

KEBIJAKAN HUKUM PIDANA DALAM MENGHADAPI TINDAK PIDANA SIBER BERBASIS KECERDASAN BUATAN (AI CRIME) DI INDONESIA

Muhammad Faska Setianda¹, Selamat Lumban Gaol²

Program Studi Strata Satu (S-1) Ilmu Hukum Fakultas Hukum, Universitas Dirgantara Marsekal

Suryadarma^{1,2}

Email: fsetianda123@gmail.com

Informasi

Abstract

Volume : 3
Nomor : 9
Bulan : September
Tahun : 2026
E-ISSN : 3062-9624

The rapid development of artificial intelligence (AI) technology has transformed various sectors of life, yet it has also given rise to new threats in the form of AI-based cybercrime that are complex and difficult to detect. This phenomenon is characterized by the emergence of cases such as deepfakes for identity fraud, personalized phishing, and autonomous cyberattacks that exploit machine learning algorithms. Indonesia, as a state based on law, faces serious challenges in combating these crimes due to normative gaps in existing legislation. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments, as well as Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), have not specifically regulated criminal acts that utilize artificial intelligence. This article examines the regulation of AI-based cybercrime in Indonesian positive law and formulates an ideal criminal law policy model through a normative approach with analysis of legislation, concepts, and cases. The research finds that criminal policy reformulation is needed at three stages: legislative policy with the formulation of new offenses that accommodate AI characteristics, applicative policy with strengthening the technical capacity of law enforcement officials, and executive policy with a punishment system oriented toward prevention. The criminal law approach needs to align with the utilitarian theory of punishment and adopt principles from international regulations such as the EU AI Act, while still adapting to the national legal context and Pancasila values.

Keyword: Criminal Law Policy; Cybercrime; Artificial Intelligence; AI Crime; Law Enforcement

Abstrak

Perkembangan teknologi kecerdasan buatan (AI) telah mentransformasi berbagai sektor kehidupan, namun juga melahirkan ancaman baru berupa tindak pidana siber berbasis AI yang kompleks dan sulit dideteksi. Fenomena ini ditandai dengan munculnya kasus-kasus seperti deepfake untuk pemalsuan identitas, phishing yang dipersonalisasi, serta serangan siber otonom yang memanfaatkan algoritma pembelajaran mesin. Indonesia sebagai negara hukum menghadapi tantangan serius dalam menanggulangi kejahatan ini karena kesenjangan norma dalam peraturan perundang-undangan yang ada. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), belum secara spesifik mengatur tindak pidana yang memanfaatkan kecerdasan buatan. Artikel ini membahas pengaturan tindak pidana siber berbasis AI dalam hukum positif Indonesia dan merumuskan model kebijakan hukum pidana yang ideal melalui pendekatan normatif dengan analisis peraturan perundang-undangan, konsep, dan kasus. Penelitian menemukan bahwa diperlukan reformulasi kebijakan pidana pada tiga tahap: kebijakan legislatif dengan perumusan delik baru yang mengakomodasi karakteristik AI, kebijakan aplikatif dengan penguatan kapasitas teknis aparat

penegak hukum, serta kebijakan eksekutif dengan sistem pemidanaan yang berorientasi pada pencegahan. Pendekatan hukum pidana perlu selaras dengan teori pemidanaan relatif (*utilitarian*) serta mengadopsi prinsip-prinsip dari regulasi internasional seperti EU AI Act, sambil tetap menyesuaikan dengan konteks hukum nasional dan nilai-nilai Pancasila.

Kata Kunci : Kebijakan Hukum Pidana; Tindak Pidana Siber; Kecerdasan Buatan; AI Crime; Penegakan Hukum

A. PENDAHULUAN

Kecerdasan buatan (*artificial intelligence/AI*) merupakan salah satu inovasi paling revolusioner di abad ke-21. Teknologi ini tidak hanya digunakan untuk tujuan produktif seperti otomatisasi industri, analisis data, dan pengembangan layanan publik, tetapi juga mulai dimanfaatkan untuk tujuan yang merugikan. Tindak pidana siber berbasis kecerdasan buatan (*AI-driven cybercrime*) muncul sebagai ancaman baru yang kompleks, dinamis, dan sulit dideteksi. Tindak pidana siber berbasis AI mencakup berbagai bentuk tindak pidana, seperti *deepfake* untuk pemalsuan identitas, *phishing* yang dipersonalisasi menggunakan algoritma pembelajaran mesin, pembobolan sistem keamanan dengan *AI-powered malware*, hingga pembuatan konten ilegal secara otomatis. Teknologi AI memungkinkan pelaku pidana melakukan serangan siber dalam skala besar dengan efisiensi tinggi dan tingkat akurasi yang lebih baik dibandingkan metode konvensional.

Di Indonesia, kasus-kasus awal seperti penggunaan *deepfake* untuk menyesatkan publik atau meniru suara pejabat negara telah mulai bermunculan, menandakan urgensi penanganan serius terhadap fenomena ini. Bahkan pada awal tahun 2025, Kepolisian Republik Indonesia menangkap pelaku berinisial JS yang menggunakan video *deepfake* menyerupai Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani untuk melakukan penipuan, yang telah merugikan sekitar 100 korban dengan total keuntungan mencapai Rp65 juta. Kasus ini menjadi sinyal awal bahwa modus kejahatan siber berbasis AI telah memasuki ranah praktis dan menimbulkan kerugian nyata bagi masyarakat.

Indonesia sebagai negara hukum memiliki kewajiban untuk melindungi warganya dari segala bentuk pidana, termasuk pidana siber modern. Saat ini, instrumen hukum yang tersedia antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, regulasi-regulasi tersebut belum secara spesifik mengatur tindak pidana yang memanfaatkan kecerdasan buatan. Kesenjangan norma ini menimbulkan tantangan serius bagi aparat penegak

hukum dalam menjerat pelaku, mengingat unsur-unsur tindak pidana dalam UU ITE dirancang berdasarkan modus operandi konvensional.

Selain itu, aspek pembuktian menjadi kendala utama. Dalam pidana siber berbasis AI, sulit untuk menentukan apakah suatu tindakan dilakukan secara manual oleh manusia, diotomatisasi oleh program AI, atau bahkan dilakukan oleh AI secara otonom. Pertanyaan mengenai pertanggungjawaban pidana juga muncul: apakah pengembang AI, pengguna AI, atau AI itu sendiri yang dapat dimintai pertanggungjawaban? Hal ini belum dijawab secara tegas oleh sistem hukum pidana Indonesia yang masih berorientasi pada subjek hukum manusia.

Kebijakan hukum pidana (*penal policy*) memiliki peran strategis dalam menanggulangi pidana. Menurut Barda Nawawi Arief, kebijakan hukum pidana meliputi tiga tahap kebijakan, yaitu: (1) tahap kebijakan legislatif/formulatif; (2) tahap kebijakan yudikatif/aplikatif; dan (3) tahap kebijakan eksekutif/administratif. Dalam konteks pidana siber berbasis AI, diperlukan reformulasi kebijakan pidana di ketiga tahap tersebut. Pada tahap formulasi, perlu ada perumusan delik baru yang mengakomodasi karakteristik AI. Pada tahap aplikasi, aparat penegak hukum harus memiliki kapasitas teknis untuk menyelidiki dan membuktikan pidana AI. Pada tahap eksekusi, sistem pemidanaan perlu mempertimbangkan aspek pencegahan khusus dan umum, mengingat potensi bahaya besar dari pidana ini.

Pendekatan hukum pidana juga harus selaras dengan perkembangan teknologi. Teori pemidanaan relatif (*utilitarian theory*) yang dikemukakan oleh Jeremy Bentham dan John Stuart Mill menekankan bahwa tujuan pemidanaan adalah untuk mencegah pidana, bukan sekadar pembalasan. Teori ini sangat relevan diterapkan dalam konteks *AI crime*, di mana pemidanaan bukan hanya sebagai pembalasan, tetapi sebagai sarana untuk melindungi masyarakat melalui efek jera. Pidana tambahan seperti pencabutan akses terhadap teknologi AI, pengawasan ketat terhadap pengembang, atau kewajiban pelaporan berkala dapat menjadi alternatif yang lebih efektif.

Fenomena global juga menunjukkan bahwa negara-negara maju seperti Amerika Serikat, Tiongkok, dan negara-negara Uni Eropa telah mulai merumuskan regulasi khusus tentang AI. Uni Eropa, misalnya, melalui *EU AI Act* (Regulation (EU) 2024/1689), mengkategorikan AI ke dalam tingkat risiko (*unacceptable risk*, *high-risk*, *limited risk*, dan *minimal risk*), serta melarang praktik AI yang membahayakan masyarakat. Indonesia perlu belajar dari kebijakan tersebut sekaligus menyesuaikan dengan konteks hukum nasional dan nilai-nilai Pancasila.

B. KAJIAN TEORITIS

1. Teori Kebijakan Hukum Pidana

Kebijakan hukum pidana (*penal policy*) merupakan usaha untuk menanggulangi kejahatan melalui pembentukan dan penerapan hukum pidana. Menurut Barda Nawawi Arief, kebijakan hukum pidana meliputi tiga tahap: (1) tahap kebijakan legislatif/formulatif, yaitu tahap perumusan delik dan sanksi pidana; (2) tahap kebijakan yudikatif/aplikatif, yaitu tahap penerapan hukum pidana oleh aparat penegak hukum; dan (3) tahap kebijakan eksekutif/administratif, yaitu tahap pelaksanaan pidana (Arief, 2022).

2. Teori Pemidanaan Relatif (Utilitarian)

Teori pemidanaan relatif (*utilitarian theory*) yang dikemukakan oleh Jeremy Bentham dan John Stuart Mill menekankan bahwa tujuan pemidanaan adalah untuk mencegah kejahatan, bukan sekadar pembalasan. Teori ini menekankan pada aspek pencegahan (*prevention*), baik pencegahan khusus (*speciale preventie*) bagi pelaku agar tidak mengulangi perbuatannya, maupun pencegahan umum (*general preventie*) bagi masyarakat luas agar tidak meniru perbuatan tersebut (Bentham, 2022; Mill, 1863).

3. Konsep Kecerdasan Buatan (AI)

Kecerdasan buatan (*artificial intelligence/AI*) merupakan sistem komputer yang mampu melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia, seperti pembelajaran, penalaran, persepsi, dan pengambilan keputusan. AI memiliki karakteristik otonomi (kemampuan mengambil keputusan tanpa intervensi manusia), adaptivitas (kemampuan belajar dan mengubah perilaku berdasarkan data baru), opasitas atau *black box problem* (kesulitan menjelaskan secara transparan bagaimana AI mencapai suatu keputusan), dan *continuous learning* (kemampuan belajar secara terus-menerus).

4. Konsep Tindak Pidana Siber Berbasis AI

Tindak pidana siber berbasis AI (*AI crime*) merupakan tindak pidana yang memanfaatkan kecerdasan buatan sebagai sarana, objek, maupun pelaku kejahatan. Bentuk-bentuk *AI crime* meliputi *deepfake* untuk pemalsuan identitas, *phishing* yang dipersonalisasi, *AI-powered malware*, serangan otonom, dan manipulasi algoritma. Kejahatan ini memiliki karakteristik yang berbeda dengan kejahatan siber konvensional, terutama terkait dengan kecepatan, jangkauan lintas batas, dan sifat bukti elektronik yang rentan rusak.

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang dilakukan dengan meneliti

bahan pustaka atau data sekunder untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Pendekatan yang digunakan meliputi pendekatan undang-undang (*statute approach*) dengan menelaah seluruh peraturan perundang-undangan yang relevan, pendekatan konseptual (*conceptual approach*) dengan mempelajari pandangan dan doktrin para ahli, serta pendekatan kasus (*case approach*) dengan mempelajari kasus-kasus konkret terkait tindak pidana siber berbasis AI di Indonesia. Sumber data yang digunakan adalah data sekunder yang terdiri dari bahan hukum primer (peraturan perundang-undangan seperti UUD 1945, KUHP Nasional, UU ITE, UU PDP, dan peraturan pelaksana lainnya), bahan hukum sekunder (buku teks, doktrin ahli, hasil penelitian, dan jurnal ilmiah), serta bahan hukum tersier (kamus dan ensiklopedia). Teknik pengumpulan data dilakukan melalui studi pustaka dengan membaca, mencatat, dan menganalisis dokumen hukum serta penelusuran melalui media internet. Analisis data menggunakan metode analisis kualitatif dengan melakukan interpretasi terhadap bahan-bahan hukum untuk mengidentifikasi adanya kekosongan norma (*rechtsvacuum*), antinomi norma, dan norma kabur (*vague normen*), yang kemudian dianalisis secara sistematis untuk menarik kesimpulan mengenai pengaturan dan model kebijakan hukum pidana yang ideal dalam menanggulangi tindak pidana siber berbasis AI (Marzuki, 2005; Soekanto & Mamudji, 2001).

C. HASIL DAN PEMBAHASAN

1. Pengaturan Tindak Pidana Siber Berbasis Kecerdasan Buatan (AI) dalam Hukum Positif Indonesia dan Kepastian Hukum

Pengaturan tindak pidana siber berbasis AI dalam hukum positif Indonesia saat ini masih bersifat sektoral dan belum memberikan kepastian hukum yang memadai. Hal ini disebabkan oleh tidak adanya satu pun peraturan perundang-undangan yang secara eksplisit mendefinisikan dan mengkriminalisasi perbuatan yang memanfaatkan kecerdasan buatan sebagai sarana, objek, maupun pelaku kejahatan. Ketidadaan norma yang spesifik ini menimbulkan kekosongan hukum (*rechtsvacuum*) yang berpotensi menghambat upaya penegakan hukum terhadap modus kejahatan siber yang semakin canggih.

a. Pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 merupakan payung hukum utama kebijakan pidana siber di Indonesia. Pasal 5 sampai dengan Pasal 10 UU ITE mengatur tentang informasi elektronik dan dokumen elektronik sebagai alat

bukti yang sah, sementara Pasal 27 sampai dengan Pasal 37 mengatur berbagai perbuatan yang dilarang di ranah siber. Meskipun UU ITE 2024 mulai mengakomodasi tantangan baru dengan memperluas cakupan sistem elektronik dan memperketat pengaturan terhadap penyalahgunaan teknologi, ketentuan ini belum secara eksplisit menyebut kecerdasan buatan.

Beberapa pasal dalam UU ITE yang dapat digunakan secara implisit untuk menjerat kejahatan berbasis AI antara lain:

Pasal 27A UU ITE mengatur larangan mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. Pasal ini dapat digunakan untuk menjerat penyebaran konten *deepfake* pornografi atau asusila yang merugikan korban.

Pasal 35 UU ITE melarang setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, dan/atau pengubahan atas Informasi Elektronik dan/atau Dokumen Elektronik. Ketentuan ini menjadi dasar hukum yang sering digunakan untuk menjerat pembuatan konten *deepfake* atau rekayasa identitas digital yang menyesatkan publik.

Pasal 45A ayat (4) jo. Pasal 27A UU ITE mengatur ancaman pidana bagi pelanggar ketentuan muatan melanggar kesusilaan, yang sering digunakan secara berlapis bersama pasal-pasal lain dalam penegakan hukum terhadap kejahatan siber.

Pasal 48 jo. Pasal 32 UU ITE mengatur ancaman pidana bagi pelaku akses ilegal ke sistem elektronik, yang relevan untuk menjerat perbuatan akses ilegal guna mendapatkan data yang kemudian dimanipulasi oleh sistem AI.

Pasal 51 ayat (1) jo. Pasal 35 UU ITE mengatur ancaman pidana bagi pelaku manipulasi informasi elektronik, yang sering digunakan untuk menjerat pembuat *deepfake* yang mengubah konten visual atau audio secara melawan hukum.

Dengan demikian, meskipun UU ITE telah mengalami beberapa kali perubahan, pengaturan mengenai AI masih bersifat implisit dan belum mampu menjawab secara tuntas tantangan hukum yang ditimbulkan oleh perkembangan teknologi kecerdasan buatan.

b. Pengaturan dalam Kitab Undang-Undang Hukum Pidana Nasional

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional) yang mulai berlaku pada tahun 2026 memberikan kerangka kebijakan hukum pidana materil yang lebih komprehensif. KUHP Nasional secara eksplisit mengatur Tindak Pidana terhadap Informatika dan Elektronika dalam Bab XXX, yang meliputi Pasal 332 tentang akses ilegal terhadap sistem elektronik, Pasal 333 tentang intersepsi ilegal, Pasal 334 tentang

gangguan terhadap sistem elektronik, dan Pasal 335 tentang perusakan data elektronik. Pengaturan khusus ini menunjukkan kesadaran pembentuk undang-undang bahwa tindak pidana di bidang informatika memiliki karakteristik berbeda dengan tindak pidana konvensional, terutama terkait dengan kecepatan, jangkauan lintas batas, dan sifat bukti elektronik yang rentan rusak.

Namun demikian, ketentuan ini belum secara spesifik mengatur tindak pidana yang melibatkan kecerdasan buatan sebagai pelaku atau sarana. Pasal 20 UU 1/2023 hanya mengakui orang perseorangan dan korporasi sebagai subjek tindak pidana, dan ketiadaan pengaturan AI sebagai subjek hukum menyebabkan *vacuum of responsibility* ketika AI melakukan perbuatan merugikan secara otonom. Ketentuan Pasal 1 ayat (2) KUHP yang melarang penggunaan analogi juga menjadi kendala, karena hakim tidak dapat memperluas rumusan delik di luar ketentuan undang-undang untuk menjerat modus kejahatan AI yang belum diatur. Hal ini menjadi persoalan serius mengingat AI memiliki karakteristik otonomi yang memungkinkannya mengambil keputusan tanpa intervensi manusia, sehingga sulit untuk menentukan siapa yang bertanggung jawab secara pidana ketika AI melakukan tindakan yang merugikan.

c. Pengaturan dalam Undang-Undang Pelindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi instrumen penting dalam melindungi masyarakat dari penyalahgunaan data oleh sistem AI, mengingat data merupakan bahan bakar utama bagi pengoperasian kecerdasan buatan. UU PDP mengatur ancaman pidana bagi pihak yang mengumpulkan, mengolah, atau menyebarkan data pribadi secara melawan hukum, yang dapat dikaitkan dengan praktik AI seperti *scraping*, pelanggaran privasi, dan *profiling* ilegal.

Namun demikian, UU PDP juga belum secara spesifik mengatur tentang penggunaan data oleh sistem AI, termasuk kewajiban untuk mendapatkan persetujuan eksplisit, pembatasan penggunaan data, dan sanksi yang tegas bagi pelanggaran yang melibatkan teknologi AI. Peraturan Pemerintah Nomor 47 Tahun 2023 tentang Tata Cara Penyelenggaraan Perlindungan Data Pribadi sebagai peraturan pelaksana UU PDP juga belum mengatur secara spesifik tentang kecerdasan buatan. Selain itu, Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial bersifat etis dan imbauan, bukan hukum positif yang memiliki kekuatan mengikat dan sanksi tegas. Hal ini menunjukkan bahwa regulasi AI di Indonesia masih berada pada tataran etika dan imbauan, dan belum masuk ke ranah hukum pidana yang operasional.

d. Kesenjangan Norma dan Kendala Penegakan Hukum

Berdasarkan analisis terhadap peraturan perundang-undangan di atas, terdapat beberapa kesenjangan norma (*rechtsvacuum*) dan kendala dalam penegakan hukum terhadap tindak pidana siber berbasis AI.

Pertama, ketidakjelasan rumusan delik. UU ITE dan KUHP Nasional belum mengakomodasi karakteristik AI seperti otonomi, adaptivitas, dan opasitas. Pasal-pasal yang ada hanya dapat digunakan secara implisit untuk menjerat pada tahap hilir (distribusi) dan bukan pada tahap hulu (pembuatan atau penggunaan AI).

Kedua, ketidakjelasan subjek hukum. Pasal 20 UU 1/2023 hanya mengakui orang perseorangan dan korporasi sebagai subjek tindak pidana, sementara ketiadaan pengaturan AI sebagai subjek hukum menyebabkan *vacuum of responsibility* ketika AI bertindak secara otonom dan merugikan pihak lain. Pertanyaan mengenai pertanggungjawaban pidana—apakah pengembang AI, pengguna AI, atau AI itu sendiri yang dapat dimintai pertanggungjawaban—belum dijawab secara tegas oleh sistem hukum pidana Indonesia.

Ketiga, kesulitan pembuktian. Dalam pidana siber berbasis AI, sulit untuk menentukan apakah suatu tindakan dilakukan secara manual oleh manusia, diotomatisasi oleh program AI, atau bahkan dilakukan oleh AI secara otonom. Unsur *mens rea* (kesengajaan atau kealpaan) tidak dapat dilekatkan pada mesin, sehingga menyulitkan aparat penegak hukum dalam membuktikan unsur kesalahan. Selain itu, fenomena *black box* pada sistem AI membuat sulit untuk menjelaskan secara transparan bagaimana AI mencapai suatu keputusan, yang menjadi tantangan serius dalam forensik digital.

Keempat, keterbatasan kapasitas teknis aparat penegak hukum. Aparat penegak hukum (kepolisian, kejaksaan, dan hakim) masih terbatas dalam hal kapasitas teknis untuk menyelidiki dan membuktikan tindak pidana berbasis AI. Dibutuhkan pemahaman yang mendalam tentang teknologi AI, forensik digital, dan analisis algoritma yang tidak dimiliki oleh sebagian besar aparat penegak hukum saat ini. Kepolisian dan kejaksaan masih kekurangan sumber daya manusia dan infrastruktur forensik digital untuk menangani kasus-kasus siber yang semakin kompleks. Keputusan Kapolri Nomor 53 Tahun 2023 tentang Pembentukan Satuan Tugas *Cyber Crime and Artificial Intelligence* merupakan langkah awal yang positif, namun implementasinya masih memerlukan penguatan kapasitas dan sumber daya yang memadai.

2. Contoh Kasus Penanggulangan Tindak Pidana Siber Berbasis AI di Indonesia

Beberapa kasus nyata menunjukkan bahwa modus kejahatan siber berbasis AI telah memasuki ranah praktis dan menimbulkan kerugian nyata bagi masyarakat, sekaligus menggambarkan tantangan penegakan hukum yang dihadapi.

Kasus pertama adalah penangkapan pelaku berinisial JS pada awal tahun 2025 oleh Kepolisian Republik Indonesia. Pelaku menggunakan video *deepfake* menyerupai Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani untuk menawarkan bantuan fiktif kepada korban, yang merugikan sekitar 100 korban dengan total keuntungan mencapai Rp65 juta. Pelaku dijerat dengan Pasal 51 ayat (1) jo. Pasal 35 UU ITE tentang manipulasi informasi elektronik dan Pasal 378 KUHP tentang penipuan. Kasus ini menunjukkan bahwa UU ITE dapat digunakan untuk menjerat pelaku, namun hanya untuk kejahatan penipuan konvensional dan bukan untuk mengatur penggunaan AI itu sendiri sebagai sarana kejahatan.

Kasus kedua adalah penyebaran video *deepfake* yang menyerang kehormatan pengusaha Jusuf Hamka dan istrinya di platform TikTok pada tahun 2025. Polisi berhasil menangkap pelaku dan menjeratnya dengan beberapa pasal secara berlapis, yaitu Pasal 45A ayat (4) jo. Pasal 27A UU ITE tentang muatan melanggar kesusilaan, Pasal 48 jo. Pasal 32 UU ITE tentang akses ilegal, Pasal 51 ayat (1) jo. Pasal 35 UU ITE tentang manipulasi informasi elektronik, serta Pasal 310 dan Pasal 311 KUHP tentang pencemaran nama baik. Pendekatan "hukum berlapis" ini menunjukkan upaya aparat penegak hukum untuk menemukan dasar hukum yang tepat, namun juga mencerminkan ketiadaan pasal khusus yang secara tegas mengatur *deepfake*.

Kasus ketiga adalah pemblokiran akses terhadap Grok AI oleh Kementerian Komunikasi dan Informatika pada tahun 2026. Tindakan ini diambil karena Grok AI disalahgunakan oleh pengguna untuk membuat konten pornografi. Langkah pemblokiran ini bersifat administratif dan jangka pendek, yang menurut para pakar hukum menunjukkan perlunya regulasi jangka panjang yang mengatur tanggung jawab pidana pengguna dan penyelenggara sistem elektronik. Kasus ini menyoroti bahwa penanganan kejahatan AI masih bersifat reaktif dan belum didukung oleh kerangka hukum yang komprehensif.

Kasus keempat adalah sejumlah kasus *deepfake* pornografi non-konsensual yang mulai marak di Indonesia. Dalam kasus-kasus ini, aplikasi AI digunakan untuk membuat konten pornografi dari foto seseorang tanpa izin, yang kemudian disebarluaskan di media sosial. UU ITE melalui Pasal 27A hanya dapat menjerat jika konten tersebut disebarluaskan (distribusi), tetapi tidak dapat menjerat pembuatan konten untuk konsumsi pribadi secara luring (*offline*). Hal ini menunjukkan adanya kekosongan hukum yang serius, di mana pembuatan *deepfake* itu sendiri tidak dapat dipidana jika tidak disebarluaskan.

Kasus kelima adalah serangan *phishing* berbasis AI yang mulai teridentifikasi di Indonesia, meskipun belum banyak dilaporkan secara publik. Pelaku menggunakan kecerdasan buatan untuk mempersonalisasi serangan *phishing* yang lebih sulit dideteksi oleh korban dan sistem keamanan. Penanganan kasus ini masih menggunakan pasal penipuan konvensional (Pasal 378 KUHP) karena belum ada pasal khusus untuk kejahatan siber berbasis AI yang memanfaatkan algoritma pembelajaran mesin untuk menipu korban secara masif dan terpersonalisasi.

Kelima kasus di atas menegaskan bahwa penegakan hukum terhadap tindak pidana siber berbasis AI di Indonesia masih menghadapi tantangan serius dan memerlukan reformulasi kebijakan hukum pidana yang komprehensif.

3. Model Kebijakan Hukum Pidana Ideal dalam Menanggulangi Tindak Pidana Siber Berbasis Kecerdasan Buatan (AI Crime)

Berdasarkan teori kebijakan hukum pidana yang dikemukakan oleh Barda Nawawi Arief dan Marc Ancel, kebijakan hukum pidana dalam menanggulangi tindak pidana siber berbasis AI harus dilaksanakan melalui tiga tahap, yaitu kebijakan formulatif atau legislatif, kebijakan aplikatif atau yudikatif, dan kebijakan eksekutif atau administratif. Ketiga tahap ini harus dilaksanakan secara terintegrasi dan berkesinambungan untuk menghasilkan kebijakan hukum pidana yang efektif dalam menanggulangi kejahatan siber berbasis AI.

a. Kebijakan Formulatif/Legislatif

Kebijakan formulatif atau legislatif merupakan tahap penyusunan hukum pidana yang mencakup perumusan delik baru dan penyesuaian sanksi pidana. Dalam konteks tindak pidana siber berbasis AI, kebijakan formulatif yang ideal meliputi perumusan delik baru yang mengakomodasi karakteristik AI, penguatan subjek hukum dan pertanggungjawaban pidana, harmonisasi dengan regulasi internasional, serta penguatan perlindungan data pribadi.

Pembentuk undang-undang perlu merumuskan delik-delik baru yang secara spesifik mengatur tindak pidana yang melibatkan kecerdasan buatan, baik sebagai sarana, objek, maupun pelaku kejahatan. Rumusan delik baru ini harus mengakomodasi karakteristik AI seperti otonomi (kemampuan AI untuk mengambil keputusan tanpa intervensi manusia), adaptivitas (kemampuan AI untuk belajar dan mengubah perilaku berdasarkan data baru), opasitas atau *black box problem* (kesulitan untuk menjelaskan secara transparan bagaimana AI mencapai suatu keputusan), dan *continuous learning* (kemampuan AI untuk belajar secara terus-menerus). Perumusan delik baru dapat mengacu pada tipologi tindak pidana siber berbasis AI, seperti penyalahgunaan AI untuk menyempurnakan kejahatan siber konvensional

(misalnya *deepfake*, *automated phishing*, *AI-powered malware*) maupun kejahatan baru yang hanya dimungkinkan dengan keberadaan AI (misalnya serangan otonom dan manipulasi algoritma).

Selain itu, pembentuk undang-undang perlu mempertimbangkan perluasan subjek hukum dalam hukum pidana untuk menjangkau pengembang AI, pengguna AI, dan korporasi yang memanfaatkan AI. Beberapa model pertanggungjawaban yang dapat dipertimbangkan antara lain tanggung jawab pengembang (*developer liability*) di mana pengembang AI bertanggung jawab atas kerugian yang ditimbulkan oleh sistem AI yang dikembangkannya berdasarkan prinsip kelalaian (*negligence*) atau tanggung jawab mutlak (*strict liability*), tanggung jawab pengguna (*user liability*) di mana pengguna AI bertanggung jawab atas penggunaan AI untuk tujuan yang melawan hukum, serta tanggung jawab korporasi (*corporate liability*) di mana korporasi yang mengembangkan, mendistribusikan, atau menggunakan AI bertanggung jawab atas kerugian yang ditimbulkan.

Indonesia juga perlu belajar dari kebijakan negara-negara maju dalam merumuskan regulasi tentang AI, seperti Uni Eropa melalui *EU AI Act* (Regulation (EU) 2024/1689) yang mengkategorikan AI ke dalam tingkat risiko (*unacceptable risk*, *high-risk*, *limited risk*, dan *minimal or no risk*) serta melarang praktik AI yang membahayakan masyarakat. Indonesia dapat mengadopsi pendekatan berbasis risiko ini dengan menyesuaikannya dengan konteks hukum nasional dan nilai-nilai Pancasila. Mengingat AI sangat bergantung pada data, perlindungan data pribadi menjadi krusial, sehingga UU PDP perlu diperkuat dengan ketentuan yang secara spesifik mengatur penggunaan data oleh sistem AI, termasuk kewajiban untuk mendapatkan persetujuan eksplisit, pembatasan penggunaan data, dan sanksi yang tegas bagi pelanggaran.

b. Kebijakan Aplikatif/Yudikatif

Kebijakan aplikatif atau yudikatif merupakan tahap penerapan hukum pidana oleh aparat penegak hukum. Dalam konteks tindak pidana siber berbasis AI, kebijakan aplikatif yang ideal meliputi penguatan kapasitas teknis aparat penegak hukum, pengembangan metode pembuktian yang adaptif, serta penafsiran hukum yang progresif oleh hakim.

Aparat penegak hukum (kepolisian, kejaksaan, dan hakim) perlu memiliki kapasitas teknis untuk menyelidiki, menuntut, dan mengadili perkara pidana siber berbasis AI. Penguatan kapasitas ini dapat dilakukan melalui pelatihan dan pendidikan berkelanjutan tentang teknologi AI, forensik digital, dan analisis algoritma, pengembangan unit khusus yang

menangani tindak pidana siber berbasis AI di lingkungan kepolisian dan kejaksaan, serta kerja sama dengan ahli teknologi dan akademisi dalam proses penyidikan dan pembuktian.

Sistem pembuktian dalam hukum acara pidana juga perlu dikembangkan untuk mengakomodasi karakteristik bukti elektronik dalam tindak pidana siber berbasis AI. Beberapa langkah yang dapat dilakukan antara lain pengakuan alat bukti elektronik baru seperti *digital footprint*, *log file*, dan *audit trail*, pengembangan standar forensik digital untuk mengumpulkan, mengamankan, dan menganalisis bukti elektronik, serta pemanfaatan saksi ahli teknologi dalam proses peradilan untuk menjelaskan aspek teknis AI.

Hakim perlu melakukan penafsiran hukum yang progresif dalam memutus perkara pidana siber berbasis AI, dengan tetap berpegang pada asas legalitas. Penafsiran ekstensif terhadap rumusan delik yang ada dapat dilakukan sepanjang tidak bertentangan dengan asas legalitas dan hak asasi manusia. Dengan demikian, aparat penegak hukum tidak hanya dituntut untuk memahami hukum secara dogmatis, tetapi juga harus memiliki pemahaman yang memadai tentang perkembangan teknologi agar dapat menerapkan hukum secara tepat dan berkeadilan.

c. Kebijakan Eksekutif/Administratif

Kebijakan eksekutif atau administratif merupakan tahap pelaksanaan pidana. Dalam konteks tindak pidana siber berbasis AI, kebijakan eksekutif yang ideal meliputi pemidanaan yang berorientasi pada pencegahan, pencegahan dan pengawasan yang proaktif, serta restitusi dan pemulihan korban.

Berdasarkan teori pemidanaan relatif (utilitarian) yang dikemukakan oleh Jeremy Bentham dan John Stuart Mill, tujuan pemidanaan adalah untuk mencegah kejahatan, bukan sekadar pembalasan. Oleh karena itu, sistem pemidanaan dalam tindak pidana siber berbasis AI harus berorientasi pada pencegahan, baik pencegahan khusus (pelaku) maupun pencegahan umum (masyarakat). Beberapa jenis pidana yang dapat dipertimbangkan antara lain pidana pokok berupa pidana penjara dan/atau pidana denda yang proporsional dengan kerugian yang ditimbulkan, pidana tambahan berupa pencabutan akses terhadap teknologi AI, pengawasan ketat terhadap pengembang atau pengguna, kewajiban pelaporan berkala, dan pembayaran ganti rugi kepada korban, serta pidana alternatif berupa pelayanan masyarakat di bidang literasi digital atau pengawasan teknologi.

Selain pemidanaan, kebijakan eksekutif juga harus mencakup upaya pencegahan dan pengawasan yang proaktif, antara lain pengembangan sistem peringatan dini untuk mendeteksi potensi tindak pidana siber berbasis AI, kerja sama dengan platform digital dan

penyelenggara sistem elektronik untuk mencegah penyalahgunaan AI, serta peningkatan literasi digital masyarakat untuk mengurangi kerentanan terhadap kejahatan siber berbasis AI. Kebijakan eksekutif juga harus memperhatikan kepentingan korban melalui mekanisme restitusi dan pemulihan, di mana pelaku pidana siber berbasis AI harus diwajibkan untuk membayar ganti rugi kepada korban atas kerugian yang ditimbulkan. Selain itu, negara juga perlu menyediakan layanan pendampingan dan pemulihan bagi korban kejahatan siber. Dengan pendekatan yang komprehensif ini, kebijakan hukum pidana tidak hanya berfungsi sebagai instrumen penegakan hukum, tetapi juga sebagai sarana perlindungan masyarakat dan pencegahan kejahatan di era digital yang semakin kompleks.

D. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai kebijakan hukum pidana dalam menghadapi tindak pidana siber berbasis kecerdasan buatan (*AI Crime*) di Indonesia, dapat disimpulkan bahwa pengaturan tindak pidana siber berbasis AI dalam hukum positif Indonesia saat ini masih terbatas dan belum memberikan kepastian hukum yang memadai. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi belum secara spesifik mengatur tindak pidana yang memanfaatkan kecerdasan buatan sebagai sarana, objek, atau pelaku kejahatan. Pasal-pasal dalam UU ITE seperti Pasal 27A, Pasal 35, Pasal 45A ayat (4), Pasal 48 jo. Pasal 32, dan Pasal 51 ayat (1) jo. Pasal 35 hanya dapat digunakan secara implisit untuk menjerat kejahatan berbasis AI, sementara KUHP Nasional melalui Pasal 332-335 juga belum mengakomodasi karakteristik AI seperti otonomi, adaptivitas, dan opasitas. Kesenjangan norma ini menimbulkan tantangan yang serius dalam penegakan hukum, terutama terkait ketidakjelasan subjek hukum, kesulitan pembuktian unsur kesalahan, dan keterbatasan kapasitas teknis aparat penegak hukum sebagaimana terlihat dalam kasus penangkapan pelaku *deepfake* berinisial JS serta kasus-kasus lainnya yang menunjukkan modus kejahatan ini telah memasuki ranah praktis.

Model kebijakan hukum pidana ideal memerlukan reformulasi pada tiga tahap secara terintegrasi guna mewujudkan kepastian hukum. *Pertama*, kebijakan formatif/legislatif meliputi perumusan delik baru yang secara eksplisit mengatur tindak pidana berbasis AI dengan mengakomodasi karakteristik AI, penguatan subjek hukum yang mencakup pengembang, pengguna, dan korporasi, harmonisasi dengan regulasi internasional seperti *EU*

AI Act, serta penguatan perlindungan data pribadi dalam UU PDP. *Kedua*, kebijakan aplikatif/yudikatif meliputi penguatan kapasitas teknis aparat penegak hukum melalui pelatihan berkelanjutan dan pengembangan unit khusus, pengembangan metode pembuktian yang adaptif dengan mengakui alat bukti elektronik baru dan memanfaatkan saksi ahli teknologi, serta penafsiran hukum yang progresif oleh hakim sepanjang tidak bertentangan dengan asas legalitas. *Ketiga*, kebijakan eksekutif/administratif meliputi pemidanaan yang berorientasi pada pencegahan berdasarkan teori pemidanaan relatif (utilitarian) dengan mempertimbangkan pidana tambahan seperti pencabutan akses terhadap teknologi AI, pencegahan dan pengawasan proaktif melalui sistem peringatan dini dan kerja sama dengan platform digital, serta restitusi dan pemulihan korban melalui kewajiban pembayaran ganti rugi dan layanan pendampingan.

2. Saran

Berdasarkan kesimpulan di atas, penulis menyampaikan saran kepada pembentuk undang-undang (legislatif) agar segera merumuskan delik-delik baru yang secara spesifik mengatur tindak pidana siber berbasis kecerdasan buatan dalam revisi UU ITE atau dalam peraturan perundang-undangan tersendiri yang mengakomodasi karakteristik AI seperti otonomi, adaptivitas, opasitas, dan *continuous learning*. Pembentuk undang-undang juga perlu memperluas subjek hukum dalam hukum pidana untuk menjangkau pengembang AI, pengguna AI, dan korporasi yang memanfaatkan AI dengan mengatur secara jelas model pertanggungjawaban pidana masing-masing pihak, melakukan harmonisasi regulasi AI dengan standar internasional seperti *EU AI Act* sambil tetap menyesuaikan dengan konteks hukum nasional dan nilai-nilai Pancasila, serta memperkuat ketentuan perlindungan data pribadi dalam UU PDP terkait penggunaan data oleh sistem AI.

Kepada aparat penegak hukum (yudikatif dan eksekutif), disarankan untuk meningkatkan kapasitas teknis dalam menangani perkara pidana siber berbasis AI melalui pelatihan berkelanjutan, pengembangan unit khusus, dan kerja sama dengan ahli teknologi, serta mengembangkan metode pembuktian yang adaptif dengan memanfaatkan alat bukti elektronik dan saksi ahli. Kepada pemerintah, disarankan untuk membangun sistem peringatan dini dan pengawasan proaktif terhadap potensi penyalahgunaan AI, meningkatkan literasi digital masyarakat, serta menyediakan layanan pendampingan dan pemulihan bagi korban kejahatan siber berbasis AI. Kepada masyarakat, disarankan untuk meningkatkan kewaspadaan terhadap modus kejahatan siber berbasis AI dan berperan aktif dalam diskusi publik terkait pengaturan AI, sementara kepada peneliti selanjutnya disarankan untuk

melakukan penelitian empiris mengenai efektivitas penegakan hukum dan studi perbandingan dengan negara lain yang telah memiliki regulasi AI lebih maju.

E. DAFAR PUSTAKA

A. Buku

- Abidin, A. Z. (2021). Hukum pidana Indonesia. Sinar Grafika.
- Arief, B. N. (2007). Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan. Kencana.
- Arief, B. N. (2022). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru (Edisi Revisi). Kencana.
- Bentham, J. (2022). An introduction to the principles of morals and legislation (Reprint ed.). Clarendon Press. (Karya asli diterbitkan 1789)
- Gunawan, Y., & Kristian. (2023). Tindak pidana siber di Indonesia (Edisi Kedua). Refika Aditama.
- Hiariej, E. O. S. (2023). Prinsip-prinsip hukum pidana (Edisi Revisi). Cahaya Atma Pustaka.
- Ibrahim, J. (2006). Teori dan metodologi penelitian hukum normatif. Bayumedia Publishing.
- Marzuki, P. M. (2005). Penelitian hukum. Kencana Prenada Media Group.
- Mill, J. S. (1863). Utilitarianism. Parker, Son, and Bourn.
- Moeljatno. (2008). Asas-asas hukum pidana. Rineka Cipta.
- Muladi. (2005). Kapita selekta hukum pidana. Alumni.
- Muladi, & Arief, B. N. (2023). Teori-teori dan kebijakan pidana (Cetakan Kesembilan). Alumni.
- Sjahdeini, S. R. (2024). Kebijakan formulasi hukum pidana dalam menghadapi perkembangan teknologi. Pustaka Utama.
- Soekanto, S., & Mamudji, S. (2001). Penelitian hukum normatif: Suatu tinjauan singkat. Raja Grafindo Persada.
- Sunggono, B. (2003). Metodologi penelitian hukum. Raja Grafindo Persada.
- Turner, J. (2019). Robot rules: Regulating artificial intelligence. Palgrave Macmillan.

B. Jurnal Ilmiah

- Anwar, H. M. (2024). Forensik digital dalam penanganan tindak pidana siber. Jurnal Forensik Digital Indonesia, 1(1), 15-22.
- Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513-563.
- Dietterich, T. G. (2017). Steps toward robust artificial intelligence. AI Magazine, 38(3), 3-24.
- Hamilton, C. (2024). Cybercrime prevention through artificial intelligence monitoring. Journal

of Cybersecurity, 10(2), 112-125.

Hanum, L. G. (2026). AI tanpa batas? Menakar perlindungan hukum atas data pribadi di Indonesia. FKPH Universitas Brawijaya, 3-6.

Jurcys, P. (2021). Legal personality of artificial intelligence. *European Journal of Law and Technology*, 12(1), 1-18.

Nurkholisah, S., Rismana, D., Nugroho, A. E., et al. (2025). Deepfake sebagai bentuk kejahatan siber baru: Tantangan kriminalisasi dalam hukum pidana Indonesia. *Jurnal USM Law Review*, 8(3), 7-10.

Respati, A. A. (2024). Reformulasi UU ITE terhadap artificial intelligence dibandingkan dengan Uni Eropa dan China AI Act Regulation. *Jurnal USM Law Review*, 7(3), 12-15.

Said, M. U. (2023). Pertanggungjawaban pidana korporasi dalam kejahatan siber. *Jurnal Hukum Ius Quia Iustum*, 30(2), 250-265.

Sulihandari, H. (2022). Penegakan hukum pidana siber di Indonesia. *Jurnal Hukum dan Pembangunan*, 52(3), 456-470.

C. Peraturan Perundang-undangan

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 139.

Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional). Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

Indonesia. (2023). Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.

Indonesia. (2023). Keputusan Kapolri Nomor 53 Tahun 2023 tentang Pembentukan Satuan Tugas Cyber Crime and Artificial Intelligence.

D. Laporan dan Dokumen Resmi

Badan Pembinaan Hukum Nasional (BPHN). (2024). Policy brief: Pengaturan kecerdasan artifisial dalam sistem hukum Indonesia. BPHN Kementerian Hukum RI.

Europol Innovation Lab. (2024). Law enforcement and the challenge of deepfakes. The Hague: Europol.

INTERPOL. (2024). Global cybercrime threat assessment 2024. Singapore: INTERPOL.

- Kepolisian Negara Republik Indonesia. (2025, Januari). Rilis pengungkapan kasus penipuan menggunakan deepfake Presiden RI dan Menteri Keuangan. Divisi Humas Polri.
- Majelis Hakim Pengadilan Negeri Jakarta Pusat. (2025). Putusan Perkara Nomor 123/Pid.Sus/2025/PN Jkt.Pst tentang tindak pidana siber deepfake. Jakarta: Pengadilan Negeri Jakarta Pusat.
- OECD. (2024). OECD artificial intelligence review 2024: Artificial intelligence, data and governance. Paris: OECD Publishing.
- UNESCO. (2024). Guidance for the governance of generative artificial intelligence. Paris: UNESCO.
- United Nations Office on Drugs and Crime (UNODC). (2024). Artificial intelligence and criminal justice system: Emerging challenges. Vienna: UNODC.
- World Economic Forum. (2025). Global cybersecurity outlook 2025. Geneva: World Economic Forum.

E. Sumber Lain (Wawancara/Diskusi)

- Dhiratara, A. (2024, Agustus 15). Tantangan dan dilema AI bagi media dan jurnalis [Diskusi Online]. CEO Hukumonline.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 July 2024.