PERTANGGUNGJAWABAN PIDANA ATAS KEJAHATAN KECERDASAN BUATAN (*ARTIFICIAL INTELLIGENCE CRIME*) DALAM SISTEM HUKUM INDONESIA [1]

Oleh :
Bunga Aprillia Paputungan [2]
Hendrik Pondaag [3]
Ollij A. Kereh [4]

ABSTRAK

Penelitian ini bertujuan untuk Untuk mengetahui dan memahami pengaturan kecerdasan buatan dalam sistem hukum Indonesia dan untuk mengetahui dan memahami pertanggungjawaban pidana terhadap tindak kejahatan dalam sistem kecerdasan buatan. Dengan menggunakan metode penelitian yuridis empiris, dapat ditarik kesimpulan yaitu : 1. Hingga saat ini Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai kecerdasan buatan (*Artificial Intelligence*). Meskipun demikian, berbagai ketentuan hukum positif, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta berbagai regulasi sektoral lainnya, telah memberikan dasar hukum yang dapat digunakan untuk mengatur penyalahgunaan teknologi AI sepanjang memenuhi unsur tindak pidana yang telah diatur dalam peraturan perundang-undangan. 2. Pertanggungjawaban pidana terhadap kejahatan yang memanfaatkan sistem kecerdasan buatan pada prinsipnya tetap dibebankan kepada manusia atau korporasi yang secara sengaja mengembangkan, mengendalikan, menggunakan, atau menyalahgunakan teknologi tersebut untuk melakukan tindak pidana. Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel menunjukkan bahwa hakim tetap menerapkan asas legalitas dan asas kesalahan dengan membebankan pertanggungjawaban pidana kepada pelaku yang secara sadar memanfaatkan sistem pengenalan wajah berbasis AI untuk melakukan akses ilegal terhadap layanan perbankan digital.

Kata Kunci : *kejahatan, kecerdasan buatan, sistem hukum indonesia*

PENDAHULUAN

A. Latar Belakang

Perkembangan pesat teknologi kecerdasan buatan (*Artificial Intelligence / AI*) telah menciptakan bentuk-bentuk kriminalitas baru yang sebelumnya sulit dibayangkan dari *deepfake* (media sintetis yang memalsukan wajah/suara), penggunaan bot untuk penipuan dan skimming, hingga keputusan otomatis yang menyebabkan kerugian ekonomi atau pelanggaran hak asasi.[5] Kejahatan yang memanfaatkan atau dihasilkan oleh teknologi AI menimbulkan persoalan klasik dalam hukum pidana: siapa yang harus dipidana dan atas dasar doktrin apa apabila kerugian dihasilkan oleh sistem yang berjalan otonom atau semi-otonom?[6]

Secara dogmatis, pertanggungjawaban pidana mensyaratkan terdapatnya perbuatan yang memenuhi unsur delik (*actus reus)* dan kesalahan (*mens rea*) pada subjek hukum yang dapat dipersalahkan. Namun, AI sebagai entitas teknologi tidak memiliki kapasitas mental untuk menaruh kesalahan; sehingga penerapan ketentuan KUHP atau peraturan pidana khusus terhadap kejadian yang melibatkan AI menuntut adaptasi doktrinal (mis. teori tindakan manusia di balik mesin, teori tanggung jawab kawal, atau model *strict liability* bagi penyelenggara). Tantangan ini makin nyata bila AI mengubah atau mempercepat skenario kejahatan (mis. otomatisasi penipuan) sehingga seringkali tindakan melibatkan banyak aktor: developer, operator, penyedia platform, dan pihak ketiga pengguna.[7]

Di lingkungan regulasi Indonesia, belum terdapat ketentuan pidana yang dengan tegas mengatur “AI” sebagai sumber tindak pidana atau sebagai pemilik kewajiban pidana. Sebaliknya, aparat penegak menggunakan norma-norma eksisting seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), KUHP, Undang-Undang Pornografi, UU Pelindungan Data Pribadi untuk menjerat perbuatan yang memanfaatkan teknologi AI. Pendekatan *patchwork* ini efektif secara kasus-per-kasus, tetapi menyisakan masalah kepastian hukum dan kesesuaian norma (mis. pembuktian peran algoritma, alur tanggung jawab, dan proporsionalitas sanksi).[8]

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010151
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Ryan Calo, ‘Robots and the Lessons of Cyberlaw’, *California Law Review*, Vol. 103, 2015, hlm. 513–516
[6] OECD, *Artificial Intelligence in Society: Opportunities and Challenges*, OECD Publishing, Paris, 2021, hlm. 5–7
[7] Cary Coglianese & David Lehr, ‘Regulating by Robot: Administrative Decision Making in the Machine-Learning Era’, *Georgetown Law Journal*, Vol. 105, 2017, hlm. 123–125
[8] N.P.M. Putri, “Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake”, *JPSS* Undiksha, 2024, hlm. 10–14

Dari perspektif kebijakan, ada tekanan ganda: negara perlu mendorong inovasi teknologi (untuk daya saing ekonomi) tetapi juga wajib menjamin perlindungan hukum terhadap korban dan publik.[9] Beberapa solusi yang dibahas di literatur internasional mencakup pengaturan berbasis risiko (*risk-based regulation*), kewajiban transparansi algoritmik dan audit independen, serta reformulasi norma pidana untuk memasukkan konsep kontribusi teknologi sebagai faktor pembantu tindak pidana. Namun, transformasi norma pidana memerlukan kehati-hatian agar tidak menciptakan kriminalisasi berlebihan atau mematikan inovasi produktif.

Permasalahan praktis di pengadilan juga menonjol: pembuktian forensik digital atas keterlibatan AI, identifikasi aktor yang memiliki kontrol teknis, dan penerapan unsur kesengajaan/kelalaian yang memenuhi standar pidana. Selain itu, penanganan perkara yang melibatkan bukti algoritmik dan data training memunculkan kebutuhan kapabilitas forensik yang belum merata di aparat penegak hukum.[10] Oleh sebab itu kajian mendalam mengenai bagaimana sistem hukum pidana Indonesia bisa merespon kejahatan yang melibatkan AI baik melalui interpretasi normatif, reformasi perundang-undangan, maupun mekanisme non-pidana (administratif, perdata, remedial) menjadi sangat relevan untuk penelitian hukum.

Penelitian ini bertujuan mengkaji celah-celah (*lacunae*) dalam tatanan hukum pidana Indonesia ketika dihadapkan pada kejahatan berbasis atau yang dipermudah oleh AI, menganalisis model-model pertanggungjawaban pidana (mis. *attribution to human actor, corporate liability, strict liability*), dan merekomendasikan kerangka normatif yang seimbang antara prinsip keadilan pidana dan kebutuhan regulasi teknologi. Kajian empirik berupa studi kasus putusan pengadilan di Indonesia yang relevan dengan konten sintetis/manipulasi informasi digital akan menjadi bahan untuk menilai bagaimana pengadilan mengisi kekosongan regulasi (*gap-filling*) dalam praktik.[11]

Contoh nyata yang terjadi di Indonesia yakni Kasus Penyalahgunaan Data Wajah dan Sistem Pengenalan Otomatis (*Face Recognition Fraud*): Putusan PN Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel. Kasus ini berkaitan dengan penggunaan teknologi pengenalan wajah

[9] Julia Black, *Risk and Regulation*, *Journal of Law and Society*, Vol. 27, No. 2, 2000, hlm. 325–327

[10] Marinews Mahkamah Agung, "Kejahatan Siber Deepfake di Era Kecerdasan Buatan", 7 Mei 2025, hlm. 2–4

[11] D. Noviantama, *Deepfake: A Review from The Victimology Perspective*, *CICL Journal*, 2025, hlm. 12–15

(*facial recognition*) untuk melakukan akses ilegal ke sistem perbankan daring (*mobile banking*). Meskipun pelaku tidak menggunakan AI untuk membuat keputusan otonom, teknologi yang digunakan merupakan bagian dari sistem otomatis berbasis *machine learning* untuk mengenali wajah pengguna. Kronologinya yakni berdasarkan fakta di persidangan, terdakwa melakukan pencurian data wajah korban (melalui video call palsu) dan kemudian menggunakan perangkat lunak pengenalan wajah yang dimodifikasi agar dapat melewati sistem keamanan aplikasi perbankan digital. Dengan cara tersebut, terdakwa berhasil melakukan transfer dana tanpa izin ke rekening lain. Dasar hukum: Jaksa mendakwa terdakwa dengan Pasal 30 ayat (1) dan (2) UU ITE tentang akses ilegal terhadap sistem elektronik dan Pasal 81 UU Perbankan. Pertimbangan hakim: Hakim Pengadilan Negeri Jakarta Selatan menyatakan bahwa terdakwa terbukti melakukan akses ilegal dan menyalahgunakan sistem elektronik. Hakim juga menegaskan bahwa meskipun sistem keamanan bank menggunakan *AI-based verification*, pelaku tetap harus bertanggung jawab karena secara sadar memanipulasi sistem tersebut dengan niat jahat (*mens rea*).

Relevansi hukum dalam kasus ini yaitu memperlihatkan kompleksitas hubungan antara manusia dan sistem otomatis. Meskipun AI hanya berperan sebagai alat, interaksi dengan pelaku manusia menimbulkan pertanyaan baru tentang sejauh mana tanggung jawab dapat dibebankan kepada manusia, pengembang sistem, atau penyelenggara jasa keuangan.[12]

B. Rumusan Masalah

1. Bagaimana pengaturan kecerdasan buatan (AI) dalam sistem hukum Indonesia?
2. Bagaimana pertanggungjawaban pidana terhadap tindak kejahatan dalam sistem kecerdasan buatan (AI)?

C. Metode Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah Metode Yuridis Normatif.

PEMBAHASAN

A. Pengaturan Kecerdasan Buatan (AI) Dalam Sistem Hukum Indonesia

Kecerdasan Buatan atau *Artificial Intelligence* (AI) merupakan salah satu perkembangan teknologi digital yang membawa perubahan besar terhadap kehidupan manusia, termasuk dalam bidang hukum pidana. AI pada

[12] A. Santoso, "Pertanggungjawaban Pidana dalam Kejahatan Berbasis Artificial Intelligence", *Jurnal Lex Crimen*, Vol. XII, No. 4, 2024, hlm. 24–26.

dasarnya merujuk pada sistem komputer atau mesin yang dirancang untuk meniru kemampuan kognitif manusia, seperti mengenali pola, mengambil keputusan, memproses bahasa, menganalisis data, dan melakukan prediksi berdasarkan algoritma tertentu. Perkembangan AI tidak hanya digunakan dalam sektor industri, kesehatan, pendidikan, dan transportasi, tetapi juga dalam sektor keamanan digital, perbankan, serta sistem verifikasi identitas seperti *facial recognition*. Dalam konteks hukum, AI menimbulkan persoalan baru karena teknologi tersebut dapat digunakan sebagai alat bantu yang sah, tetapi juga dapat disalahgunakan sebagai sarana kejahatan. Oleh sebab itu, pengaturan AI dalam sistem hukum Indonesia menjadi penting untuk memberikan kepastian hukum, perlindungan data, serta batas pertanggungjawaban pidana terhadap pihak yang menyalahgunakannya.

Dalam sistem hukum Indonesia, hingga saat ini belum terdapat satu undang-undang khusus yang secara komprehensif mengatur mengenai kecerdasan buatan atau *Artificial Intelligence*. Namun, pengaturan mengenai AI dapat ditemukan secara tersebar dalam berbagai peraturan perundang-undangan yang berkaitan dengan informasi elektronik, transaksi elektronik, perlindungan data pribadi, sistem elektronik, keamanan siber, perbankan digital, dan hukum pidana. Hal ini menunjukkan bahwa pengaturan AI di Indonesia masih bersifat sektoral dan belum sepenuhnya membentuk rezim hukum yang mandiri. Meskipun demikian, ketentuan-ketentuan tersebut tetap dapat digunakan untuk menilai tanggung jawab hukum atas penyalahgunaan teknologi AI, terutama apabila teknologi tersebut digunakan untuk mengakses sistem elektronik secara ilegal, mencuri data pribadi, memanipulasi identitas, atau melakukan kejahatan terhadap sistem elektronik.[13]

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi salah satu instrumen hukum utama yang dapat digunakan untuk mengatur penyalahgunaan teknologi berbasis AI. UU ITE tidak secara eksplisit menggunakan istilah AI sebagai objek pengaturan utama, tetapi ketentuan mengenai sistem elektronik, informasi elektronik, dokumen elektronik, akses ilegal, intersepsi ilegal, manipulasi data elektronik, serta penyalahgunaan sistem elektronik dapat diterapkan terhadap perbuatan yang menggunakan

[13] Edmon Makarim, *Kompilasi Hukum Telematika*, Jakarta: RajaGrafindo Persada, 2003, hlm. 31–34

teknologi AI sebagai sarana kejahatan. Dalam konteks kejahatan AI, yang menjadi fokus bukan semata-mata teknologinya, melainkan perbuatan manusia yang secara sadar menggunakan atau memanipulasi sistem elektronik untuk memperoleh keuntungan secara melawan hukum. Dengan demikian, UU ITE tetap memiliki relevansi sebagai dasar hukum dalam menjerat pelaku kejahatan berbasis AI, terutama apabila AI digunakan sebagai alat untuk menembus, mengelabui, atau memanipulasi sistem elektronik milik pihak lain.

Selain UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga memiliki kedudukan penting dalam pengaturan AI di Indonesia. AI pada umumnya bekerja dengan menggunakan data dalam jumlah besar, termasuk data pribadi dan data biometrik seperti wajah, sidik jari, suara, atau karakteristik tubuh lainnya. Dalam konteks tersebut, penggunaan AI harus memperhatikan prinsip perlindungan data pribadi, termasuk keabsahan pemrosesan data, persetujuan subjek data, pembatasan tujuan, keamanan data, dan pertanggungjawaban pengendali data.

Penyalahgunaan data wajah dalam sistem facial recognition dapat dikualifikasikan sebagai pelanggaran terhadap perlindungan data pribadi apabila dilakukan tanpa dasar hukum yang sah. Oleh karena itu, UU Perlindungan Data Pribadi menjadi instrumen penting dalam mencegah dan menindak penyalahgunaan AI yang berbasis pada pemrosesan data pribadi secara ilegal.

Perkembangan kecerdasan buatan di Indonesia juga harus dipahami dalam kerangka kebijakan nasional mengenai transformasi digital. Pemerintah pada dasarnya telah menunjukkan komitmen untuk mendorong pemanfaatan AI sebagai bagian dari pembangunan ekonomi digital, peningkatan kualitas pelayanan publik, pengembangan industri, pendidikan, kesehatan, hingga keamanan nasional. Namun demikian, perkembangan tersebut harus diimbangi dengan regulasi yang mampu memberikan kepastian hukum terhadap risiko-risiko yang ditimbulkan oleh penggunaan AI. Risiko tersebut meliputi penyalahgunaan data pribadi, manipulasi identitas digital, penyebaran informasi palsu (*deepfake*), serangan siber berbasis AI, hingga penggunaan AI sebagai instrumen tindak pidana ekonomi dan perbankan. Oleh karena itu, arah kebijakan hukum Indonesia tidak hanya berorientasi pada pengembangan inovasi teknologi, tetapi juga pada perlindungan hak konstitusional masyarakat sebagaimana dijamin dalam Pasal 28G ayat (1) dan Pasal 28D ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Keberadaan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana juga memberikan landasan baru bagi pengaturan kejahatan yang berkaitan dengan perkembangan teknologi. Meskipun KUHP Nasional belum mengatur secara khusus mengenai *Artificial Intelligence Crime*, pembaruan hukum pidana nasional telah mengakomodasi perkembangan masyarakat melalui pengakuan terhadap hukum yang hidup (*living law*), perlindungan kepentingan hukum masyarakat, serta pendekatan yang lebih adaptif terhadap bentuk-bentuk kejahatan modern. Dalam konteks ini, tindak pidana yang dilakukan dengan memanfaatkan AI tetap dapat dijerat melalui ketentuan umum mengenai kesengajaan, penyertaan, percobaan, maupun tindak pidana khusus yang diatur dalam peraturan perundang-undangan di luar KUHP. Hal tersebut menunjukkan bahwa sistem hukum Indonesia telah memiliki fondasi normatif yang cukup untuk menindak pelaku kejahatan berbasis AI, meskipun pengaturan khusus mengenai AI masih memerlukan penyempurnaan.

Selain peraturan perundang-undangan, pemerintah juga telah menerbitkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial sebagai pedoman awal dalam penggunaan AI di Indonesia. Surat edaran tersebut memuat prinsip-prinsip etika yang harus diperhatikan oleh penyelenggara, pengembang, dan pengguna AI, antara lain prinsip inklusivitas, kemanusiaan, keamanan, transparansi, akuntabilitas, perlindungan data pribadi, serta mitigasi risiko. Walaupun secara hierarki peraturan perundang-undangan surat edaran bukan merupakan norma pidana yang mengikat layaknya undang-undang, keberadaannya mempunyai arti penting sebagai kebijakan administratif (*soft law*) yang memberikan arah bagi pengembangan AI yang bertanggung jawab. Dalam praktik internasional, pendekatan *soft law* semacam ini juga banyak digunakan sebagai tahap awal sebelum dibentuk regulasi yang lebih komprehensif mengenai AI.[14]

Perkembangan regulasi kecerdasan buatan di tingkat internasional menunjukkan bahwa AI tidak lagi dipandang semata-mata sebagai inovasi teknologi, melainkan juga sebagai objek pengaturan hukum yang memerlukan keseimbangan antara kepentingan inovasi dan perlindungan hak asasi manusia. Negara-negara maju serta organisasi internasional mulai

[14] Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial;

UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, Paris: UNESCO, 2021, hlm. 9–15.

membentuk prinsip-prinsip hukum yang mengatur pengembangan dan penggunaan AI secara bertanggung jawab. Pendekatan tersebut didasarkan pada kesadaran bahwa AI mampu menghasilkan manfaat yang sangat besar, namun sekaligus berpotensi menimbulkan risiko terhadap privasi, keamanan data, diskriminasi algoritmik, penyalahgunaan identitas digital, hingga ancaman terhadap demokrasi dan supremasi hukum. Oleh karena itu, regulasi AI pada tingkat global lebih menekankan pendekatan berbasis risiko (risk-based approach), transparansi, akuntabilitas, dan penghormatan terhadap hak asasi manusia. Pendekatan tersebut menjadi rujukan penting bagi negara-negara yang sedang membangun sistem hukum AI, termasuk Indonesia.

Salah satu pedoman internasional yang memiliki pengaruh besar adalah OECD Principles on Artificial Intelligence yang diterbitkan oleh OECD pada tahun 2019. Prinsip-prinsip tersebut menegaskan bahwa AI harus dikembangkan untuk memberikan manfaat bagi manusia dan planet, menghormati supremasi hukum (rule of law), hak asasi manusia, nilai-nilai demokrasi, serta menjamin adanya transparansi dan akuntabilitas dalam setiap proses pengambilan keputusan otomatis. OECD juga menekankan pentingnya pengawasan manusia (human oversight) terhadap sistem AI agar keputusan yang dihasilkan tetap dapat dipertanggungjawabkan secara hukum. Prinsip ini memiliki arti penting karena AI tidak boleh menggantikan tanggung jawab manusia sebagai subjek hukum, khususnya dalam konteks pertanggungjawaban pidana. Dengan demikian, meskipun suatu sistem AI bekerja secara otomatis, tanggung jawab hukum tetap berada pada pihak yang merancang, mengendalikan, atau menggunakan sistem tersebut secara melawan hukum.

Selain OECD, UNESCO melalui Recommendation on the Ethics of Artificial Intelligence Tahun 2021 memberikan pedoman etik yang lebih komprehensif mengenai tata kelola AI. Rekomendasi tersebut menempatkan martabat manusia sebagai pusat pengembangan AI serta menekankan perlindungan terhadap hak privasi, kebebasan berekspresi, kesetaraan, non-diskriminasi, keamanan digital, dan keberlanjutan. UNESCO juga mendorong setiap negara untuk membangun regulasi nasional yang mampu mengantisipasi risiko penyalahgunaan AI tanpa menghambat perkembangan inovasi teknologi. Bagi Indonesia, rekomendasi tersebut memiliki relevansi yang kuat karena sejalan dengan nilai-nilai Pancasila, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, serta prinsip negara hukum yang menghendaki adanya

perlindungan terhadap hak-hak warga negara dalam pemanfaatan teknologi digital. Oleh sebab itu, penyusunan regulasi AI di Indonesia seyogianya tidak hanya berorientasi pada kepentingan ekonomi digital, tetapi juga pada perlindungan hak asasi manusia dan keadilan sosial.

Perkembangan yang paling signifikan saat ini terlihat melalui lahirnya EU AI Act yang disusun oleh Uni Eropa sebagai regulasi komprehensif pertama di dunia mengenai kecerdasan buatan. Regulasi tersebut mengklasifikasikan penggunaan AI berdasarkan tingkat risiko, yaitu unacceptable risk, high risk, limited risk, dan minimal risk. Setiap kategori memiliki konsekuensi hukum yang berbeda, terutama terhadap kewajiban penyedia dan pengguna AI. Sistem AI yang berpotensi mengancam keselamatan publik, melanggar hak asasi manusia, atau digunakan untuk manipulasi sosial dikenakan persyaratan yang sangat ketat bahkan dapat dilarang. Pendekatan berbasis risiko ini menjadi model regulasi yang banyak dijadikan acuan oleh berbagai negara karena mampu memberikan keseimbangan antara inovasi teknologi dan perlindungan kepentingan masyarakat.[15]

Apabila dibandingkan dengan perkembangan hukum internasional tersebut, pengaturan AI di Indonesia masih berada pada tahap awal dan belum memiliki undang-undang yang secara khusus mengatur kecerdasan buatan. Regulasi yang ada masih tersebar dalam berbagai ketentuan mengenai sistem elektronik, perlindungan data pribadi, keamanan informasi, dan tindak pidana siber. Kondisi ini menunjukkan perlunya harmonisasi regulasi agar mampu menjawab berbagai persoalan hukum yang muncul akibat perkembangan AI, termasuk mengenai status hukum sistem AI, standar keamanan algoritma, tanggung jawab pengembang (*developer*), penyelenggara sistem elektronik, pengguna AI, serta mekanisme pertanggungjawaban pidana apabila AI digunakan sebagai sarana melakukan tindak pidana. Dengan demikian, pembentukan regulasi AI nasional merupakan kebutuhan yang mendesak agar Indonesia memiliki kepastian hukum sekaligus mampu mengikuti perkembangan hukum teknologi pada tingkat global tanpa mengabaikan nilai-nilai konstitusional dan prinsip keadilan yang hidup dalam masyarakat.[16]

Sebagai contoh konkret perkembangan

[15] EU AI Act; European Parliament, *Artificial Intelligence Act*, Brussels, 2024, hlm. 15–42.

[16] Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung: Refika Aditama, 2015, hlm. 151–160.

kejahatan yang memanfaatkan teknologi kecerdasan buatan di Indonesia, dapat dikemukakan perkara Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel yang berkaitan dengan penyalahgunaan teknologi facial recognition dalam sistem perbankan digital. Perkara tersebut memperlihatkan bahwa kemajuan teknologi verifikasi biometrik yang semula dirancang untuk meningkatkan keamanan transaksi justru dapat dimanfaatkan oleh pelaku kejahatan melalui rekayasa teknologi dan pencurian data pribadi. Berdasarkan fakta yang terungkap di persidangan, terdakwa memperoleh data wajah korban melalui media elektronik, kemudian menggunakan perangkat lunak yang dimodifikasi sehingga mampu melewati mekanisme verifikasi identitas pada aplikasi mobile banking. Akibat tindakan tersebut, pelaku berhasil mengakses rekening korban tanpa hak dan melakukan pemindahan dana ke rekening lain sehingga menimbulkan kerugian finansial yang cukup besar. Perkara ini menunjukkan bahwa perkembangan AI tidak hanya menghadirkan manfaat bagi masyarakat, tetapi juga membuka ruang lahirnya bentuk-bentuk kejahatan baru yang membutuhkan respons hukum yang adaptif.

Dalam proses pembuktian, Jaksa Penuntut Umum mendakwa terdakwa menggunakan ketentuan mengenai akses ilegal terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 ayat (1) dan ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, disertai ketentuan pidana dalam Undang-Undang Perbankan yang berkaitan dengan perlindungan sistem dan data nasabah. Unsur yang ditekankan oleh penuntut umum bukanlah keberadaan teknologi AI itu sendiri, melainkan tindakan melawan hukum berupa akses tanpa hak terhadap sistem elektronik dengan menggunakan sarana teknologi digital. Pendekatan tersebut memperlihatkan bahwa hukum pidana Indonesia masih memandang AI sebagai alat (instrument of crime) yang digunakan oleh manusia untuk melakukan tindak pidana. Dengan demikian, unsur kesalahan tetap dilekatkan kepada pelaku yang secara sadar mengendalikan penggunaan teknologi tersebut untuk memperoleh keuntungan secara melawan hukum. Pendekatan ini sekaligus menegaskan bahwa AI belum diposisikan sebagai subjek hukum yang dapat dimintai pertanggungjawaban pidana.

Dalam pertimbangannya, Majelis Hakim menilai bahwa seluruh unsur tindak pidana akses ilegal terhadap sistem elektronik telah terpenuhi

karena terdakwa secara sengaja memperoleh dan menggunakan data biometrik korban tanpa hak untuk melewati sistem keamanan perbankan digital. Hakim juga mempertimbangkan bahwa penggunaan teknologi berbasis machine learning dalam sistem verifikasi identitas tidak menghilangkan unsur kesengajaan (mens rea) maupun hubungan kausal antara tindakan pelaku dan kerugian yang dialami korban. Justru sebaliknya, kemampuan pelaku memanfaatkan kelemahan teknologi menunjukkan adanya perencanaan serta pemanfaatan kecanggihan teknologi secara sadar untuk melakukan kejahatan. Pertimbangan tersebut memperlihatkan bahwa perkembangan teknologi tidak mengubah prinsip-prinsip dasar hukum pidana mengenai kesalahan, pertanggungjawaban, maupun pembuktian. Oleh karena itu, hakim tetap menjadikan kehendak jahat pelaku sebagai dasar utama dalam menjatuhkan pidana.

Apabila dianalisis dari perspektif pertanggungjawaban pidana, perkara tersebut menunjukkan bahwa perkembangan AI tidak menimbulkan kekosongan hukum (*rechtvacuum*). Selama masih terdapat manusia yang merancang, mengendalikan, memprogram, atau menggunakan sistem AI untuk melakukan perbuatan melawan hukum, maka pertanggungjawaban pidana tetap dibebankan kepada manusia tersebut berdasarkan asas kesalahan. Pendekatan demikian sejalan dengan doktrin hukum pidana klasik yang menyatakan bahwa pertanggungjawaban pidana mensyaratkan adanya kemampuan bertanggung jawab, kesalahan, dan hubungan antara perbuatan dengan akibat yang ditimbulkan. AI sebagai sistem teknologi tidak memiliki kehendak bebas (free will), kesadaran moral, maupun kapasitas hukum sebagaimana dimiliki manusia sehingga tidak dapat dipidana secara mandiri. Oleh sebab itu, setiap penyalahgunaan AI harus tetap dianalisis melalui konstruksi pertanggungjawaban pidana terhadap individu maupun korporasi yang mengendalikan penggunaan teknologi tersebut.[17]

Berdasarkan uraian tersebut, dapat dipahami bahwa pengaturan AI dalam sistem hukum Indonesia saat ini masih bertumpu pada pendekatan fungsional melalui berbagai peraturan mengenai sistem elektronik, perlindungan data pribadi, hukum pidana, dan keamanan siber. Meskipun pendekatan tersebut masih mampu menjangkau berbagai bentuk penyalahgunaan AI sebagaimana terlihat dalam Putusan Pengadilan Negeri Jakarta Selatan Nomor

[17] Simester, A.P., Spencer, J.R., Sullivan, G.R., dan Virgo, G., *Simester and Sullivan's Criminal Law: Theory and Doctrine*, 7th ed., Oxford: Hart Publishing, 2019, hlm. 115–123.

892/Pid.Sus/2022/PN Jkt.Sel, perkembangan teknologi yang sangat cepat menuntut pembentukan regulasi yang lebih komprehensif mengenai Artificial Intelligence. Regulasi tersebut idealnya mengatur klasifikasi sistem AI, standar keamanan algoritma, kewajiban pengembang, tanggung jawab penyelenggara sistem elektronik, perlindungan hak-hak pengguna, mekanisme audit AI, hingga bentuk pertanggungjawaban hukum apabila AI digunakan sebagai sarana melakukan tindak pidana. Dengan adanya pengaturan yang lebih komprehensif, kepastian hukum, perlindungan masyarakat, dan pengembangan inovasi teknologi dapat berjalan secara seimbang sesuai dengan prinsip negara hukum serta tujuan pembangunan hukum nasional.[18]

B. Pertanggungjawaban Pidana Terhadap Tindak Kejahatan Dalam Sistem Kecerdasan Buatan (AI)

Pertanggungjawaban pidana terhadap tindak kejahatan dalam sistem kecerdasan buatan atau *Artificial Intelligence* pada dasarnya harus diletakkan dalam kerangka asas-asas umum hukum pidana. Dalam sistem hukum pidana Indonesia, seseorang hanya dapat dipidana apabila perbuatannya memenuhi unsur tindak pidana, dilakukan dengan kesalahan, serta tidak terdapat alasan pembenar maupun alasan pemaaf. AI sebagai teknologi digital tidak dapat dipersamakan dengan manusia sebagai subjek hukum pidana karena tidak memiliki kesadaran, kehendak bebas, niat jahat, maupun kemampuan bertanggung jawab. Oleh karena itu, dalam perkara kejahatan berbasis AI, titik utama pertanggungjawaban pidana tetap diarahkan kepada manusia atau korporasi yang merancang, mengendalikan, menggunakan, atau menyalahgunakan teknologi tersebut. Dengan demikian, AI lebih tepat ditempatkan sebagai sarana atau alat kejahatan, bukan sebagai pelaku pidana yang dapat dijatuhi hukuman.[19]

Asas legalitas menjadi dasar pertama dalam menentukan dapat atau tidaknya seseorang dimintai pertanggungjawaban pidana atas kejahatan berbasis AI. Asas ini menegaskan bahwa tidak ada suatu perbuatan yang dapat dipidana kecuali berdasarkan ketentuan peraturan perundang-undangan yang telah ada sebelum perbuatan dilakukan. Dalam konteks AI *Crime*, ketiadaan undang-undang khusus mengenai kecerdasan buatan tidak selalu berarti terjadi

[18] Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung: Refika Aditama, 2015, hlm. 165–171.
[19] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2015, hlm. 153–156.

kekosongan hukum, karena perbuatan yang dilakukan dengan menggunakan AI tetap dapat dijerat apabila memenuhi unsur tindak pidana yang telah diatur dalam UU ITE, KUHP, UU Perlindungan Data Pribadi, UU Perbankan, maupun peraturan sektoral lainnya. Oleh karena itu, yang menjadi dasar pemidanaan bukanlah istilah "AI" sebagai teknologi, melainkan perbuatan konkret pelaku yang menggunakan teknologi tersebut untuk melakukan akses ilegal, pencurian data, penipuan digital, manipulasi sistem elektronik, atau pemindahan dana tanpa hak.

Dalam doktrin hukum pidana, pertanggungjawaban pidana mensyaratkan adanya kesalahan (*schuld*) pada diri pelaku. Kesalahan tersebut dapat berbentuk kesengajaan (*dolus*) maupun kealpaan (*culpa*), tergantung pada hubungan batin antara pelaku dan perbuatan yang dilakukan. Pada kejahatan berbasis AI, pembuktian kesalahan menjadi penting karena teknologi sering kali bekerja secara otomatis dan kompleks. Namun, otomatisasi sistem tidak serta-merta menghilangkan kesalahan manusia apabila dapat dibuktikan bahwa pelaku secara sadar memanfaatkan, mengarahkan, atau memanipulasi sistem AI untuk mencapai tujuan melawan hukum. Dengan demikian, unsur mens rea tetap dapat ditemukan pada orang yang mengendalikan teknologi tersebut, meskipun proses teknis kejahatan dilakukan melalui sistem otomatis.[20]

Selain unsur kesalahan, pertanggungjawaban pidana juga memerlukan adanya perbuatan lahiriah atau *actus reus*. Dalam kejahatan AI, *actus reus* dapat berupa tindakan memasukkan data palsu, mencuri data biometrik, memanipulasi algoritma, mengakses sistem elektronik tanpa izin, membuat perangkat lunak tiruan, atau menggunakan sistem otomatis untuk menembus perlindungan keamanan digital. Perbuatan-perbuatan tersebut dapat dikualifikasikan sebagai tindakan melawan hukum apabila dilakukan tanpa hak dan menimbulkan kerugian bagi pihak lain. Oleh karena itu, AI tidak mengaburkan konsep actus reus, melainkan hanya mengubah bentuk teknis dari perbuatan pidana yang dilakukan. Dengan kata lain, tindakan kriminal tetap dapat diidentifikasi melalui jejak digital, alat bukti elektronik, dan akibat hukum yang ditimbulkan.[21]

Pertanggungjawaban pidana atas kejahatan AI juga harus memperhatikan hubungan kausal antara perbuatan pelaku dan akibat yang ditimbulkan. Dalam perkara yang melibatkan

[20] Andi Hamzah, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2018, hlm. 126–132.

[21] Jonathan Clough, *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2015, hlm. 45–52.

sistem otomatis, pembuktian kausalitas menjadi lebih kompleks karena terdapat keterlibatan perangkat lunak, data, algoritma, jaringan elektronik, dan sistem keamanan digital. Namun, kompleksitas teknologi tersebut tidak menghapus kemungkinan penegakan hukum sepanjang penyidik, penuntut umum, dan hakim dapat membuktikan bahwa tindakan pelaku menjadi sebab yang relevan terhadap terjadinya akses ilegal, kerugian korban, atau gangguan terhadap sistem elektronik. Di sinilah pentingnya digital forensik sebagai sarana pembuktian dalam perkara AI *Crime*. Dengan demikian, pertanggungjawaban pidana dalam kejahatan AI tetap dapat dibangun melalui analisis unsur perbuatan, kesalahan, akibat, dan hubungan kausal secara sistematis.[22]

Selain individu, perkembangan teknologi kecerdasan buatan juga membuka kemungkinan adanya pertanggungjawaban pidana korporasi apabila kejahatan dilakukan dalam ruang lingkup kegiatan perusahaan. Dalam praktik modern, banyak sistem AI dikembangkan, dioperasikan, maupun dipasarkan oleh badan hukum yang memiliki struktur organisasi, kebijakan internal, dan sistem pengawasan tertentu. Apabila korporasi dengan sengaja mengembangkan atau membiarkan penggunaan sistem AI yang diketahui digunakan untuk melakukan tindak pidana, maka korporasi tersebut dapat dimintai pertanggungjawaban pidana sesuai ketentuan peraturan perundang-undangan. KUHP Nasional telah mengakui korporasi sebagai subjek tindak pidana, sehingga pemidanaan tidak lagi terbatas kepada orang perseorangan semata. Oleh karena itu, dalam perkara AI Crime, pertanggungjawaban dapat dibebankan baik kepada pengurus, pemberi perintah, maupun korporasi sebagai entitas hukum apabila seluruh unsur pertanggungjawaban telah terpenuhi.

Kedudukan pengembang (*developer*) perangkat lunak AI juga perlu dianalisis secara hati-hati dalam menentukan adanya pertanggungjawaban pidana. Pada prinsipnya, seorang pengembang tidak dapat langsung dipidana hanya karena sistem yang dibuatnya kemudian disalahgunakan oleh pihak lain. Namun demikian, apabila dapat dibuktikan bahwa pengembang secara sengaja merancang algoritma untuk memfasilitasi tindak pidana, memasukkan fitur yang memang ditujukan untuk menghindari deteksi hukum, atau secara aktif bekerja sama dengan pelaku utama, maka pengembang tersebut dapat dimintai pertanggungjawaban pidana sebagai pelaku, penyuruh melakukan, turut serta

[22] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa, 2012, hlm. 270–276

melakukan, maupun pembantu tindak pidana. Dengan demikian, parameter utama yang harus dibuktikan bukanlah keberadaan teknologi AI itu sendiri, melainkan adanya kesengajaan, pengetahuan, dan kontribusi nyata terhadap terjadinya tindak pidana.[23]

Di samping pengembang, operator atau pengguna sistem AI juga mempunyai posisi yang sangat penting dalam menentukan pertanggungjawaban pidana. Dalam praktik penggunaan AI, operator merupakan pihak yang mengendalikan data masukan (*input*), menentukan tujuan penggunaan sistem, mengawasi proses operasional, serta memanfaatkan hasil yang dihasilkan AI. Oleh sebab itu, apabila operator mengetahui bahwa sistem AI digunakan untuk melakukan akses ilegal, manipulasi biometrik, pemalsuan identitas digital, atau pengambilalihan akun perbankan, tetapi tetap menjalankan sistem tersebut, maka operator dapat dimintai pertanggungjawaban pidana berdasarkan teori penyertaan maupun teori penguasaan terhadap perbuatan (*control over the act*). Pendekatan demikian menunjukkan bahwa hukum pidana tetap menempatkan manusia sebagai pengambil keputusan akhir (*ultimate decision maker*) meskipun teknologi AI menjalankan sebagian besar proses teknis secara otomatis.[24]

Pengaturan mengenai pertanggungjawaban pidana atas penyalahgunaan AI pada dasarnya telah memperoleh dasar normatif dalam berbagai peraturan perundang-undangan di Indonesia, meskipun belum terdapat undang-undang khusus mengenai Artificial Intelligence. Penyalahgunaan AI untuk memperoleh akses tanpa hak terhadap sistem elektronik dapat dijerat melalui ketentuan mengenai akses ilegal dalam Undang-Undang Informasi dan Transaksi Elektronik. Apabila penyalahgunaan tersebut melibatkan pengambilan data pribadi, maka pelaku juga dapat dimintai pertanggungjawaban berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam sektor jasa keuangan, penyalahgunaan AI yang mengakibatkan penguasaan rekening nasabah tanpa hak juga dapat dikualifikasikan sebagai tindak pidana di bidang perbankan berdasarkan Undang-Undang Nomor 7 Tahun 1992 sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Oleh karena itu, meskipun AI berkembang jauh lebih cepat daripada

[23] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana, 2014, hlm. 214–220.

[24] Jonathan Clough, *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2015, hlm. 71–79

regulasinya, sistem hukum Indonesia sesungguhnya telah memiliki berbagai instrumen hukum yang dapat digunakan untuk menjerat pelaku kejahatan berbasis kecerdasan buatan melalui pendekatan interpretasi sistematis dan perkembangan hukum pidana modern.

Sebagai salah satu contoh konkret penerapan pertanggungjawaban pidana terhadap kejahatan yang memanfaatkan sistem kecerdasan buatan, Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel memberikan gambaran mengenai bagaimana hukum pidana Indonesia tetap mampu menjangkau perkembangan teknologi digital. Perkara tersebut berawal dari tindakan terdakwa yang memperoleh data biometrik wajah milik korban melalui media elektronik, kemudian memanfaatkan perangkat lunak berbasis *facial recognition* untuk melewati sistem verifikasi keamanan pada layanan *mobile banking*. Melalui manipulasi tersebut, terdakwa berhasil memperoleh akses terhadap rekening korban dan melakukan transaksi keuangan tanpa persetujuan pemilik rekening. Perbuatan tersebut menunjukkan bahwa kecerdasan buatan dimanfaatkan sebagai alat untuk melakukan tindak pidana, sedangkan kehendak dan tujuan melawan hukum tetap berasal dari pelaku sebagai manusia. Oleh karena itu, pertanggungjawaban pidana tetap dibebankan kepada terdakwa karena AI hanya berfungsi sebagai instrumen dalam melaksanakan kejahatan.

Dalam proses pembuktian di persidangan, jaksa penuntut umum mendasarkan dakwaannya pada ketentuan mengenai akses ilegal terhadap sistem elektronik sebagaimana diatur dalam Pasal
30 ayat (1) dan ayat (2) Undang-Undang Informasi dan Transaksi Elektronik, disertai ketentuan pidana yang berkaitan dengan penyalahgunaan sistem perbankan. Unsur utama yang harus dibuktikan ialah adanya tindakan mengakses sistem elektronik tanpa hak serta adanya kesengajaan untuk memperoleh keuntungan secara melawan hukum. Berdasarkan alat bukti elektronik, keterangan saksi, hasil pemeriksaan digital forensik, dan pengakuan terdakwa, majelis hakim berpendapat bahwa seluruh unsur tindak pidana telah terpenuhi. Fakta bahwa sistem keamanan bank menggunakan teknologi AI tidak menghapus sifat melawan hukum dari tindakan terdakwa, karena sistem tersebut justru dimanipulasi secara sengaja agar dapat memberikan akses yang seharusnya tidak dimiliki oleh pelaku. Dengan demikian, perkembangan teknologi tidak mengubah substansi pertanggungjawaban pidana, melainkan hanya mengubah modus operandi kejahatan yang dilakukan.

Pertimbangan hakim dalam perkara tersebut memperlihatkan penerapan teori kesalahan (*schuld*) sebagai dasar pertanggungjawaban pidana. Hakim menilai bahwa terdakwa memiliki kemampuan bertanggung jawab, mengetahui akibat dari tindakannya, serta secara sadar menghendaki penggunaan perangkat lunak pengenal wajah untuk mengakses rekening korban. Unsur *mens rea* tercermin dari adanya perencanaan, pengumpulan data biometrik korban, penggunaan perangkat lunak tertentu, serta tujuan memperoleh keuntungan ekonomi secara melawan hukum. Di sisi lain, unsur *actus reus* diwujudkan melalui tindakan nyata berupa akses ilegal terhadap sistem elektronik, pengambilalihan akun, dan pemindahan dana dari rekening korban. Oleh sebab itu, baik unsur subjektif maupun unsur objektif tindak pidana telah terbukti secara kumulatif sehingga pertanggungjawaban pidana dapat dibebankan sepenuhnya kepada terdakwa.[25]

Apabila dianalisis dari perspektif hukum pidana modern, perkara tersebut menunjukkan bahwa AI belum dapat diposisikan sebagai subjek hukum pidana yang berdiri sendiri. Sistem kecerdasan buatan memang mampu melakukan proses pengenalan wajah secara otomatis melalui algoritma *machine learning*, namun seluruh proses tersebut tetap bergantung pada data, perintah, dan konfigurasi yang diberikan oleh manusia. AI tidak mempunyai kehendak bebas, kesadaran moral, maupun kemampuan memahami konsekuensi hukum dari tindakannya. Oleh karena itu, meskipun teknologi yang digunakan semakin canggih, pertanggungjawaban pidana tetap harus diarahkan kepada manusia yang mengendalikan teknologi tersebut. Pendekatan demikian sejalan dengan doktrin hukum pidana klasik maupun perkembangan hukum pidana kontemporer yang tetap menempatkan manusia sebagai subjek utama pemidanaan.[26]

Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel juga memiliki arti penting sebagai preseden dalam menghadapi perkembangan AI *Crime* di Indonesia. Putusan tersebut menunjukkan bahwa pengadilan tidak mengalami hambatan untuk menerapkan ketentuan pidana yang telah ada terhadap bentuk-bentuk kejahatan digital yang memanfaatkan teknologi kecerdasan buatan. Dengan menggunakan pendekatan interpretasi sistematis, hakim berhasil menghubungkan unsur-unsur tindak pidana konvensional dengan modus

[25] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2015, hlm. 155–163.

[26] H.L.A. Hart, *Punishment and Responsibility*, Oxford: Oxford University Press, 2008, hlm. 28–35.

operandi berbasis AI sehingga tercapai kepastian hukum tanpa harus menunggu lahirnya undang-undang khusus mengenai kecerdasan buatan. Dari sudut pandang kebijakan hukum pidana, pendekatan tersebut mencerminkan fleksibilitas sistem hukum Indonesia dalam menghadapi perkembangan teknologi informasi yang berlangsung sangat cepat. Namun demikian, putusan ini sekaligus menjadi indikator perlunya pembentukan regulasi khusus mengenai Artificial Intelligence agar pengaturan mengenai tanggung jawab pengembang, operator, penyedia platform, serta pengguna AI menjadi lebih jelas dan komprehensif pada masa yang akan datang.[27]

Ditinjau dari perspektif filsafat hukum, pertanggungjawaban pidana terhadap pelaku kejahatan yang menggunakan sistem kecerdasan buatan harus tetap berorientasi pada keseimbangan antara kepastian hukum, keadilan, dan kemanfaatan sebagaimana dikemukakan Gustav Radbruch. Kepastian hukum diperlukan agar setiap penyalahgunaan AI memiliki dasar pemidanaan yang jelas sehingga tidak menimbulkan kekosongan hukum. Di sisi lain, keadilan menuntut agar pemidanaan hanya dijatuhkan kepada pihak yang benar-benar memiliki kesalahan, bukan kepada teknologi yang secara hakikat tidak mempunyai kehendak maupun kesadaran. Sementara itu, kemanfaatan hukum menghendaki agar hukum pidana mampu mengikuti perkembangan teknologi digital tanpa menghambat inovasi yang bermanfaat bagi masyarakat. Oleh karena itu, penerapan pertanggungjawaban pidana dalam perkara AI harus dilakukan secara proporsional dengan tetap menjadikan manusia sebagai pusat pertanggungjawaban hukum.[28]

Apabila dianalisis berdasarkan teori pertanggungjawaban pidana modern, kecerdasan buatan pada saat ini belum memenuhi syarat sebagai subjek hukum pidana. AI tidak mempunyai kemampuan untuk memahami nilai moral, menentukan pilihan secara bebas, maupun mempertanggungjawabkan akibat dari tindakan yang dihasilkannya. Walaupun sistem AI mampu menghasilkan keputusan yang tampak otonom melalui proses *machine learning*, seluruh mekanisme tersebut tetap merupakan hasil rancangan algoritma, data pelatihan, parameter sistem, dan tujuan penggunaan yang ditentukan manusia. Oleh sebab itu, konsep *electronic personhood* yang pernah berkembang dalam

[27] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Jakarta: Kencana, 2014, hlm. 231–238.

[28] Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Citra Aditya Bakti, 2014, hlm. 212–218.

diskursus akademik belum dapat dijadikan dasar pemidanaan dalam sistem hukum Indonesia. Pertanggungjawaban pidana tetap harus diarahkan kepada individu, korporasi, atau pihak yang memiliki penguasaan efektif terhadap penggunaan sistem AI tersebut.[29]

Dari perspektif hukum komparatif, berbagai negara telah mulai membangun kerangka regulasi khusus mengenai kecerdasan buatan. Uni Eropa, misalnya, mengembangkan pendekatan berbasis risiko melalui *EU Artificial Intelligence Act*, yang mengklasifikasikan sistem AI berdasarkan tingkat risiko serta menetapkan kewajiban hukum bagi pengembang, penyedia, dan pengguna AI. Demikian pula *OECD AI Principles dan UNESCO Recommendation on the Ethics of Artificial Intelligence* menekankan pentingnya transparansi algoritma, akuntabilitas, pengawasan manusia (*human oversight*), perlindungan hak asasi manusia, serta tata kelola AI yang bertanggung jawab. Meskipun instrumen-instrumen tersebut belum mengatur pertanggungjawaban pidana secara langsung, prinsip-prinsip tersebut dapat menjadi referensi penting dalam pembentukan kebijakan hukum nasional mengenai *Artificial Intelligence*. Dengan demikian, Indonesia memiliki kesempatan untuk mengembangkan regulasi AI yang tidak hanya adaptif terhadap kemajuan teknologi, tetapi juga selaras dengan standar internasional mengenai keamanan, etika, dan perlindungan hak masyarakat.

Apabila dikaitkan dengan Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel, terlihat bahwa majelis hakim telah menerapkan pendekatan yang sesuai dengan prinsip-prinsip hukum pidana modern. Hakim tidak menjadikan kecerdasan buatan sebagai pihak yang dipersalahkan, melainkan memfokuskan analisis pada tindakan, kesengajaan, dan tujuan terdakwa yang memanfaatkan sistem AI untuk memperoleh akses ilegal terhadap layanan perbankan digital. Pendekatan tersebut menunjukkan bahwa unsur *mens rea* tetap menjadi fondasi utama pertanggungjawaban pidana meskipun alat yang digunakan berupa teknologi berbasis AI. Di samping itu, putusan tersebut memberikan kepastian hukum bahwa pemanfaatan teknologi yang semakin kompleks tidak menghilangkan tanggung jawab manusia sebagai pelaku utama tindak pidana. Oleh karena itu, putusan tersebut dapat dipandang sebagai salah satu contoh penerapan hukum pidana yang responsif terhadap

[29] H. L. A. Hart, *Punishment and Responsibility*, Oxford: Oxford University Press, 2008, hlm. 28–39

perkembangan teknologi informasi tanpa mengabaikan asas legalitas dan asas kesalahan.

Ke depan, perkembangan *Artificial Intelligence* yang semakin otonom menuntut adanya pembaruan hukum pidana Indonesia secara lebih komprehensif. Pembentuk undang-undang perlu merumuskan pengaturan khusus mengenai definisi AI, klasifikasi sistem AI, tanggung jawab pengembang, penyedia layanan, operator, pengguna, mekanisme audit algoritma, standar keamanan siber, serta sistem pembuktian dalam perkara yang melibatkan kecerdasan buatan. Pengaturan tersebut juga perlu diintegrasikan dengan ketentuan mengenai perlindungan data pribadi, keamanan siber, transaksi elektronik, serta pertanggungjawaban korporasi agar tercipta kepastian hukum yang utuh. Dengan adanya regulasi yang lebih komprehensif, aparat penegak hukum akan memiliki pedoman yang lebih jelas dalam menangani berbagai bentuk AI *Crime* yang terus berkembang. Pada akhirnya, pembaruan hukum tersebut diharapkan mampu menjaga keseimbangan antara perlindungan masyarakat, kepastian hukum, kemajuan teknologi, dan daya saing Indonesia dalam era transformasi digital global.

PENUTUP

A. Kesimpulan

1. Berdasarkan hasil pembahasan, dapat disimpulkan bahwa hingga saat ini Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai kecerdasan buatan (*Artificial Intelligence*). Meskipun demikian, berbagai ketentuan hukum positif, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor
   27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta berbagai regulasi sektoral lainnya, telah memberikan dasar hukum yang dapat digunakan untuk mengatur penyalahgunaan teknologi AI sepanjang memenuhi unsur tindak pidana yang telah diatur dalam peraturan perundang-undangan. Oleh karena itu, pengaturan AI di Indonesia saat ini masih bersifat sektoral dan menggunakan pendekatan interpretasi terhadap ketentuan hukum yang telah ada, sehingga diperlukan pembentukan regulasi khusus yang mampu memberikan kepastian hukum, perlindungan hukum, serta pedoman

yang komprehensif mengenai pengembangan, penggunaan, pengawasan, dan pemanfaatan kecerdasan buatan di Indonesia.

2. Pertanggungjawaban pidana terhadap kejahatan yang memanfaatkan sistem kecerdasan buatan pada prinsipnya tetap dibebankan kepada manusia atau korporasi yang secara sengaja mengembangkan, mengendalikan, menggunakan, atau menyalahgunakan teknologi tersebut untuk melakukan tindak pidana. AI tidak dapat diposisikan sebagai subjek hukum pidana karena tidak memiliki kemampuan bertanggung jawab, kehendak bebas, maupun kesalahan (*mens rea*) sebagaimana disyaratkan dalam hukum pidana. Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel menunjukkan bahwa hakim tetap menerapkan asas legalitas dan asas kesalahan dengan membebankan pertanggungjawaban pidana kepada pelaku yang secara sadar memanfaatkan sistem pengenalan wajah berbasis AI untuk melakukan akses ilegal terhadap layanan perbankan digital. Dengan demikian, keberadaan AI tidak menghapus pertanggungjawaban pidana pelaku, melainkan hanya menjadi sarana yang digunakan untuk melakukan tindak pidana sehingga pelaku tetap wajib mempertanggungjawabkan seluruh akibat hukum dari perbuatannya sesuai dengan ketentuan hukum pidana yang berlaku.

B. Saran

1. Pemerintah bersama Dewan Perwakilan Rakyat Republik Indonesia perlu segera menyusun dan menetapkan regulasi khusus mengenai kecerdasan buatan (*Artificial Intelligence*) yang mengatur secara komprehensif mengenai definisi AI, klasifikasi tingkat risiko, tanggung jawab pengembang, penyedia layanan, operator, pengguna, mekanisme pengawasan, audit algoritma, perlindungan data pribadi, keamanan siber, serta sistem pertanggungjawaban pidana atas penyalahgunaan AI. Pembentukan regulasi tersebut juga perlu diselaraskan dengan Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta perkembangan standar internasional agar mampu memberikan kepastian hukum sekaligus mendukung inovasi teknologi yang bertanggung jawab.
2. Aparat penegak hukum, khususnya Kepolisian, Kejaksaan, dan Pengadilan, perlu meningkatkan kapasitas kelembagaan dan kompetensi sumber daya manusia di bidang teknologi informasi, digital forensik, kecerdasan buatan, serta pembuktian elektronik agar mampu menangani perkara AI *Crime* secara efektif dan profesional. Selain itu, hakim diharapkan terus mengembangkan penafsiran hukum yang adaptif terhadap perkembangan teknologi dengan tetap berpedoman pada asas legalitas, asas kesalahan, kepastian hukum, keadilan, dan kemanfaatan hukum, sehingga penegakan hukum terhadap tindak pidana berbasis AI dapat memberikan perlindungan hukum yang optimal bagi masyarakat tanpa menghambat perkembangan inovasi teknologi di Indonesia.

DAFTAR PUSTAKA

Buku

Andi Hamzah. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2018.

Andi Hamzah. *Pertanggungjawaban Pidana Korporasi*. Jakarta: Sinar Grafika, 2020.

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2017.

Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2014.

Bell, John, dan Marie-Claire Cordonier Segger (eds.). *Regulatory Law and Governance for the Anthropocene*. London: Routledge, 2020.

Blauth, T.F., dkk. *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*. 2022.

Black, Julia. *Risk and Regulation*. London: Journal of Law and Society, 2000.

Calo, Ryan. *Robots and the Lessons of Cyberlaw*. California Law Review, Vol.103, 2015.

Clough, Jonathan. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2015.

Coglianese, Cary, dan David Lehr. *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*. Georgetown: Georgetown Law Journal, 2017.

Dewi Rosadi, Sinta. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: Refika Aditama, 2015.

Dworkin, H.M.G.S. *Responsibility and Technology*. London: Duckworth, berbagai edisi.

Edmon Makarim. *Kompilasi Hukum Telematika*. Jakarta: RajaGrafindo Persada, 2003.

Edmon Makarim. *Pengantar Hukum Telematika*. Jakarta: RajaGrafindo Persada, 2005.

Erkan, F. *Artificial Intelligence and Liability for Damages*. 2025.

Floridi, Luciano, dan Josh Cowls. *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review, 2019.

Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.

Hart, H.L.A. *Punishment and Responsibility*. Oxford: Oxford University Press, 2008.

Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.

King, T.C. *Artificial Intelligence Crime: An Interdisciplinary Analysis of AI-enabled Offending*. European Commission, 2019.

Kusumaatmadja, Mochtar. *Hukum, Masyarakat dan Pembinaan Hukum Nasional*. Bandung: Binacipta, 1976.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 2006.

Mahfud MD. *Politik Hukum di Indonesia*. Jakarta: LP3ES, 2009.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2008.

Mertokusumo, Sudikno. *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Liberty, 2010.

Mertokusumo, Sudikno. *Metode Penelitian Hukum*. Yogyakarta: Liberty, 2010.

Mertokusumo, Sudikno. *Penemuan Hukum*. Yogyakarta: Liberty, 2012.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2015.

Muladi, dan Dwidja Priyatno. *Pertanggungjawaban Pidana Korporasi*. Jakarta: Kencana, 2012.

Noviantama, D. *Deepfake: A Review from The Victimology Perspective*. 2025.

OECD. *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019.

OECD. *Artificial Intelligence in Society: Opportunities and Challenges*. Paris: OECD Publishing, 2021.

OECD. *Regulatory Policy and Governance*. Paris: OECD Publishing, 2012.

OECD. *OECD Principles on Artificial Intelligence*. Paris: OECD Publishing, 2019.

OECD. *State of Implementation of the OECD AI Principles*. Paris: OECD Publishing, 2021.

OECD dan Eurostat. *Oslo Manual 2018*. Paris: OECD Publishing, 2018.

Oxford University Press. *Oxford English Dictionary*. Oxford: Oxford University Press, 2010.

Putri, N.P.M. *Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake*. Singaraja: JPSS Undiksha, 2024.

Rahardjo, Satjipto. *Hukum dan Masyarakat*. Bandung: Angkasa, 1980.

Rahardjo, Satjipto. *Hukum dan Masyarakat: Dinamika Pemikiran*. Jakarta: Rajawali Pers, 2004.

Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2000.

Rosadi, Sinta Dewi. *Cyber Law*. Bandung: Refika Aditama, 2015.

Roxin, Claus. *Causation in the Law*. Oxford: Oxford University Press, 2014.

Russell, Stuart J., dan Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th Edition. New Jersey: Pearson, 2021.

Simester, A.P., Spencer, J.R., Sullivan, G.R., dan Virgo, G. *Simester and Sullivan's Criminal Law: Theory and Doctrine*. Oxford: Hart Publishing, 2019.

Soekanto, Soerjono. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: RajaGrafindo Persada, 1983.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 1989.

Soekanto, Soerjono. *Pokok-Pokok Sosiologi Hukum*. Jakarta: Rajawali Pers, 2010.

Soemitro, Ronny Hanitijo. *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta: Ghalia Indonesia, 1990.

Soepomo, R. *Sistem Hukum di Indonesia Sebelum Perang Dunia II*. Jakarta: UI Press, 1980.

Solove, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

Subagyo, P. Joko. *Metode Penelitian dalam Teori dan Praktik*. Jakarta: Rineka Cipta, 2011.

UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021.

UNODC. *Artificial Intelligence and Crime: The Dual Role of AI in Criminal Activity and Crime Prevention*. Vienna: United Nations Office on Drugs and Crime, 2021.

Van Bemmelen, H.J. *Principles of Corporate Criminal Liability*. Leiden: Leiden University Press, 1987.

Voigt, Paul, dan Axel von dem Bussche. *The EU Artificial Intelligence Act*. Cham: Springer, 2024.

Von Liszt, Franz. *Einführung in die Strafrechtswissenschaft*. Berlin, 1924.

Jurnal

Black, Julia. "Risk and Regulation." *Journal of Law and Society*, Vol. 27, No. 2, 2000.

Calo, Ryan. "Robots and the Lessons of Cyberlaw." *California Law Review*, Vol. 103, 2015.

Coglianese, Cary, dan David Lehr. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." *Georgetown Law Journal*, Vol. 105, 2017.

Floridi, Luciano, dan Josh Cowls. "A Unified Framework of Five Principles for AI in Society." *Harvard Data Science Review*, Vol. 1, No. 1, 2019.

Mahanani, A., dan Sulistyanta. "Tinjauan Yuridis ...." *Recidive*, Vol. 11, No. 1, 2022.

Putri, N.P.M. "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake." *JPSS Undiksha*, 2024.

Santoso, A. "Pertanggungjawaban Pidana dalam Kejahatan Berbasis Artificial Intelligence." *Lex Crimen*, Vol. XII, No. 4, 2024.

Peraturan Perundang-Undangan

Undang - Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

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

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

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

Putusan Pengadilan

Putusan Pengadilan Negeri Jakarta Selatan Nomor 892/Pid.Sus/2022/PN Jkt.Sel.

Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn.

Dokumen Internasional

Council of Europe. Convention on Cybercrime (Budapest Convention). Budapest, 2001.

European Commission. Proposal for Artificial Intelligence Act. Brussels, 2021.

European Parliament. Artificial Intelligence Act. Brussels, 2024.

Europol. European Serious and Organised Crime Threat Assessment 2025. The Hague, 2025.

Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. Paris, 2019.

United Nations Educational, Scientific and Cultural Organization. Recommendation on the Ethics of Artificial Intelligence. Paris, 2021.

United Nations Office on Drugs and Crime. Artificial Intelligence and Crime: The Dual Role of AI in Criminal Activity and Crime Prevention. Vienna, 2021.

Internet / Publikasi Resmi

Mahkamah Agung Republik Indonesia. Marinews Mahkamah Agung: Kejahatan Siber Deepfake di Era Kecerdasan Buatan. 7 Mei 2025.

Kementerian Komunikasi dan Digital Republik Indonesia. Dokumen Resmi Undang-Undang Nomor 1 Tahun 2024.

Pemerintah Republik Indonesia. Strategi Nasional Kecerdasan Artifisial Indonesia 2020–2045.