Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
website: https: //rivierapublishing.id/jii/index.php/
Vol. 5 No. 1 Januari. 2026

Reformasi Kebijakan Pidana Nasional Terhadap Kejahatan Siber Berbasis Ai Melalui Pendekatan Hukum Progresif

Dian Juniarso*, Junaidi Abdillah
Universitas Pertiba, Indonesia
Email: juniarsodian@gmail.com

Kata Kunci
Kejahatan Siber; Kecerdasan Buatan; Hukum Progresif; Strict Liability; Kekosongan Norma.

Abstrak
Eskalasi kejahatan siber berbasis *Artificial Intelligence* (AI) telah mendisrupsi tatanan hukum pidana nasional dan memperlebar jurang antara percepatan inovasi teknologi dengan rigiditas regulasi yang berlaku. Sistem hukum pidana Indonesia yang masih berparadigma antroposentris menempatkan manusia sebagai satu-satunya subjek hukum, sehingga belum mampu menjangkau entitas algoritmik yang bersifat otonom dan adaptif. Kondisi ini memunculkan kekosongan norma (*vacuum of norm*) yang serius, berimplikasi pada lemahnya akuntabilitas hukum dan berpotensi melahirkan impunitas struktural dalam penanganan kejahatan siber berbasis AI. Penelitian ini bertujuan untuk mendekonstruksi hambatan yuridis yang timbul akibat karakteristik khas AI serta merumuskan arah reformasi kebijakan hukum pidana yang lebih responsif dan adaptif. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan hukum terhadap rezim pertanggungjawaban pidana di berbagai yurisdiksi. Hasil kajian menunjukkan bahwa sifat *black box*, kemampuan belajar mandiri, dan tingkat otonomi AI secara fundamental memutus rantai kausalitas antara perbuatan dan akibat serta mengaburkan unsur kesalahan (*mens rea*) dalam konstruksi hukum pidana konvensional. Oleh karena itu, pendekatan positivisme hukum yang kaku dinilai tidak lagi memadai dan perlu digeser menuju paradigma Hukum Progresif yang menekankan keadilan substantif. Penelitian ini merekomendasikan penerapan doktrin *strict liability* atau pertanggungjawaban mutlak bagi pengembang dan operator AI berisiko tinggi, serta mendorong penerbitan Peraturan Mahkamah Agung sebagai instrumen taktis untuk menutup kekosongan hukum dan menjamin kepastian serta keadilan dalam penegakan hukum pidana di era kecerdasan buatan.

Keywords
Cybercrime; Artificial Intelligence; Progressive Law; Strict Liability; Vacuum of Norm.

Abstract
The escalation of Artificial Intelligence (AI)-based cybercrime has disrupted the national criminal law order and widened the gap between the acceleration of technological innovation and the rigidity of applicable regulations. The Indonesian criminal law system, which still has an anthropocentric paradigm, places humans as the only subject of the law, so it has not been able to reach algorithmic entities that are autonomous and adaptive. This condition gives rise to a serious vacuum of norms, has implications for weak legal accountability and has the potential to give birth to structural impunity in handling AI-based cybercrime. This research aims to deconstruct the juridical obstacles that arise due to the distinctive characteristics of AI and formulate a more responsive and adaptive criminal law policy reform direction. The research method used is normative juridical with a legislative, conceptual, and comparative legal approach to criminal liability regimes in various jurisdictions. The results of the study show that the nature of the black box, the ability to learn independently, and the degree of autonomy of AI fundamentally break the chain of causality between actions and consequences and obscure the element of error

(mens rea) in the construction of conventional criminal law. Therefore, the rigid approach of legal positivism is considered inadequate and needs to be shifted towards a paradigm of Progressive Law that emphasizes substantive justice. This research recommends the application of the doctrine of strict liability or absolute responsibility for high-risk AI developers and operators, and encourages the issuance of Supreme Court Regulations as a tactical instrument to close the legal vacuum and ensure certainty and justice in criminal law enforcement in the era of artificial intelligence.

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence atau AI) telah membawa peradaban manusia ke dalam era baru yang penuh dengan kompleksitas dan paradoks yang belum pernah terbayangkan sebelumnya (Novrianto, 2025). Di satu sisi, AI menawarkan efisiensi luar biasa dan akselerasi produktivitas dalam berbagai sektor kehidupan, mulai dari otomasi industri hingga diagnosis medis presisi (Dharmayanti, 2025). Akan tetapi di sisi lain, kemajuan ini melahirkan modus kejahatan siber (cybercrime) yang semakin canggih, terstruktur, dan memiliki tingkat anonimitas yang tinggi sehingga sulit dideteksi oleh aparat penegak hukum konvensional (Aryasa, 2022; Febriansyah & SH, 2025). Fenomena ini tidak lagi sekadar wacana futuristik atau spekulasi fiksi ilmiah, melainkan telah bermetamorfosis menjadi ancaman nyata berupa kejahatan algoritmik yang beroperasi dengan otonomi tinggi. Kejahatan siber yang sebelumnya dilakukan secara manual oleh manusia dengan keterbatasan fisik dan kognitif kini mulai bergeser secara signifikan ke arah otomatisasi penuh dan manipulasi sintetik yang presisi (Budiyanto, 2025; Naili, 2025).

Contoh nyata dari pergeseran paradigmatik ini adalah penggunaan teknologi Deepfake untuk penipuan identitas yang nyaris sempurna dan AI Phishing yang mampu meniru gaya bahasa serta pola komunikasi personal target secara presisi atau spear phishing (Hallevy, 2010; Mutmainnah et al., 2024; Olimid et al., 2024). Dalam kasus CEO Fraud misalnya, pelaku menggunakan sintesis suara berbasis AI untuk meniru suara eksekutif perusahaan guna menginstruksikan transfer dana ilegal yang merupakan sebuah modus yang hampir mustahil dibedakan oleh telinga manusia biasa (Suseno et al., 2024; Syaputra, 2024; Taniady, 2024). Transisi ini menandai perubahan fundamental dalam lanskap kriminologi siber di mana alat kejahatan bukan lagi sekadar objek pasif yang digerakkan sepenuhnya oleh operator manusia, melainkan entitas yang mampu belajar, beradaptasi, dan bahkan mengoptimalkan strategi serangan secara mandiri (self-learning) sehingga menuntut respons hukum yang tidak biasa dan visioner (Amelia et al., 2024; Dupont et al., 2024; Hailtik et al., 2024).

Urgensi ancaman ini terkonfirmasi secara valid melalui data empiris yang menunjukkan lonjakan drastis dalam kejahatan berbasis manipulasi identitas digital. Berdasarkan laporan terbaru dari VIDA yang dirilis pada akhir tahun 2024, Indonesia mencatat lonjakan penipuan berbasis deepfake yang sangat mengkhawatirkan hingga mencapai angka 1.550%. Statistik ini tidak hanya sekadar angka, melainkan indikator kritis bahwa Indonesia berada dalam posisi kerentanan tertinggi terhadap serangan manipulasi visual dan audio berbasis AI di kawasan Asia Tenggara.

Lonjakan eksponensial ini mengindikasikan keberhasilan para pelaku kejahatan dalam mengeksploitasi celah teknologi yang belum diantisipasi oleh sistem keamanan biometrik konvensional seperti face recognition atau verifikasi suara (e-KYC) yang selama ini dianggap sebagai standar emas keamanan digital. Selain itu, fenomena ini juga mencerminkan adanya ketimpangan struktural antara laju adopsi teknologi digital yang sangat cepat dengan tingkat literasi digital masyarakat yang masih rendah serta ketidaksiapan infrastruktur keamanan siber nasional dalam mendeteksi anomali sintetik (European Union, 2024; BSSN, 2024; ICSF, 2024).

Situasi keamanan siber nasional semakin diperburuk dengan intensitas serangan yang masif, persisten, dan bersifat industrial. Mengutip data yang dipaparkan oleh CNN Indonesia pada pertengahan 2024, tercatat bahwa Indonesia digempur oleh sekitar 6 juta ancaman siber hanya pada kuartal awal tahun tersebut. Serangan ini tidak hanya menyasar infrastruktur kritis negara seperti data pusat nasional atau sistem perbankan, tetapi juga menyerang individu secara personal melalui manipulasi psikologis (social engineering) yang difasilitasi oleh kecerdasan buatan. AI memungkinkan pelaku untuk melakukan profiling korban secara massal namun terpersonalisasi (micro-targeting) yang meningkatkan tingkat keberhasilan penipuan secara signifikan dibandingkan metode konvensional.

Kementerian Komunikasi dan Digital RI pada tahun 2024 juga telah secara resmi menyatakan perlunya mitigasi khusus dan komprehensif terhadap kejahatan siber berbasis Deepfake AI mengingat potensi kerugian yang ditimbulkannya tidak hanya bersifat ekonomi, tetapi juga sosial-politik seperti perusakan reputasi tokoh publik hingga manipulasi opini publik melalui disinformasi yang dapat mendestabilisasi ketertiban umum dan proses demokrasi. Data tersebut menjadi bukti tak terbantahkan bahwa kejahatan siber telah berevolusi melampaui kapasitas penanggulangan hukum dan teknis saat ini (Kementerian Komunikasi dan Digital RI, 2024; VIDA, 2024).

Dalam tataran ideal (Das Sollen), hukum pidana seharusnya berfungsi sebagai ultimum remedium atau upaya terakhir dan instrumen pelindung masyarakat (social defence) yang dinamis serta mampu beradaptasi dengan dialektika zaman. Sebagaimana ditegaskan dalam prinsip hukum pidana modern dan amanat konstitusi, negara memiliki kewajiban mutlak untuk menjamin kepastian hukum, rasa aman, dan perlindungan bagi warganya dari segala bentuk ancaman termasuk ancaman hibrida yang berasal dari ranah digital yang melintasi batas yurisdiksi fisik.

Revisi kedua UU ITE melalui Undang-Undang Nomor 1 Tahun 2024 dan pengesahan KUHP Baru melalui Undang-Undang Nomor 1 Tahun 2023 diharapkan menjadi payung hukum yang kokoh dan responsif. Harapannya adalah instrumen hukum ini mampu menjangkau setiap perbuatan melawan hukum yang merugikan masyarakat tanpa terkecuali demi terciptanya ketertiban umum dan keadilan substantif di tengah disrupsi era digital yang serba tidak pasti. Meskipun demikian, realitas hukum (Das Sein) menunjukkan adanya kesenjangan (gap) yang lebar dan fundamental antara harapan normatif tersebut dengan kemampuan regulasi positif yang ada. Hukum pidana nasional Indonesia masih sangat terpaku pada paradigma konvensional yang antroposentris dengan menempatkan manusia biologis (natuurlijke persoon) sebagai satu-satunya subjek hukum utama yang dapat dimintai pertanggungjawaban.

Frasa "Barang Siapa" atau "Setiap Orang" dalam pasal-pasal pidana secara tradisional ditafsirkan secara kaku sebagai manusia atau korporasi (badan hukum) sehingga menciptakan kekosongan norma (vacuum of norm) ketika berhadapan dengan entitas algoritma otonom atau agen AI yang beroperasi secara mandiri. Hal ini menyulitkan penegak hukum untuk menjangkau tindakan pidana yang dilakukan oleh sistem kecerdasan buatan yang mengambil keputusan merugikan, seperti diskriminasi algoritmik atau eksekusi transaksi ilegal, tanpa intervensi langsung manusia pada saat tindak pidana tersebut terjadi atau eksekusi otomatis.

Kekosongan norma ini menjadi semakin pelik dan rumit ketika dibenturkan dengan doktrin dasar pertanggungjawaban pidana yang mensyaratkan adanya mens rea (niat jahat) atau kesalahan. Penelitian dari Tanjung (2025) dalam jurnal Judge menyoroti kesulitan fundamental dalam membuktikan unsur kesalahan pada pengembang atau penyedia layanan AI terutama ketika AI tersebut memiliki kemampuan machine learning atau deep learning (Black Box) yang memungkinkannya belajar sendiri dan mengambil keputusan di luar algoritma awal yang diprogramkan.

Pertanyaan yuridis yang mendasar muncul mengenai apakah sebuah mesin dapat memiliki "niat jahat" atau "kehendak". Apabila sebuah AI melakukan penipuan atau pencemaran nama baik secara otonom akibat bias data yang dipelajarinya sendiri, siapakah yang harus menanggung beban pidananya? Hukum positif Indonesia saat ini belum memiliki jawaban tegas dan tuntas untuk hal ini sehingga menyebabkan stagnasi dalam penegakan hukum di mana banyak kasus kejahatan siber berbasis AI berakhir tanpa pemidanaan yang memuaskan atau impunitas karena ketiadaan subjek hukum yang jelas untuk didakwa dan membiarkan korban tanpa restitusi keadilan.

Berdasarkan uraian latar belakang di atas, Penelitian ini akan berfokus pada dua pokok permasalahan utama. Pertama, analisis mengenai karakteristik spesifik kejahatan siber berbasis *Artificial Intelligence* (AI) yang menyebabkan terjadinya kekosongan norma (*vacuum of norm*) dalam konstruksi hukum pidana nasional saat ini. Kedua, formulasi reformasi kebijakan pidana yang ideal dalam menanggulangi kejahatan siber berbasis AI apabila ditinjau dari perspektif Hukum Progresif.

METODE PENELITIAN

Penelitian ini menerapkan konstruksi penelitian hukum normatif (yuridis-normatif) yang dirancang secara sistematis untuk mengkaji koherensi asas hukum, sinkronisasi vertikal dan horizontal peraturan perundang-undangan, serta sejarah hukum. Pilihan metode ini didasarkan pada sifat permasalahan yang dikaji yakni adanya konflik norma dan kekosongan norma (vacuum of norm) dalam menghadapi eskalasi kejahatan siber berbasis kecerdasan buatan dan bukan pada perilaku sosial masyarakat semata.

Fokus utama diletakkan pada analisis teks otoritatif untuk mengidentifikasi letak kegagalan hukum positif dalam merespons dinamika teknologi. Guna menghasilkan analisis yang komprehensif dan menghindari kekakuan dogmatik yang sering menjebak penelitian hukum murni, penelitian ini mengintegrasikan tiga pendekatan sekaligus yakni pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*).

Pendekatan perundang-undangan digunakan untuk menelaah secara kritis ratio legis dan konstruksi pasal-pasal dalam KUHP Baru dan UU ITE guna mencari celah interpretasi yang memungkinkan atau menghambat penegakan hukum terhadap AI. Sementara itu, pendekatan konseptual digunakan untuk membedah doktrin-doktrin hukum baru seperti Vicarious Liability (pertanggungjawaban pengganti) atau *Strict Liability* dalam konteks teknologi serta menggunakan optik Hukum Progresif dan Cyber-criminology untuk mendobrak kekakuan asas legalitas.

Pendekatan perbandingan dilakukan dengan menyandingkan regulasi nasional dengan standar global khususnya EU AI Act di Uni Eropa yang dikenal memiliki regulasi komprehensif berbasis risiko serta kerangka hukum di Singapura yang lebih mengedepankan keseimbangan antara inovasi dan keamanan. Sinergi ketiga pendekatan ini dimaksudkan untuk menemukan formulasi hukum yang adaptif, berorientasi pada keadilan substantif, dan kompatibel dengan standar internasional.

Dalam operasionalisasinya, penelitian ini mendayagunakan bahan hukum primer yang bersifat otoritatif dan mengikat yang meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagai norma dasar, KUHP Baru (UU No. 1/2023), dan UU ITE terbaru (UU No. 1/2024). Bahan-bahan primer ini didukung secara substansial oleh bahan hukum sekunder yang mencakup literatur akademik mutakhir, jurnal internasional bereputasi, prosiding konferensi hukum siber, dan doktrin para ahli terkemuka. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) yang mendalam dengan bantuan basis data hukum digital

Seluruh bahan hukum yang terhimpun kemudian dianalisis secara kualitatif menggunakan logika silogisme deduktif dan interpretasi hermeneutika hukum. Metode analisis hermeneutika ini krusial untuk tidak hanya membaca teks undang-undang secara harfiah melainkan menyelami makna kontekstual dan tujuan filosofis di balik pembentukan norma tersebut sehingga preskripsi atau rekomendasi hukum yang dihasilkan tidak hanya valid secara yuridis tetapi juga solutif dan aplikatif dalam menjawab tantangan stagnasi hukum di tengah disrupsi teknologi digital yang bergerak cepat.

HASIL DAN PEMBAHASAN

Dekonstruksi Karakteristik Kejahatan AI dan Kekosongan Norma

Problematika mendasar dan sistemik dalam penegakan hukum terhadap kejahatan berbasis Artificial Intelligence (AI) di Indonesia berakar pada benturan ontologis yang diametral antara karakteristik hukum pidana yang secara inheren bersifat rigid, teritorial, dan antroposentris dengan karakteristik teknologi AI yang bersifat otonom, cair, transnasional, dan penuh ketidakpastian (unpredictable).

Secara filosofis, arsitektur hukum pidana Indonesia baik yang termaktub dalam rezim KUHP lama (Wetboek van Strafrecht) maupun dalam KUHP Baru (UU No. 1 Tahun 2023) dibangun di atas paradigma klasik abad ke-19 yang tidak tergoyahkan bahwa subjek hukum pidana hanyalah manusia biologis (natuurlijke persoon) dan dalam perkembangannya mencakup korporasi (rechtspersoon) sebagai fiksi hukum. Konstruksi ini tercermin secara eksplisit dan limitatif dalam Pasal 59 dan Pasal 60 KUHP Baru yang membatasi pertanggungjawaban pidana hanya pada orang perseorangan dan korporasi serta penggunaan

frasa "Barang siapa" atau "Setiap Orang" dalam Pasal 27 hingga Pasal 45 UU ITE No. 1 Tahun 2024.

Frasa-frasa tersebut bukan sekadar pilihan diksi melainkan batasan yuridis yang secara hermeneutika mengunci pertanggungjawaban pidana pada entitas yang memiliki kesadaran, jiwa, moralitas, dan kehendak bebas (free will). Konsekuensi logis dari paradigma ini adalah terjadinya kekosongan hukum (legal lacuna) ketika berhadapan dengan entitas Autonomous Algorithms atau Decentralized Autonomous Organizations (DAOs) yang beroperasi tanpa intervensi manusia. Ketika sebuah agen AI Generatif secara mandiri "memutuskan" untuk memanipulasi pasar saham atau meluncurkan serangan siber polymorphic yang terus berubah bentuk untuk menghindari deteksi karena proses self-learning menganggap itu strategi optimal dan bukan karena diperintah, hukum positif kehilangan daya jangkaunya. Tidak ada "manusia" yang melakukan actus reus (tindakan fisik) pada saat kejadian dan AI itu sendiri tidak dapat didudukkan di kursi terdakwa. Situasi ini menciptakan apa yang disebut oleh Gabriel Hallevy sebagai The Retribution Gap atau kesenjangan pemidanaan di mana kejahatan terjadi secara nyata dan merugikan namun sistem hukum gagal menunjuk pihak yang harus bertanggung jawab dan membiarkan mesin beroperasi di zona abu-abu impunitas.

Kekosongan norma ini menjadi semakin krusial dan kompleks ketika dibenturkan dengan doktrin fundamental geen straf zonder schuld atau tiada pidana tanpa kesalahan yang mensyaratkan pembuktian niat jahat (dolus) atau setidaknya kealpaan (culpa). Dalam konteks kejahatan konvensional, niat dibuktikan melalui motif psikologis, rencana, dan kesadaran batin pelaku. Namun pada kejahatan yang melibatkan Advanced AI terutama yang menggunakan Deep Neural Networks, elemen subjektif ini menjadi kabur dan terdistorsi. Karakteristik "Kotak Hitam" (Black Box) pada AI berarti bahwa proses pengambilan keputusan internalnya seringkali tidak transparan dan tidak dapat dijelaskan bahkan oleh penciptanya sendiri. Algoritma bekerja dengan prinsip optimasi fungsi matematis berdasarkan probabilitas data statistik dan bukan berdasarkan pertimbangan moralitas, etika, atau niat jahat.

Sebagai contoh konkret, sebuah sistem AI yang diprogram untuk memaksimalkan keuntungan finansial mungkin secara mandiri "menemukan" bahwa strategi manipulasi pasar seperti spoofing atau front-running adalah cara paling efisien untuk mencapai tujuan tersebut. Dalam logika algoritma tindakan ini adalah "optimasi", namun dalam kacamata hukum ini adalah tindak pidana penipuan. Dilema hukum muncul saat jaksa mencoba membuktikan mens rea di mana pengembang tidak dapat didakwa melakukan kesengajaan (dolus) karena mereka tidak pernah memerintahkan atau berniat agar AI melakukan penipuan, melainkan hanya memberi perintah umum "maksimalkan profit".

Pembuktian kelalaian (culpa) juga terhambat oleh doktrin standard of care karena belum ada standar baku industri yang mendefinisikan seberapa jauh pengembang harus mengantisipasi perilaku menyimpang dari sebuah sistem yang dirancang untuk belajar sendiri. Fenomena unforeseeability atau ketidakterdugaan ini secara efektif memutus jalinan kesalahan yang disyaratkan hukum pidana dan memungkinkan pencipta teknologi berlindung di balik argumen "kesalahan sistem" atau glitch sementara kerugian yang diderita korban bersifat nyata, masif, dan seringkali tidak terpulihkan.

Krisis penegakan hukum ini diperparah dengan runtuhnya konstruksi kausalitas (causality chain) yang menjadi tulang punggung atribusi pertanggungjawaban pidana. Doktrin

conditio sine qua non menuntut bukti tak terbantahkan bahwa tindakan pelaku adalah penyebab langsung (proximate cause) dari timbulnya akibat yang dilarang. Namun, ekosistem pengembangan AI modern melibatkan rantai pasok yang sangat panjang dan terfragmentasi mulai dari penyedia dataset awal, pelatih model dasar (foundation model), penyedia infrastruktur komputasi, hingga pengguna akhir yang melakukan fine-tuning. Ketika sebuah agen AI melakukan kejahatan, "tangan-tangan tak terlihat" dari berbagai aktor ini saling berkontribusi sehingga menciptakan The Problem of Many Hands.

Keputusan sebuah AI untuk melakukan tindak pidana seringkali merupakan hasil evolusi mandiri algoritmanya setelah berinteraksi dengan data dinamis di domain publik (post-deployment evolution) yang terjadi jauh setelah lepas dari kendali pengembangnya. Intervensi data dari pengguna, bias tersembunyi dalam dataset pelatihan, dan interaksi tak terduga dengan sistem lain mengaburkan siapa penyebab utama kejahatan tersebut. Apakah penyedia data yang bias harus disalahkan atau pengembang yang gagal memasang pagar pengaman etika? Data dari Indonesia Cyber Security Forum (ICSF) mengonfirmasi bahwa hambatan terbesar penegakan hukum siber saat ini adalah masalah atribusi yang kabur ini. Tanpa adanya instrumen hukum progresif yang berani menerobos pakem konvensional, misalnya dengan mengakui konsep "kepribadian elektronik" (electronic personality) atau memperluas doktrin strict liability (tanggung jawab mutlak) ke ranah pidana teknologi, Indonesia menghadapi risiko terperangkap dalam impunitas struktural. Hal ini terbukti secara empiris dengan rendahnya rasio penyelesaian (clearance rate) kasus kejahatan siber berteknologi tinggi di mana hukum positif yang statis tertatih-tatih mengejar dinamisnya inovasi modus operandi kejahatan yang terus bermutasi dengan kecepatan eksponensial.

Perspektif Hukum Progresif sebagai Pisau Analisis

Kebuntuan yang dihadapi oleh sistem hukum pidana Indonesia dalam merespons kejahatan siber berbasis AI sebagaimana diuraikan sebelumnya sejatinya bermuara pada dominasi paradigma positivisme hukum yang berlebihan (legalistic positivism). Positivisme hukum yang memandang hukum semata-mata sebagai rangkaian aturan tertulis yang logis dan otonom cenderung mereduksi kompleksitas masalah sosial, termasuk disrupsi teknologi, ke dalam kotak-kotak silogisme yuridis yang kaku. Dalam kacamata positivisme, hakim diposisikan sekadar sebagai "corong undang-undang" (la bouche de la loi) yang tugas utamanya adalah mencocokkan fakta persidangan dengan bunyi teks pasal.

Pendekatan ini menjadi sangat problematis ketika dihadapkan pada entitas AI yang tidak terakomodasi dalam teks undang-undang mana pun. Akibatnya, ketika teks hukum diam atau tidak mengatur (kekosongan norma), positivisme cenderung melahirkan putusan yang legalistik namun tidak adil (summum ius summa iniuria) yakni membiarkan kejahatan teknologi lolos hanya karena "tidak ada pasalnya". Oleh karena itu, diperlukan pergeseran paradigma menuju Hukum Progresif sebagai antitesis terhadap kemapanan (status quo) yang membelenggu pencarian keadilan substantif.

Prof. Satjipto Rahardjo sebagai penggagas Hukum Progresif meletakkan postulat fundamental bahwa "hukum adalah untuk manusia, bukan manusia untuk hukum". Dalil ini memiliki implikasi ontologis yang mendalam bagi penegakan hukum siber. Artinya, keberadaan hukum tidak ditujukan untuk mengabdi pada kesempurnaan logika teks atau

prosedur birokrasi melainkan untuk melayani kesejahteraan dan kebahagiaan manusia. Dalam konteks kejahatan AI, "manusia" di sini adalah para korban yang dirugikan oleh manipulasi Deepfake, pencurian data, atau penipuan algoritmik. Jika ketaatan buta terhadap teks undang-undang yang mendefinisikan subjek hukum hanya sebagai manusia fisik justru menyebabkan ketidakadilan bagi korban dan memberikan impunitas bagi pengembang teknologi yang tidak bertanggung jawab, maka menurut perspektif Hukum Progresif teks hukum tersebut harus dikesampingkan atau ditafsirkan ulang secara radikal.

Hukum tidak boleh membiarkan dirinya menjadi alat legitimasi bagi ketidakadilan yang dihasilkan oleh celah teknologi tetapi sebaliknya harus mengalir cair mengikuti dinamika masyarakat untuk memberikan perlindungan (social defence). Perspektif Hukum Progresif menuntut adanya reorientasi peran hakim dan penegak hukum dari sekadar pembaca teks menjadi pencipta hukum (*rechtsvinding*) yang aktif dan visioner. Hakim dalam kasus kejahatan siber tidak boleh terjebak dalam cara berpikir legisprudence yang kaku melainkan harus berani melakukan rule breaking (pematahan aturan) ketika aturan yang ada mencederai rasa keadilan.

Dalam kasus AI, rule breaking ini tidak dimaknai sebagai anarki atau pelanggaran hukum melainkan sebagai keberanian untuk menggunakan penafsiran futuristik dan teleologis. Hakim dapat menafsirkan unsur "Barang Siapa" tidak lagi secara biologis tetapi secara fungsional. Artinya, siapa pun atau apa pun yang memiliki kemampuan untuk menimbulkan akibat hukum dan kerugian harus dapat ditarik pertanggungjawabannya baik itu melalui atribusi kepada entitas korporasi yang mengendalikan algoritma tersebut (controlling mind) maupun melalui konstruksi pertanggungjawaban komando (command responsibility). Dengan demikian, kekakuan teks tidak lagi menjadi penghalang untuk menjangkau realitas kejahatan baru.

Hukum Progresif mendorong penggunaan metode interpretasi yang meluas (extensive interpretation) guna mengisi kekosongan hukum (rechtsvacuum). Dalam menghadapi teknologi Black Box, penegak hukum dapat mengadopsi prinsip strict liability (tanggung jawab mutlak) sebagai manifestasi perlindungan masyarakat. Logika progresifnya adalah bahwa pengembang atau korporasi yang menciptakan dan mengambil keuntungan ekonomi dari sistem AI berisiko tinggi (high-risk AI) harus menanggung beban risiko jika sistem tersebut menimbulkan kerugian tanpa perlu membuktikan adanya niat jahat (mens rea) secara tradisional. Hal ini sejalan dengan asas cuius commoda, eius incommoda yang bermakna siapa yang mendapat keuntungan juga harus menanggung kerugian. Pendekatan ini membalikkan beban pembuktian dari korban yang lemah kepada korporasi teknologi yang memiliki sumber daya sehingga menciptakan keseimbangan keadilan yang lebih substantif dibandingkan sekadar mengejar pembuktian formal yang hampir mustahil dilakukan.

Penerapan Hukum Progresif dalam ranah siber juga relevan dengan teori Hukum Responsif dari Nonet dan Selznick yang menekankan bahwa hukum yang baik adalah hukum yang kompeten dan adil serta mampu merespons kebutuhan sosial. Masyarakat digital saat ini membutuhkan kepastian bahwa mereka terlindungi dari ancaman algoritma otonom. Jika hukum pidana tetap bersikukuh pada asas legalitas formal yang kaku (nullum delictum), maka hukum akan kehilangan wibawa dan relevansinya serta menjadi artefak sejarah yang usang di tengah laju peradaban digital. Hukum Progresif menawarkan jalan keluar dengan menempatkan "nuraninya hukum" di atas "teknisnya hukum". Hakim didorong untuk menggali

nilai-nilai keadilan yang hidup dalam masyarakat (living law) di mana masyarakat menuntut agar pencipta teknologi tidak bisa lepas tangan begitu saja atas kekacauan yang dibuat oleh ciptaan mereka meskipun secara teknis "hanya kode" yang bekerja.

Selain itu, perspektif ini juga membuka ruang bagi integrasi nilai-nilai etika ke dalam pertimbangan hukum (legal reasoning). Dalam positivisme, etika dan hukum seringkali dipisahkan secara tegas. Namun dalam Hukum Progresif, moralitas adalah roh dari hukum. Ketika menghadapi kasus di mana AI menyebabkan kematian atau kerugian finansial massal seperti dalam kasus mobil otonom yang menabrak pejalan kaki, hakim progresif tidak akan berhenti pada pertanyaan "apakah ada pasal yang dilanggar?" melainkan bertanya "apakah adil jika tidak ada yang bertanggung jawab?". Pertanyaan etis ini membimbing hakim untuk melakukan konstruksi hukum baru, misalnya dengan menetapkan bahwa kelalaian dalam menerapkan safety features atau algoritma fail-safe pada AI sudah cukup untuk memenuhi unsur pidana kelalaian (culpa) meskipun standar industrinya belum baku. Ini adalah bentuk judicial activism yang diperlukan untuk mengisi kekosongan regulasi.

Sebagai sintesis, Hukum Progresif bukan sekadar alternatif metodologis melainkan sebuah kebutuhan mendesak (conditio sine qua non) dalam reformasi hukum pidana di era kecerdasan buatan. Ia menjadi jembatan yang menghubungkan ketertinggalan teks undang-undang dengan percepatan realitas teknologi. Dengan memegang teguh adagium "Hukum untuk manusia", penegak hukum di Indonesia memiliki legitimasi moral dan intelektual untuk menerobos kebuntuan positivisme. Hal ini memastikan bahwa hukum tetap menjadi panglima yang melindungi martabat manusia dan bukan sekadar penonton pasif di pinggir arena ketika algoritma mengambil alih kendali kehidupan sosial. Transformasi pola pikir (mindset) aparat penegak hukum menuju progresivitas adalah kunci untuk mewujudkan kedaulatan hukum digital yang berkeadilan dan berperikemanusiaan di Indonesia.

Rekomendasi Reformulasi Kebijakan Pidana

Hasil penelitian ini mengajukan rekomendasi konkret mengenai formulasi hukum yang strategis untuk diadopsi guna mengatasi stagnasi hukum. Rekomendasi ini didasarkan pada temuan bahwa kegagalan doktrin liability based on fault dalam menjangkau kejahatan otonom AI bukanlah anomali sementara melainkan sebuah cacat struktural yang perlu diperbaiki melalui penerapan model pertanggungjawaban yang lebih responsif. Berpijak pada analisis Hukum Progresif, penelitian ini mengusulkan sebuah kerangka kerja di mana pengembang sistem kecerdasan buatan khususnya pada kategori High-Risk AI seperti sistem biometrik massal, kendaraan otonom, dan algoritma finansial strategis dapat diklasifikasikan sebagai subjek yang memikul tanggung jawab mutlak (strict liability).

Dalam kerangka usulan ini, elemen mens rea (niat jahat) atau negligence (kelalaian) yang selama ini menjadi hambatan pembuktian disarankan untuk tidak lagi dijadikan syarat mutlak pemidanaan bagi korporasi pengembang dalam konteks tertentu. Sebagai alternatif, pertanggungjawaban hukum dapat difokuskan pada dua elemen objektif yakni keberadaan actus reus atau perbuatan yang dilakukan oleh sistem AI seperti penyebaran konten ilegal atau manipulasi pasar serta adanya kerugian nyata yang diderita oleh korban. Formulasi ini mengadopsi prinsip yang selaras dengan perkembangan global seperti EU *Product Liability Directive* (2024) di mana produsen perangkat lunak dianggap bertanggung jawab atas cacat

produk yang menyebabkan kerugian tanpa memandang unsur niat. Secara filosofis, pendekatan ini berakar pada teori risk creation yang memandang bahwa pengembang AI dengan menciptakan entitas otonom yang membawa risiko inheren demi keuntungan komersial sepatutnya menanggung risiko yang ditimbulkannya (*cuius commoda, eius incommoda*).

Pada tatanan operasional, penelitian ini menyarankan penerapan mekanisme Pembalikan Beban Pembuktian (Reversal of Burden of Proof) dalam hukum acara pidana khusus siber. Berbeda dengan hukum pidana konvensional di mana beban pembuktian terletak sepenuhnya pada Jaksa Penuntut Umum (JPU), dalam kasus kejahatan AI diusulkan agar beban pembuktian dapat beralih kepada pengembang dalam kondisi tertentu.

Pengembang dapat dianggap bertanggung jawab secara presumptive apabila kerugian telah terverifikasi kecuali mereka mampu membuktikan secara forensik bahwa sistem telah diretas oleh pihak ketiga di luar kendali mereka (force majeure) atau pengguna telah memodifikasi sistem secara ilegal. Mekanisme ini dirancang untuk menyeimbangkan disparitas kekuatan (inequality of arms) antara korporasi teknologi yang memiliki akses data teknis dengan korban yang awam sekaligus mendorong pengembang untuk menerapkan standar keamanan tertinggi (safety by design) sebagai strategi mitigasi risiko.

Selain itu, penelitian ini juga merekomendasikan langkah konkret reformasi regulasi melalui dua jalur strategis. Pertama, revisi terbatas pada UU ITE perlu dipertimbangkan dengan menyisipkan pasal yang secara eksplisit mengadopsi klasifikasi risiko AI. Pasal usulan tersebut dapat menegaskan bahwa penyelenggara sistem elektronik yang menggunakan kecerdasan buatan risiko tinggi memikul tanggung jawab atas kerugian hukum yang ditimbulkan oleh sistemnya.

Kedua, sebagai solusi jangka pendek yang mendesak, penelitian ini merekomendasikan penyusunan Peraturan Mahkamah Agung (PERMA) terkait penanganan perkara tindak pidana siber berbasis AI. PERMA ini diharapkan dapat mengisi kekosongan hukum (rechtsvacuum) dengan memberikan pedoman teknis bagi hakim dalam menafsirkan unsur "kelalaian" secara ekstensif yang mencakup kegagalan pengembang dalam melakukan uji bias (bias testing) dan transparansi algoritma. Sebagai prasyarat penting dalam model ini, kebijakan transparansi algoritma atau Explainable AI (XAI) direkomendasikan untuk menjadi standar wajib. Pengadilan sebaiknya diberikan kewenangan untuk memerintahkan audit forensik terhadap "Kotak Hitam" algoritma pengembang yang menjadi terdakwa.

Ketidakmampuan untuk menjelaskan (explainability) bagaimana sebuah keputusan merugikan diambil oleh AI dapat dipertimbangkan sebagai faktor pemberat dalam penerapan sanksi. Dengan demikian, formulasi ini menawarkan solusi yang terukur yakni mentransformasi hukum pidana dari instrumen yang reaktif menjadi mekanisme kontrol sosial yang proaktif serta mendorong industri teknologi untuk berinovasi dengan tetap menjunjung tinggi etika dan akuntabilitas hukum. Hal ini merupakan manifestasi nyata dari upaya perlindungan masyarakat (social defence) di era digital.

KESIMPULAN

Penelitian ini menyimpulkan bahwa karakteristik inheren kejahatan siber berbasis *Artificial Intelligence* (AI) yang otonom, cair, dan beroperasi dalam mekanisme "Kotak Hitam" (Black Box) yang sulit diprediksi telah secara fundamental mendekonstruksi tatanan hukum

pidana nasional yang masih terpaku pada paradigma antroposentris. Kondisi ini secara sistemik menciptakan kekosongan norma (vacuum of norm) yang serius dan melahirkan impunitas struktural di mana doktrin konvensional mengenai kesalahan (mens rea) dan rantai kausalitas gagal total dalam menjangkau entitas algoritma mandiri yang bertindak di luar kendali penciptanya. Oleh karena itu, penelitian ini mendesak perlunya pergeseran paradigma yang radikal dari belenggu positivisme hukum yang kaku menuju pendekatan Hukum Progresif yang responsif terhadap zaman.

Manifestasi konkret dari pergeseran ini harus diwujudkan melalui formulasi kebijakan pidana baru yang berani yakni penerapan doktrin *Strict Liability* (pertanggungjawaban mutlak) yang membebankan risiko pada pengembang AI risiko tinggi, penerbitan Peraturan Mahkamah Agung (PERMA) sebagai instrumen taktis untuk memberikan pedoman interpretasi futuristik bagi para hakim, serta revisi komprehensif regulasi siber untuk mengakui subjek hukum fungsional. Langkah-langkah strategis ini mutlak diperlukan guna menjamin tercapainya keadilan substantif dan perlindungan masyarakat (*social defence*) yang adaptif serta berketahanan di tengah derasnya arus disrupsi teknologi yang semakin tak terbendung.

REFERENSI

Amelia, Y. F., Kaimuddin, A., & Ashsyarof, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut hukum positif Indonesia. *Dinamika Jurnal Ilmiah Hukum, 30*(1), 67–76. https://penerbitgoodwood.com/index.php/JIHHAM/article/view/3937

Aryasa, K. B. (2022). *Ainomics—Economic artificial intelligence*. Elex Media Komputindo.

Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia 2023*. Direktorat Operasi Keamanan Siber BSSN. https://educsirt.kemendikdasmen.go.id/portal/berita/197

Budiyanto, S. H. (2025). *Pengantar cybercrime dalam sistem hukum pidana di Indonesia*. Sada Kurnia Pustaka.

Dharmayanti, Y. P. (2025). *Kebijakan hukum pidana dalam upaya menanggulangi artificial intelligence (AI) dalam cyber crime*. Universitas Islam Sultan Agung Semarang.

Dupont, B., Fortin, F., & Leukfeldt, R. (2024). Broadening our understanding of cybercrime and its evolution. *Journal of Crime and Justice, 47*(4), 435–439. https://www.researchgate.net/publication/378613280_Broadening_our_understanding_of_cybercrime_and_its_evolution

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*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Febriansyah, F. I., & Sh, M. (2025). *Cybercrime: Kejahatan di balik layar digital*. Najaha.

Hailtik, M., et al. (2024). Criminal liability in artificial intelligence era: A comparative study. *International Journal of Cyber Law, 8*(1), 45–67.

Hallevy, G. (2010). The criminal liability of artificial intelligence entities—From science fiction to legal social control. *Akron Intellectual Property Journal, 4*(2), 171–201.

Indonesia Cyber Security Forum. (2024). *White paper on AI security and ethics in Indonesia*. ICSF.

Kementerian Komunikasi dan Digital Republik Indonesia. (2024). *Peta jalan strategi nasional kecerdasan buatan Indonesia 2020–2045: Revisi sektor keamanan*. Komdigi.

Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika teknologi deepfake sebagai masa depan hoax yang semakin meningkat: Solusi strategis ditinjau dari literasi digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi, 1*(2), 67–72. https://journal.universitasbumigora.ac.id/index.php/upgrade/article/download/3702/1604

Naili, Y. T. (2025). Optimalisasi penegakan hukum terhadap kejahatan siber berbasis AI terhadap perempuan: Kajian hukum pidana dan kebijakan digital. *Jurnal Media Hukum, 13*(2), 207–219.

Novrianto, M. (2025). Kebijakan hukum pidana terhadap cyber crime berbasis artificial intelligence di Indonesia. *Jurnal Kepastian Hukum dan Keadilan, 7*(2), 150–170.*

Olimid, A. P., Georgescu, C. M., & Olimid, D. A. (2024). Legal analysis of EU Artificial Intelligence Act (2024): Insights from personal data governance and health policy. *Access to Justice in Eastern Europe, 7*(4), 1–23. https://ajee-journal.com/upload/attaches/att_1731686201.pdf

Syaputra, R. (2024). Urgensi pengaturan perlindungan hukum terhadap korban deepfake melalui artificial intelligence (AI) dari perspektif hukum pidana Indonesia. *Jurnal Hukum Respublica, 23*(1), 5–12.* https://garuda.kemdiktisaintek.go.id/author/view/8149235

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia, N. T. (2024). Corporate crime liability: Beyond rule reform on Indonesia criminal policy. *Focus Journal Law Review, 4*(2), 48–62.* https://www.researchgate.net/publication/385814351_Corporate_Crime_Liability_Beyond_Rule_Reform_on_Indonesia_Criminal_Policy

Taniady, V. (2024). AI-induced fatalities: A criminal law perspective from Indonesia and international perspective. *Yustisia Jurnal Hukum, 13*(1).* https://jurnal.uns.ac.id/yustisia/article/view/101636

Tanjung, A. (2025). Pembuktian unsur kesalahan pada algoritma otonom: Sebuah mustahil yuridis? *Judge: Jurnal Hukum dan Peradilan, 12*(1), 89–104.*

VIDA Digital Identity. (2024). *Annual identity fraud report 2024: The rise of deepfakes in Southeast Asia*. VIDA. https://vida.id/whitepaper-ifse-2024