hukum yang ada. Namun dalam praktiknya, AI merupakan sistem yang dibangun manusia dan tidak dapat berperan sebagai subjek hukum. Oleh sebab itulah diperlukan adanya penafsiran secara terperinci dalam regulasi hukum baru yang mengatur secara jelas mengenai kecerdasan buatan, khususnya dalam rangka penanggulangan kejahatan siber berbasis AI dalam hukum Indonesia.

Seperti yang diketahui bersama, AI kedudukannya masih sangat kabur di Indonesia. UU ITE dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi, diamana dua produk hukum ini pun tidak menyebutkan AI secara jelas, hanya diksi "Agen Elektronik" saja yang dijelaskan dalam kedua peraturan tersebut.

Regulasi mengenai AI belum diatur dalam KUHP Nasional UU No 1 tahun 2023. Dalam KUHP Nasional UU No 1 tahun 2023, yang diatur

[14] Ni Made Yordha Ayu Astiti. "*Strict Llliability of Artificial Intelegence*: Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban". *Jurnal Magister Hukum Udayana.* Vol. 12, No. 4, Desember 2023, hlm. 969.

hanyalah mengenai kejahatan siber atau *Cyber Crime* saja. Namun instrumen *Cyber Crime* dalam KUHP Nasional UU No 1 tahun 2023 yang sudah disusun juga sangat penting sebagai salah satu instrumen hukum yang mengatur kejahatan dengan menggunakan media teknologi dan internet. Regulasi baru dalam menghadapi *Cyber Crime* dalam KUHP Nasional UU No 1 tahun 2023 diantaranya seperti *hacking*, pencurian data, hingga penyebaran *malware*. Ini menunjukkan bahwa Undang-Undang Nomor 1 Tahun 2024 memiliki landasan hukum yang lebih kuat dibandingkan regulasi sebelumnya dengan menjelaskan unsur-unsur tindak pidana secara lebih rinci.[15]

Pasal-pasal dalam undang-undang tersebut mencakup berbagai *Cyber Crime*, termasuk akses ilegal dalam Pasal 32, serangan terhadap sistem informasi negara dalam Pasal 33, hingga pelanggaran pada sistem keuangan dan perbankan dalam Pasal 34. Sanksi yang ditetapkan tergolong berat, baik dalam bentuk pidana penjara hingga denda besar, guna menciptakan efek jera. Sebagai contoh, akses ilegal yang melibatkan pelanggaran sistem pengamanan dapat dipidana hingga 8 tahun, sementara pelanggaran yang berkaitan dengan informasi rahasia pemerintah dapat mencapai hukuman penjara 12 tahun.

Penelitian ini menyoroti bahwa regulasi dalam Undang-Undang Nomor 1 Tahun 2024 dirancang untuk menghadapi kompleksitas dan dinamika *Cyber Crime* yang terus berkembang. Selain itu, perlindungan terhadap sektor keuangan dan perbankan juga diperkuat melalui sanksi yang signifikan. Analisis yuridis menunjukkan bahwa undang-undang ini memberikan landasan hukum yang lebih jelas untuk menangani *Cyber Crime* yang memiliki sifat lintas batas dan berkembang pesat. Ini artinya bahwa UU No. 1 tahun 2023 yang direncanakan akan segera berlaku telah memberikan kerangka hukum yang lebih komprehensif dalam melindungi masyarakat dari *Cyber Crime*. Dengan revisi dan reformasi hukum yang berkelanjutan, regulasi ini diharapkan mampu mengikuti perkembangan teknologi dan

[15] Yosua Hia. "Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)". *Jurnal SELISIK.* Vol. 10, No. 1, Juni 2024, hlm. 158.

modus kejahatan modern, sehingga menciptakan lingkungan digital yang lebih aman di Indonesia.

Kehadiran Undang-Undang Nomor 1 Tahun 2024 yang mengatur *Cyber Crime* secara komprehensif menjadi pijakan penting untuk pengembangan regulasi di masa depan, khususnya dalam menghadapi tantangan baru terkait kejahatan yang melibatkan AI. Dengan pesatnya perkembangan teknologi AI, modus operandi *Cyber Crime* semakin kompleks, mulai dari serangan otomatis melalui bot hingga manipulasi data menggunakan algoritma cerdas. Dalam konteks ini, pembaharuan hukum positif menjadi sangat mendesak agar sistem hukum dapat mengantisipasi dan menanggulangi ancaman yang muncul.

Urgensi pembaharuan regulasi terkait AI dalam *Cyber Crime* terletak pada kemampuan teknologi ini untuk mempercepat, memperluas, dan menyembunyikan jejak kejahatan. AI dapat digunakan untuk menciptakan *malware* adaptif, *deepfake,* hingga manipulasi data yang sangat sulit dideteksi. Dalam hukum positif yang ada, seperti UU ITE atau KUHP baru, belum ada pengaturan eksplisit mengenai penggunaan AI untuk tujuan kriminal. Hal ini menciptakan kekosongan hukum yang dapat dimanfaatkan oleh pelaku kejahatan. Oleh karena itu, revisi regulasi yang ada harus memasukkan elemen- elemen spesifik tentang AI dalam tindak pidana *cyber*.

Pembaharuan yang diperlukan meliputi penambahan ketentuan mengenai kejahatan yang melibatkan pengembangan, penggunaan, atau distribusi teknologi AI untuk tujuan ilegal. Misalnya, regulasi perlu mengatur secara khusus tentang pembuatan *Deepfake* untuk penipuan, penggunaan AI untuk serangan pada infrastruktur kritis, dan manipulasi pasar melalui algoritma cerdas. Selain itu, penting untuk mendefinisikan tanggung jawab hukum bagi pengembang dan pengguna AI yang tidak bertanggung jawab, termasuk mekanisme audit algoritma dan sanksi pidana yang sesuai.

Gambaran pembaharuan hukum juga harus mencakup kolaborasi internasional, mengingat sifat lintas batas dari *Cyber Crime* berbasis AI. Indonesia dapat belajar dari negara-negara lain yang telah mulai mengatur

teknologi ini, seperti Uni Eropa dengan *Artificial Intelligence Act* atau pendekatan Amerika Serikat melalui undang-undang yang mengatur keamanan data berbasis AI. Pembaharuan hukum di Indonesia harus menekankan pada integrasi standar global, pemantauan algoritma, dan pengembangan kapasitas penegak hukum untuk menangani kasus AI *Cyber Crime*. Dengan pembaharuan ini, sistem hukum Indonesia tidak hanya menjadi responsif terhadap tantangan teknologi modern, tetapi juga menciptakan kerangka hukum yang adil dan relevan. Hal ini sejalan dengan tujuan Undang-Undang Nomor 1 Tahun 2024, yaitu memberikan perlindungan hukum yang lebih kuat bagi masyarakat di era digital. Langkah ini juga mencerminkan visi hukum progresif yang tidak hanya bereaksi terhadap ancaman, tetapi juga proaktif dalam menciptakan ruang digital yang aman dan adil.

Meskipun pengaturan mengenai *Cyber Crime* telah ada dan dibuat mengenai *Cyber Crime* dalam KUHP Nasional UU No 1 tahun 2023. Namun hal tersebut tidak membuat AI tidak perlu dibuatkan regulasinya. Produk hukum undang- undang dan turunannya tetap diperlukan hadir dalam mengatur AI *Cyber Crime*. Kekosongan hukum yang saat ini terjadi sangat berdampak terhadap penegakan hukum dan upaya preventif yang bisa dilakukan oleh pemerintah, penegak hukum, serta praktisi hukum. Kekosongan hukum juga dikhawatirkan dapat menyebabkan terjadinya peningkatan angka penyalahgunaan AI untuk berbagai jenis *Cyber Crime* dan kejahatan lainnya di Indonesia. Oleh sebab itulah diperlukan rekonstruksi hukum yang bertujuan menghadirkan pembaharuan hukum pidana yang mengatur secara jelas, rinci, dan lengkap mengenai AI dan penegakan hukumnya.

Berdasarkan penjelasan di atas dan dengan melihat fakta hukum dan fakta dalam masyarakat yang saat ini terjadi, terdapat beberapa rekomendasi hukum untuk melakukan pembaharuan hukum penanggulangan *Cyber Crime* berbasis AI khususnya di wilayah hukum Indonesia. Pembaharuan hukum dan tindakan yang dapat dilakukan secepatnya antara lain sebagai berikut:

a. Pembentukan Undang-Undang *Artificial Intelegence*

b. Revisi Undang-Undang Informasi dan Transaksi Elektronik
c. Peningkatan Teknologi Forensik Digital
d. Kerja Sama Internasional
e. Penguatan Edukasi dan Literasi Digital

Rekomendasi di atas dapat dituangkan dalam kebijakan-kebijakan pemerintah baik melalui pembaharuan hukum dan peraturan perundang-undangan maupun melalui program pemerintah. Tujuan dari dilakukannya tindakan dan pembaharuan hukum terhadap penanggulangan dan penegakan hukum *Cyber Crime* berbasis AI di atas pada dasarnya ialah untuk menciptakan regulasi yang adaptif dengan perkembangan teknologi yang semakin maju di tengah-tengah masyarakat saat ini. Dengan langkah-langkah di atas, harapannya Indonesia akan semakin melek dengan perkembangan teknologi yang terjadi serta mampu mengatasi dan menanggulangi *Cyber Crime* berbasis AI yang semakin banyak kejadiannya.

Dalam rangka menangani dan menegakkan hukum *Cyber Crime* berbasis AI di Indonesia, pemerintah diharapkan dapat segera membentuk regulasi yang secara khusus mengatur mengenai hal tersebut. Jika didasarkan atas permasalahan yang ada, perlu Undang-Undang tentang Penggunaan dan Pengawasan AI dalam sistem hukum nasional Indonesia. Dibuatnya peraturan perundang-undangan ini bertujuan sebagai landasan hukum dan pondasi penting dalam penanganan dan penegakkan hukum *Cyber Crime* berbasis AI di Indonesia yang saat ini belum diatur. Dengan dibentuknya Undang-Undang tentang Penggunaan dan Pengawasan AI diharapkan akan ada landasan hukum yang kuat dalam pengaturan pengembangan, penggunaan, serta pengawasan teknologi AI sekaligus penanggulangan potensi adanya penyalahgunaan AI untuk membantu manusia melakukan kejahatan.

Undang-Undang tentang Penggunaan dan Pengawasan AI juga diharapkan mencakup berbagai aspek penting. Beberapa aspek penting yang diharapkan diatur dalam undang-undang ini diantaranya ialah:

1) Ketentuan umum

Ketentuan umum berfungi untuk mendefinisikan konsep utama dari *Cyber Crime* dengan basis AI, ruang lingkup kejahatan siber berbasis AI, dan hal-hal lain dalam bidang AI yang masih membutuhkan definisi secara lebih jelas untuk menghindari kontradiksi dalam memahami AI dan undang-undang ini.

2) Prinsip-Prinsip Penggunaan AI

Pengaturan mengenai prinsip penggunaan AI di sini termasuk juga pengaturan mengenai sertifikasi teknologi AI bagi pengembang atau *Developer* sistem. Selain itu, pengaturan mengenai tanggung jawab hukum penyalahgunaan dan kejahatan dengan AI juga harus dibuat. Tujuannya ialah untuk memastikan sistem AI yang dibuat oleh pengembang dapat berjalan dengan baik, aman digunakan, serta dapat diminimalisir kemungkinannya digunakan untuk berbuat kejahatan.

3) Pengawasan terhadap Teknologi AI

Pengawasan pengembangan dan penggunaan AI harus dilakukan dengan membentuk lembaga khusus yang bertugas melakukan audit secara berkala dalam rangka memastikan AI yang dibuat dapat dijalankan dengan baik dan sesuai dengan etika hukum dan norma hukum yang dibuat. Keberadaan lembaga pengawas juga penting guna memberikan perlindungan data pribadi masyarakat pengguna sistem, aplikasi, atau piranti yang menggunakan kecerdasan buatan, serta evaluasi terhadap risiko keamanan kecerdasan buatan.

4) Rincian Jenis-Jenis Kejahatan Siber Berbasis AI

Undang-Undang tentang Penggunaan dan Pengawasan AI perlu merinci secara jelas mengenai jenis-jenis kejahatan siber berbasis kecerdasan buatan, seperti pembuatan *deepfake* dalam modus kejahatan penipuan atau pembuatan *malware* dengan memenfaatkan AI, serta lain sebagainya.

5) Sanksi atau Hukuman bagi Pihak yang Menyalahgunakan AI

Sebagai salah instrumen hukum pidana, tentunya Undang-Undang tentang Penggunaan dan Pengawasan AI juga harus mengatur jenis hukuman dan sanksi yang diberikan kepada pihak-pihak yang menyalahgunakan AI untuk melakukan kejahatan siber dan kejahatan lainnya.

6) Pencegahan dan Penanggulangan *Cyber Crime*

Dalam bidang pencegahan dan penanggulangan kejahatan siber berbasis AI ini diperlukan pengaturan secara jelas mengenai tanggung jawab perusahaan penyedia layanan AI jika terjadi penyalahgunaan atau kegagalan dalam mengamakan produk yang dibuatnya.

7) Literasi dan Edukasi Digital

Perlu dilakukan pendidikan, pelatihan, ataupun kampanye mengenai pemanfaatan AI dalam kehidupan sehari-hari. Bukan hanya itu, dalam edukasi juga perlu disampaikan mengenai penyalahgunaan AI dan penanggulangannya agar masyarakat tidak menjadi pelaku ataupun korban dari *Cyber Crime* berbasis AI yang semakin marak.

Pemerintah Indonesia harus bertindak proaktif dan strategis dalam menghadapi ancaman ini. Langkah pertama adalah meningkatkan kapasitas literasi digital masyarakat. Kampanye edukasi tentang risiko teknologi AI dan cara mengenali ancaman siber harus dilakukan secara luas untuk memperkuat ketahanan masyarakat terhadap serangan. Selanjutnya, pemerintah perlu memperkuat infrastruktur keamanan siber nasional. Pembentukan pusat komando khusus yang memanfaatkan teknologi AI untuk mendeteksi dan merespons ancaman secara *real-time* menjadi kebutuhan mendesak. Kolaborasi dengan sektor swasta dan pakar teknologi juga diperlukan untuk memastikan pertahanan siber yang komprehensif.

Kerangka hukum yang baik untuk menanggulangi *Cyber Crime* berbasis AI harus mencakup tiga aspek utama: regulasi preventif, penegakan hukum yang efektif, dan perlindungan hak-hak masyarakat. Pertama, regulasi preventif harus mencakup kewajiban bagi pengembang AI untuk memastikan teknologi mereka tidak disalahgunakan. Misalnya, pemerintah dapat mengadopsi pendekatan Uni Eropa yang mewajibkan audit risiko sebelum AI diluncurkan ke pasar. Aturan ini dapat mencakup ketentuan mengenai transparansi algoritma, pengujian keamanan, dan kewajiban pelaporan insiden.

Kedua, kerangka hukum harus memberikan wewenang yang jelas kepada lembaga penegak hukum untuk menangani kejahatan siber berbasis AI. Hal ini mencakup pelatihan khusus bagi aparat penegak hukum untuk memahami teknologi AI, serta pemberian alat dan teknologi yang memadai untuk menyelidiki kasus kejahatan siber. Terakhir, kerangka hukum harus memastikan perlindungan hak asasi manusia, termasuk privasi dan kebebasan informasi. Regulasi harus seimbang, sehingga tidak menciptakan pengawasan berlebihan yang dapat melanggar hak-hak masyarakat.

Rekonstruksi dan pembaharuan hukum pidana yang mengatur mengenai *Cyber Crime* yang menggunakan sistem AI sebagai alat kejahatan menjadi sebuah hal yang penting. Pemerintah harus segera mengambil tindakan untuk mengisi kekosongan hukum tentang AI yang saat ini terjadi. Jika kekosongan hukum mengenai penanggulangan *Cyber Crime* menggunakan AI dibiarkan terus terjadi, yang ditakutkan ialah penegakkan hukum terhadap kasus serupa tidak dapat dilakukan dengan baik.

Pembaharuan hukum yang mengatur AI di Indonesia dilakukan agar sistem hukum nasional lebih responsif dalam menghadapi perkembangan teknologi, masyarakat, dan modus kejahatan yang selalu berkembang setiap saat. Selain itu, dengan kehadiran peraturan perundang-undangan yang mengatur mengenai penggunaan dan pengawasan AI di Indonesia akan menciptakan kerangka hukum yang lebih adil, bermanfaat, dan relevan dengan kebutuhan masyarakat saat ini dan di masa yang akan datang.

Risiko peningkatan dan perkembangan *Cyber Crime* berbasis AI di masa yang akan datang harus diimbangi dengan upaya aktif pemerintah dalam membentuk kebijakan yang mengatur permasalahan tersebut. Bukan hanya pemerintah, aparat penegak hukum juga dituntut terus melakukan upgrade terhadap perkembangan jenis kejahatan yang ada agar penanganan kejahatan dapat dilakukan dengan baik dan adil. Selain itu, masyarakat sebagai subjek hukum yang rentan menjadi pelaku ataupun korban juga harus memahami bagaimana pemanfaatan AI yang baik dan memahami bagaimana norma hukum dalam pemanfaatan AI tersebut supaya terhindar dari risiko

penyalahgunaan AI baik sebagai korban atau justru sebagai pelaku tindak kejahatan tersebut.

D. KESIMPULAN

Berdasarkan pembahasan diatas, maka dapat ditarik kesimpulan sebagai berikut: (1) Hukum positif Indonesia saat ini belum sepenuhnya mampu mengakomodasi kompleksitas dan perkembangan *cyber crime* berbasis *Artificial Intelligence* (AI). Meskipun beberapa ketentuan dalam KUHP Nasional dan UU ITE telah mengatur jenis-jenis tindak pidana *cyber* secara umum, namun belum ada pengaturan yang secara spesifik dan komprehensif mengatur peran serta dampak dari penggunaan AI dalam kejahatan digital. Ketiadaan regulasi yang eksplisit mengenai AI sebagai alat maupun subjek yang berkontribusi dalam tindak pidana siber menimbulkan kekosongan hukum yang dapat melemahkan upaya penegakan hukum dan perlindungan terhadap masyarakat; (2) Dalam hukum positif ke depan, diperlukan kebijakan hukum pidana yang secara eksplisit mengatur tentang bentuk, pertanggungjawaban, serta sanksi pidana terhadap kejahatan yang melibatkan teknologi AI, baik sebagai alat maupun sebagai pelaku melalui sistem otomatisasi. Selain itu, penting pula untuk memperkuat kapasitas aparat penegak hukum, memperjelas standar etik penggunaan AI, serta membangun kerangka hukum yang mampu mengantisipasi risiko dan dampak sosial dari penggunaan AI secara tidak bertanggung jawab.

DAFTAR PUSTAKA

Aini, Nurul dan Fauziah Lubis. 2024. *"Tantangan Pembuktian Dalam Kasus Kejahatan Siber*", Jurnal Hukum, Vol. 5 No. 02.

Aldya, Aldy Putra. 2019. "*Reverse Engineering untuk Analisis Malware Remote Access Trojan"*, JEPIN (Jurnal Edukasi dan Penelitian Informatika), Vol. 5 No. 1.

Arief, Barda Nawawi. 2010. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Prenada Media.

Ashton, Annie Long. 2024. *"Penegakan Hukum Terhadap Peran Artificial Intelligence di Indonesia*", Jurnal Analogi Hukum, Vol. 6 Issue 3.

Astiti, Ni Made Yordha Ayu. 2023. *"Strict Llliability of Artificial Intelegence:* Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban". Jurnal Magister Hukum Udayana. Vol. 12, No. 4.

BSSN, Laporan Tahunan Statistik Keamanan Siber Indonesia, 2023. Diakses melalui: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-023.pdf.

European Commission, Proposal for a Regulation of The European Parliament and Of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 2021. Diakses melalui : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

Hia, Yosua. 2024. "*Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)*". Jurnal SELISIK. Vol. 10, No. 1.

Latifatunnisa, Raihani dan Made Wira Yudha. 2025. *"Urgensi Pembaruan Regulasi Dalam Menanggulangi Penyalahgunaan Teknologi Artificial Intelligence Dan Deepfake di Indonesia: Perspektif Perlindungan Hak Privasi*", Jurnal Hukum dan Kewarganegaraan, Vol. 11 No. 1 tahun 2025.

Modus Baru Penipuan Kartu Kredit dengan Aplikasi AI, 2 Pelaku Ditangkap, 07 Feb 2025, diakses melalui: https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap.

Mulyana, Yusep. 2024. *"Sosialisasi Implikasi Hukum Penggunaan Artificial Intellegence Dalam Tindak Pidana Cyber Crime Di Kabupaten Garu",* Besiru Jurnal Pengabdian Masyarakat, Vol. 1 No. 11.

Penipuan Canggih, Gunakan AI Tiru Wajah dan Suara Kapolres Jepara Korban Rugi Ratusan Juta, 25 Desember 2024, diakses melalui: https://suarabaru.id/2024/12/25/penipuan-canggih-gunakan-ai-tiru-

wajah-dan-suara-kapolres-jepara-korban-rugi-ratusan-juta pada tanggal 18 juni 2025.

Ravizki, Eka Nanda dan Lintang Yudhantaka, 2022. "*Artificial Intelligence* Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia", Notaire Journal of notarial law, Vol. 5 No. 3.

Wahid, Abdul dan Mohammad Labib. 2005. *Kejahatan Siber (Cyber Crime),* Refika Aditama.

Yanti, Yeni. 2024. "Deteksi Serangan *Distributed Deniel of Service* Pada Jaringan Sensor Nirkabel Menggunakan *Support Vector Machine*, G-Tech: Jurnal Teknologi Terapan, Vol. 8 No. 4.