



Challenges for Criminal Law in Addressing Artificial Intelligence Based Crime in Indonesia

Dima Sentosa¹, Muhamad Jhohan², Hafidza Zia³

^{1,2,3}Fakultas Hukum Universitas Bengkulu

dimanadira02@gmail.com¹, muhamadjj10@gmail.com², hzia@unib.ac.id³

ABSTRACT

The development of Artificial Intelligence (AI) has provided various benefits to society while also creating risks associated with the emergence of new forms of crime that exploit this technology. AI can be used as a means to commit fraud, identity theft, digital content manipulation through deepfakes, the dissemination of false information, personal data violations, and various other forms of cybercrime. These developments pose significant challenges to criminal law in Indonesia, particularly in determining criminal liability, establishing evidence, and enforcing the law against offenses committed through the use of AI. This study aims to analyze the regulation of criminal law in Indonesia in addressing AI-based crime and to identify the various challenges associated with its enforcement. This study employs normative legal research using a statutory approach and a conceptual approach. Legal materials were collected through a literature review and analyzed qualitatively. The findings indicate that Indonesia does not yet have specific and comprehensive regulations governing AI-based crime. Nevertheless, various provisions of the Indonesian Criminal Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law can be applied depending on the nature of the offense and its consequences. The main challenges in law enforcement include difficulties in determining the responsible parties, establishing the elements of criminal intent and liability, collecting and establishing digital evidence, conducting digital forensics, limited law enforcement capacity, the cross-border nature of AI-related crimes, and the gap between technological developments and legal frameworks. Therefore, adaptive legal reform, enhanced law enforcement capacity, strengthened digital forensic infrastructure, and national and international cooperation are needed to effectively address the development of AI-based crime.

Keywords: Artificial Intelligence; AI-Based Crime; Criminal Law; Law Enforcement; Criminal Liability

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan dalam berbagai bidang kehidupan. Salah satu teknologi yang berkembang pesat saat ini adalah Artificial Intelligence (AI) atau kecerdasan buatan. AI mampu membantu manusia dalam berbagai kegiatan, seperti mengolah informasi, mengenali pola, mengambil keputusan, dan menghasilkan berbagai bentuk konten. Teknologi ini memberikan banyak manfaat, tetapi di sisi lain juga dapat digunakan untuk melakukan tindak pidana.

Pemanfaatan AI yang semakin mudah diakses membuka peluang terjadinya berbagai bentuk kejahatan baru. Teknologi seperti generative AI dan deepfake dapat digunakan untuk membuat gambar, video, atau suara yang menyerupai aslinya. Teknologi tersebut berpotensi digunakan untuk penipuan, pemalsuan identitas, penyebaran informasi palsu, manipulasi konten, pelanggaran privasi, hingga berbagai bentuk kejahatan siber lainnya.

Perkembangan tersebut menjadi tantangan bagi hukum pidana di Indonesia. Peraturan hukum yang ada pada umumnya dibuat ketika perkembangan AI belum seperti saat ini. Akibatnya, muncul pertanyaan mengenai apakah hukum pidana yang berlaku telah mampu menjangkau berbagai tindak pidana yang dilakukan dengan memanfaatkan AI. Karakter kejahatan berbasis AI yang dapat dilakukan secara otomatis dan melibatkan teknologi lintas negara juga menimbulkan kesulitan dalam proses penegakan hukum.

Permasalahan penting lainnya adalah mengenai pertanggungjawaban pidana. Dalam penggunaan AI dapat terlibat berbagai pihak, seperti pembuat sistem, pengembang, penyedia platform, dan pengguna. Oleh karena itu, apabila AI digunakan dalam suatu tindak pidana, diperlukan kejelasan mengenai pihak yang dapat dimintai pertanggungjawaban. Selain itu, teknologi seperti deepfake juga dapat menimbulkan persoalan dalam pembuktian karena aparat penegak hukum harus memastikan apakah suatu gambar, video, atau rekaman suara merupakan bukti yang asli atau telah dimanipulasi.

Indonesia telah memiliki beberapa instrumen hukum, seperti KUHP dan Undang-Undang Informasi dan Transaksi Elektronik, yang dapat digunakan untuk menangani tindak pidana di ruang digital. Namun, perkembangan AI menimbulkan tantangan baru mengenai efektivitas penerapan hukum tersebut terhadap bentuk-bentuk kejahatan yang semakin berkembang. Oleh karena itu, diperlukan kajian mengenai kesiapan hukum pidana Indonesia dalam menghadapi kejahatan berbasis AI, khususnya terkait pengaturan tindak pidana, pertanggungjawaban pidana, pembuktian, dan penegakan hukum.

Berdasarkan uraian tersebut, perkembangan Artificial Intelligence telah menimbulkan tantangan baru bagi hukum pidana di Indonesia. Oleh karena itu, penting untuk mengkaji sejauh mana hukum pidana Indonesia mampu menghadapi perkembangan kejahatan berbasis AI serta berbagai langkah yang diperlukan agar hukum dapat memberikan perlindungan yang efektif kepada masyarakat.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau penelitian hukum doktrinal. Penelitian hukum normatif dilakukan dengan mengkaji peraturan perundang-undangan, asas-asas hukum, teori hukum, serta berbagai literatur yang berkaitan dengan hukum pidana dan perkembangan Artificial Intelligence (AI).

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menganalisis berbagai ketentuan hukum pidana di Indonesia yang berkaitan dengan tindak pidana berbasis teknologi dan kejahatan siber. Sementara itu, pendekatan konseptual digunakan untuk memahami konsep kejahatan berbasis AI, pertanggungjawaban pidana, serta tantangan penegakan hukum terhadap penyalahgunaan teknologi AI.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan hukum pidana, teknologi informasi, dan transaksi elektronik. Bahan hukum sekunder meliputi buku, jurnal ilmiah, hasil penelitian, dan pendapat para ahli yang berkaitan dengan objek penelitian. Selanjutnya, bahan hukum tersier digunakan sebagai bahan pendukung untuk memberikan penjelasan terhadap bahan hukum primer dan sekunder.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan cara menelaah dan mengkaji berbagai sumber hukum yang relevan. Bahan hukum yang telah dikumpulkan kemudian dianalisis secara kualitatif dan disajikan secara deskriptif-analitis untuk menjawab permasalahan mengenai pengaturan hukum pidana dan tantangan penegakan hukum terhadap kejahatan berbasis Artificial Intelligence di Indonesia.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pidana Di Indonesia Dalam Menghadapi Kejahatan Yang Dilakukan Dengan Memanfaatkan Artificial Intelligence (AI)?

Perkembangan Artificial Intelligence atau kecerdasan artifisial telah membawa perubahan besar terhadap cara manusia berkomunikasi, bekerja, bertransaksi, mengakses informasi, dan mengambil keputusan. AI pada dasarnya merupakan teknologi yang memungkinkan sistem komputer melakukan fungsi tertentu yang sebelumnya membutuhkan kecerdasan manusia, seperti mengenali pola, menganalisis data, membuat prediksi, menghasilkan tulisan maupun gambar, menerjemahkan bahasa, hingga meniru suara dan wajah seseorang. Di satu sisi, pemanfaatan AI memberikan manfaat besar bagi sektor pendidikan, kesehatan, keuangan, pemerintahan, industri, serta penegakan hukum. Namun, di sisi lain, kemampuan AI yang semakin maju juga dapat digunakan sebagai sarana untuk melakukan tindak pidana dengan cara yang lebih cepat, masif, sulit dideteksi, dan berpotensi melintasi batas negara.¹ Fenomena tersebut menunjukkan bahwa AI tidak selalu menjadi pelaku tindak pidana, tetapi dapat berfungsi sebagai alat, medium, atau sarana yang digunakan oleh manusia untuk melaksanakan kejahatan.²

Dalam praktiknya, kejahatan yang memanfaatkan AI dapat muncul dalam berbagai bentuk. Salah satu bentuk yang paling dikenal adalah deepfake, yaitu teknologi yang dapat menghasilkan atau memanipulasi gambar, video, dan suara seseorang secara realistis. Deepfake dapat dipakai untuk penipuan, pencemaran nama baik, pemerasan, penyebaran pornografi palsu, manipulasi informasi, serta pemalsuan identitas.³ Selain itu, AI juga dapat dipakai untuk membuat pesan penipuan secara otomatis, melakukan serangan siber, membuat akun palsu dalam jumlah besar, mencuri data pribadi, meniru suara anggota keluarga untuk meminta uang, atau menghasilkan dokumen digital palsu yang meyakinkan. Maraknya penyalahgunaan deepfake telah terlihat dalam kasus penipuan yang mencatut tokoh publik, termasuk perkara yang ditangani oleh Ditressiber Polda Jawa Timur terkait manipulasi video Gubernur Jawa Timur untuk tujuan penipuan. Modus tersebut memperlihatkan bahwa teknologi AI dapat memperbesar daya tipu pelaku karena korban sulit membedakan antara konten asli dan konten yang telah direkayasa.⁴

Secara normatif, Indonesia belum memiliki undang-undang yang secara khusus, menyeluruh, dan terintegrasi mengatur tindak pidana berbasis AI. Belum terdapat ketentuan yang secara tegas merumuskan definisi AI, klasifikasi sistem AI berdasarkan risiko, kewajiban khusus bagi pengembang dan penyedia AI, maupun bentuk pertanggungjawaban pidana yang secara spesifik dirancang untuk kerugian yang timbul dari keputusan sistem AI.⁵ Kondisi tersebut tidak serta-merta berarti bahwa kejahatan yang menggunakan AI tidak dapat dipidana. Hukum pidana Indonesia tetap dapat digunakan untuk menjerat pelaku berdasarkan perbuatan

¹ Supuan Sultan Al Alif, Anis Rindiani, dan Cik Marhayati, "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia," *Legal Standing: Jurnal Ilmu Hukum* 9, no. 5 (2025): 1169–1183.

² Siti Nurkholisah, Daud Rismana, Afrizal Eko Nugroho, Amrina Munjiyah, dan Qurota Ayunisa, "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia," *Jurnal USM Law Review* 8, no. 3 (2025): 2421–2445.

³ Tri Nurwahid, Sri Amlinawati Muin, dan Rizki Ramadhani, "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia," *LEGAL DIALOGICA* 1, no. 2 (2026).

⁴ Nabila Aprillia, Dian Ratu Ayu Uswatun Khasanah, dan Ronald Jolly Pongantung, "Implikasi Hukum tentang Penyalahgunaan Teknologi Deepfake terhadap Kejahatan Identitas Digital," *Dinamika Hukum* 26, no. 2 (2025): 148–157.

⁵ Siti Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia," *Jurnal USM Law Review* 8, no. 3 (2025).

konkret yang dilakukan, akibat yang ditimbulkan, serta alat atau media yang digunakan dalam pelaksanaan tindak pidana tersebut. Dengan kata lain, fokus hukum pidana tidak terutama terletak pada kecanggihan alatnya, melainkan pada perbuatan melawan hukum yang dilakukan oleh manusia atau korporasi melalui alat tersebut.⁶

Pengaturan hukum pidana terhadap penyalahgunaan AI di Indonesia saat ini tersebar dalam beberapa instrumen hukum. Instrumen tersebut meliputi Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan mengenai penyelenggaraan sistem elektronik dan pedoman etika AI. Struktur pengaturan seperti ini menunjukkan bahwa pendekatan Indonesia masih bersifat sektoral dan tersebar. Satu jenis perbuatan yang memanfaatkan AI dapat dijerat berdasarkan lebih dari satu undang-undang, sepanjang unsur delik dalam masing-masing ketentuan terpenuhi.⁷

Landasan pertama yang perlu dikaji adalah KUHP baru dalam Undang-Undang Nomor 1 Tahun 2023. KUHP baru merupakan hukum pidana umum yang menjadi dasar untuk menentukan apakah suatu perbuatan dapat disebut sebagai tindak pidana, siapa yang dapat dimintai pertanggungjawaban, serta jenis pidana atau tindakan yang dapat dijatuhkan. KUHP tersebut telah berlaku sejak 2 Januari 2026. Dalam konteks penyalahgunaan AI, KUHP penting karena tetap menempatkan manusia sebagai pusat pertanggungjawaban pidana. AI pada hakikatnya merupakan sistem, perangkat lunak, atau alat teknologi; AI tidak memiliki kesadaran moral, kehendak hukum, maupun kemampuan untuk memahami akibat pidana dari perbuatannya. Oleh sebab itu, AI tidak dapat diposisikan sebagai subjek hukum pidana yang berdiri sendiri sebagaimana manusia atau korporasi.⁸

Prinsip tersebut berkaitan erat dengan asas kesalahan dalam hukum pidana. Seseorang tidak dapat dipidana hanya karena terdapat akibat yang merugikan, melainkan harus dibuktikan adanya perbuatan pidana dan kesalahan pada diri pelaku. Kesalahan tersebut dapat berupa kesengajaan atau kealpaan. Dalam kejahatan AI, penegak hukum perlu membuktikan apakah pengguna AI memang mempunyai niat untuk melakukan penipuan, menyebarkan konten melanggar hukum, mengakses data tanpa hak, atau memalsukan identitas seseorang. Sebagai contoh, seseorang yang menggunakan aplikasi voice cloning untuk meniru suara orang lain dan meminta korban mentransfer uang dapat dipandang memiliki kesengajaan karena ia mengetahui fungsi teknologi tersebut, menggunakan teknologi itu untuk menciptakan kebohongan, dan mengarahkan korban agar menyerahkan harta benda. Dalam keadaan demikian, AI hanya merupakan alat yang dipakai untuk memperkuat modus penipuan.

KUHP dapat diterapkan dalam kasus AI melalui delik-delik umum, seperti penipuan, pemalsuan, pengancaman, pemerasan, pencemaran nama baik, penyebaran berita bohong yang menimbulkan akibat tertentu, ataupun tindak pidana terhadap kehormatan dan kesusilaan. Sebagai ilustrasi, penggunaan AI untuk membuat video palsu yang memperlihatkan seseorang melakukan tindakan memalukan dapat mengarah pada tindak pidana pencemaran nama baik, penghinaan, pemerasan, atau bahkan tindak pidana kesusilaan apabila konten tersebut bersifat pornografis. Apabila pelaku menggunakan video palsu itu untuk meminta uang dengan ancaman akan menyebarkannya, perbuatannya dapat memenuhi unsur pemerasan atau pengancaman. Apabila pelaku membuat identitas digital palsu dan menggunakannya untuk

⁶ Supuan Sultan Alif et al., "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia," *Legal Standing: Jurnal Ilmu Hukum* 9, no. 5 (2025).

⁷ Nabila Aprillia et al., "Implikasi Hukum tentang Penyalahgunaan Teknologi Deepfake terhadap Kejahatan Identitas Digital," *Dinamika Hukum* 26, no. 2 (2025).

⁸ Tri Nurwahid et al., "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia," *LEGAL DIALOGICA* 1, no. 2 (2026).

memperoleh pinjaman atau keuntungan ekonomi, perbuatannya juga dapat dianalisis berdasarkan ketentuan tentang penipuan dan pemalsuan.

KUHP baru juga penting karena mengakui korporasi sebagai subjek hukum pidana. Pengakuan terhadap pertanggungjawaban pidana korporasi relevan dalam perkembangan AI karena banyak sistem AI dikembangkan, disediakan, dioperasikan, dan dikendalikan oleh badan usaha. Sebuah perusahaan dapat menjalankan platform AI, menyediakan layanan pengolahan data, membuat sistem pengenalan wajah, atau membangun aplikasi otomatis yang dipakai jutaan pengguna. Dalam kondisi tertentu, tindak pidana tidak semata-mata terjadi akibat tindakan pengguna individu, melainkan dapat berkaitan dengan kegagalan perusahaan dalam membangun sistem keamanan, melakukan pengawasan, mencegah penyalahgunaan, atau melindungi data penggunanya.

Selain KUHP, instrumen utama dalam penanganan kejahatan AI adalah UU ITE. UU ITE memiliki kedudukan penting karena sebagian besar penyalahgunaan AI berlangsung melalui internet, aplikasi digital, media sosial, sistem elektronik, jaringan komputer, atau perangkat yang terhubung secara elektronik. UU ITE telah mengalami perubahan kedua melalui Undang-Undang Nomor 1 Tahun 2024. Dalam konteks kejahatan AI, UU ITE dapat digunakan untuk menjerat perbuatan yang secara langsung berkaitan dengan informasi elektronik, dokumen elektronik, akses terhadap sistem elektronik, manipulasi data, gangguan sistem, penyebaran informasi palsu, dan bentuk penyalahgunaan teknologi digital lainnya.⁹

Penggunaan AI untuk menciptakan dan menyebarkan informasi palsu merupakan salah satu contoh yang dapat dijangkau oleh UU ITE. Konten deepfake yang dibuat untuk menipu masyarakat, memanipulasi opini publik, atau menciptakan kerusuhan dapat dikualifikasikan berdasarkan ketentuan mengenai penyebaran informasi elektronik yang mengandung berita bohong atau informasi menyesatkan. UU ITE hasil perubahan kedua juga memuat ketentuan pidana atas penyebaran informasi elektronik yang diketahui memuat pemberitahuan bohong dan menimbulkan kerusuhan di masyarakat, dengan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1 miliar. Ketentuan tersebut penting ketika AI digunakan untuk menghasilkan video, audio, atau gambar palsu yang tampak autentik sehingga berpotensi memengaruhi keamanan, ketertiban, atau kepercayaan masyarakat.

UU ITE juga relevan terhadap tindakan akses ilegal dan gangguan sistem elektronik. AI dapat meningkatkan kemampuan pelaku dalam melakukan serangan siber, misalnya melalui otomatisasi pencarian kelemahan sistem, pembuatan phishing email yang lebih personal, pembuatan kode berbahaya, atau serangan yang dilakukan secara berulang oleh bot. Dalam keadaan tersebut, perbuatan pelaku dapat dijerat berdasarkan larangan mengakses komputer atau sistem elektronik milik orang lain tanpa hak, mengubah atau memindahkan informasi elektronik tanpa kewenangan, melakukan intersepsi atau penyadapan secara melawan hukum, serta mengganggu sistem elektronik. Oleh karena itu, UU ITE pada dasarnya cukup fleksibel untuk menjangkau serangan siber yang dilakukan menggunakan teknologi baru, termasuk AI, karena yang menjadi titik tekan adalah tindakan tanpa hak terhadap sistem atau data elektronik.

Dalam kaitannya dengan deepfake, UU ITE tidak selalu dapat digunakan secara tunggal. Hal ini disebabkan satu konten deepfake dapat menghasilkan berbagai bentuk kerugian dan memenuhi unsur beberapa tindak pidana sekaligus. Misalnya, video palsu yang digunakan untuk menjatuhkan reputasi korban dapat berkaitan dengan penghinaan atau pencemaran nama baik. Apabila video tersebut digunakan untuk meminta uang, unsur penipuan atau pemerasan dapat muncul. Jika konten palsu itu memuat wajah atau data biometrik korban tanpa izin, terdapat pula potensi pelanggaran terhadap UU PDP. Oleh karena itu, aparat penegak hukum perlu melakukan konstruksi hukum secara cermat agar pasal yang diterapkan sesuai dengan perbuatan inti, tujuan pelaku, akibat yang dialami korban, serta bukti digital yang tersedia.

⁹ Siti Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru...", *Jurnal USM Law Review* 8, no. 3 (2025).

Pendekatan ini diperlukan untuk menghindari penerapan pasal yang terlalu luas ataupun tidak tepat sasaran.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi perangkat hukum penting lainnya dalam menghadapi kejahatan berbasis AI. Hal ini karena data merupakan unsur mendasar dalam pengembangan dan pengoperasian sebagian besar sistem AI. Sistem AI memerlukan data untuk melakukan pelatihan, pengenalan pola, prediksi, atau pembuatan keluaran tertentu. Data yang diproses dapat berupa nama, nomor telepon, alamat, rekaman suara, foto wajah, lokasi, rekam jejak digital, informasi kesehatan, data keuangan, hingga data biometrik. Apabila data tersebut dikumpulkan, diakses, dipakai, atau disebarluaskan tanpa dasar hukum yang sah, maka hak privasi dan hak atas pelindungan data pribadi seseorang dapat terlanggar.¹⁰

UU PDP memberikan pengaturan mengenai hak subjek data, kewajiban pengendali dan prosesor data, pemrosesan data pribadi, transfer data, serta sanksi administratif dan pidana. Dalam konteks AI, UU PDP dapat diterapkan terhadap pihak yang secara melawan hukum memperoleh atau mengumpulkan data pribadi untuk kepentingan pelatihan AI, mengungkapkan data pribadi milik orang lain, atau menggunakan data tersebut tanpa hak. Ketentuan pidana dalam UU PDP mengancam pihak yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi milik orang lain untuk menguntungkan diri sendiri atau orang lain dan mengakibatkan kerugian bagi subjek data, dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp5 miliar. Selain itu, pengungkapan data pribadi tanpa hak dapat dipidana dengan pidana penjara paling lama empat tahun dan/atau denda paling banyak Rp4 miliar.

Ketentuan mengenai pemalsuan data pribadi juga sangat relevan untuk penyalahgunaan AI. Pasal 66 UU PDP melarang pembuatan data pribadi palsu atau pemalsuan data pribadi dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Pelanggaran terhadap ketentuan tersebut dapat dipidana paling lama enam tahun dan/atau denda paling banyak Rp6 miliar. Dalam praktik kejahatan AI, aturan ini dapat diterapkan misalnya ketika pelaku membuat identitas digital sintesis, memanipulasi foto atau data biometrik untuk membuka rekening, membuat akun pinjaman, melewati sistem verifikasi, atau memperoleh fasilitas keuangan atas nama orang lain. Dengan demikian, UU PDP tidak hanya berfungsi untuk melindungi kerahasiaan data, tetapi juga menyediakan basis pidana terhadap praktik pemalsuan identitas yang semakin mungkin dilakukan melalui AI generatif.

Di luar hukum pidana positif yang mengandung sanksi, pemerintah juga telah menerbitkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Surat edaran tersebut memuat nilai-nilai etika dalam pengembangan dan pemanfaatan AI, antara lain inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, pelindungan data pribadi, pembangunan berkelanjutan, serta penghormatan terhadap kekayaan intelektual. Pedoman tersebut penting sebagai respons awal pemerintah terhadap perkembangan AI dan sebagai rambu bagi penyelenggara sistem elektronik, pelaku usaha, pengembang, maupun pengguna teknologi AI agar memanfaatkan teknologi secara bertanggung jawab.

Akan tetapi, Surat Edaran Nomor 9 Tahun 2023 tidak dapat dipersamakan dengan undang-undang atau peraturan yang memiliki ancaman pidana langsung. Surat edaran tersebut lebih tepat dipahami sebagai bentuk *soft law*, yaitu pedoman kebijakan yang mendorong kepatuhan tetapi tidak secara mandiri menciptakan delik pidana. Bahkan, pemberitaan mengenai penerbitannya menegaskan bahwa aturan etika AI tersebut tidak memuat sanksi bagi pelanggarnya. Meskipun demikian, keberadaan pedoman etika tetap penting dalam

¹⁰ Nabila Aprillia et al., "Implikasi Hukum tentang Penyalahgunaan Teknologi Deepfake...", *Dinamika Hukum* 26, no. 2 (2025).

pembentukan standar kehati-hatian. Ketika terjadi perkara pidana, prinsip transparansi, keamanan, akuntabilitas, dan perlindungan data dapat dijadikan bahan pertimbangan untuk menilai apakah pengembang, penyedia layanan, atau pengguna AI telah bertindak secara patut dan bertanggung jawab atau justru mengabaikan risiko yang seharusnya dapat diperkirakan.

Secara keseluruhan, pengaturan hukum pidana Indonesia dalam menghadapi kejahatan yang memanfaatkan AI belum berbentuk rezim hukum AI yang terpadu. Indonesia masih mengandalkan KUHP sebagai hukum pidana umum, UU ITE sebagai dasar penindakan kejahatan dalam ruang digital, UU PDP sebagai instrumen perlindungan terhadap penyalahgunaan data dan identitas, serta pedoman etika AI sebagai arah kebijakan non-pidana. Pendekatan tersebut memungkinkan aparat untuk tetap melakukan penegakan hukum terhadap banyak bentuk kejahatan AI, khususnya ketika terdapat unsur penipuan, pemalsuan, akses tanpa hak, penyebaran informasi palsu, gangguan sistem, atau penyalahgunaan data pribadi. Namun, pengaturan tersebut juga menunjukkan adanya kebutuhan untuk membangun regulasi AI yang lebih jelas dan adaptif. Indonesia dapat mempertimbangkan pembentukan pengaturan yang memuat definisi AI, pembagian AI menurut tingkat risiko, kewajiban transparansi terhadap konten hasil AI, kewajiban human oversight, audit sistem untuk AI berisiko tinggi, standar keamanan data, serta mekanisme akuntabilitas yang jelas bagi pengembang, penyedia, dan pengguna. Sebagai perbandingan, Uni Eropa telah membangun kerangka yang lebih terpadu melalui EU AI Act dengan pendekatan berbasis tingkat risiko, kewajiban transparansi, dan pengawasan manusia terhadap sistem tertentu. Pengalaman tersebut dapat menjadi bahan pembelajaran bagi Indonesia, meskipun penerapannya tetap harus disesuaikan dengan sistem hukum nasional, kebutuhan masyarakat, perkembangan industri digital, dan perlindungan hak asasi manusia

Tantangan Hukum Pidana dalam Penegakan Hukum terhadap Kejahatan Berbasis Artificial Intelligence (AI) di Indonesia

Meskipun Indonesia telah memiliki sejumlah instrumen hukum yang dapat diterapkan terhadap kejahatan berbasis AI, penegakan hukum di lapangan menghadapi berbagai tantangan struktural, teknis, dan konseptual yang cukup kompleks. Tantangan paling mendasar adalah kesulitan dalam menentukan subjek hukum yang dapat dimintai pertanggungjawaban pidana, atau yang dikenal sebagai attribution problem. Karakteristik AI yang semakin otonom memungkinkan sistem untuk mengambil keputusan dan melakukan tindakan tanpa intervensi manusia secara langsung, sehingga menyulitkan penegak hukum untuk membuktikan siapa yang memiliki unsur kesengajaan (*mens rea*) atau kealpaan yang menjadi syarat mutlak pidana menurut KUHP.¹¹ Penelitian oleh Sulistio dan Salsabilla (2023) menunjukkan bahwa dalam banyak kasus, seperti penggunaan autonomous trading bot untuk manipulasi pasar atau chatbot yang menyebarkan konten ilegal, sulit untuk menentukan apakah yang bertanggung jawab adalah pengembang algoritma, pemilik data pelatihan, operator sistem, atau pengguna akhir.¹²

Kesulitan atribusi ini berkaitan langsung dengan asas kesalahan. Dalam hukum pidana, seseorang tidak cukup dipidana karena memiliki hubungan dengan alat yang dipakai untuk melakukan tindak pidana. Penyidik dan penuntut umum harus membuktikan adanya kehendak jahat, pengetahuan, atau setidaknya kelalaian yang dapat dipersalahkan. Jika seseorang menggunakan AI untuk membuat suara palsu dan menipu korban, unsur kesengajaan relatif lebih mudah ditelusuri dari riwayat penggunaan aplikasi, isi percakapan, aliran dana, atau instruksi yang diberikan kepada sistem. Akan tetapi, apabila AI menghasilkan keluaran yang berbahaya tanpa instruksi eksplisit dari pengguna, pembuktian menjadi lebih sulit. Penelitian

¹¹ Aldin, Jumanudin, dan Anugrah Ryandra Fahlevi, "Pertanggungjawaban Pidana Dalam Tindak Pidana Berbasis Artificial Intelligence," *RIGGS: Journal of Artificial Intelligence and Digital Business* 5, no. 1 (2026): 6033–6042.

¹² Riska Fitriya et al., "Melacak Jejak Pidana AI: Status Subjek Hukum dan Model Pertanggungjawaban di Indonesia," *As-Syar'it: Jurnal Bimbingan & Konseling Keluarga* 8, no. 1 (2026).

oleh Ravizki dan Yudhantaka (2022) menegaskan bahwa AI tidak dapat digolongkan menjadi subjek hukum karena dalam konsep suatu pertanggungjawaban menurut beberapa ahli ialah memiliki kesadaran dan dapat menghendaki perbuatannya, dan sebagaimana diketahui AI tidak memiliki kesadaran terhadap perbuatan yang dilakukannya.¹³ Kondisi ini menciptakan apa yang disebut dalam literatur sebagai “retribution gap” atau “responsibility gap”, yaitu situasi di mana kerugian yang ditimbulkan oleh AI sering kali tidak dapat dipertanggungjawabkan kepada subjek hukum mana pun secara memuaskan.¹⁴ Dalam konteks ini, beberapa model pertanggungjawaban mulai diusulkan, antara lain model pertanggungjawaban pengembang di mana pengembang algoritma dapat dimintai pertanggungjawaban jika terbukti lalai dalam merancang sistem yang aman atau tidak melakukan uji risiko yang memadai, model pertanggungjawaban operator di mana pihak yang mengoperasikan sistem AI dapat bertanggung jawab jika gagal melakukan pengawasan yang wajar terhadap keluaran sistem, serta model pertanggungjawaban berlapis di mana tanggung jawab dibagi di antara beberapa pihak dalam rantai nilai AI, mulai dari pengumpul data, pelatih model, pengembang, hingga pengguna akhir, sesuai dengan tingkat kontrol dan kontribusi masing-masing terhadap risiko. Namun, implementasi model-model ini dalam praktik masih menghadapi hambatan besar, terutama karena belum adanya regulasi yang secara eksplisit mengatur alokasi tanggung jawab tersebut.¹⁵

Tantangan berikutnya adalah ketiadaan definisi legal yang baku mengenai apa yang dimaksud dengan “AI” dalam peraturan perundang-undangan Indonesia, serta tidak adanya klasifikasi risiko yang jelas terhadap berbagai jenis sistem AI. Tanpa definisi yang tegas, sulit bagi penegak hukum untuk menentukan batasan penerapan hukum dan standar kepatuhan yang harus dipenuhi oleh pengembang atau pengguna AI. Hal ini diperparah oleh fakta bahwa Surat Edaran Komdigi No. 9 Tahun 2023 tentang Etika AI hanya bersifat pedoman etika tanpa sanksi hukum yang tegas, sehingga banyak pelanggaran etika AI berada di area abu-abu (grey zone) yang sulit dijerat secara pidana. Penelitian oleh tim dari Jurnal Rewang Rencang (2025) menunjukkan bahwa pengaturan saat ini masih bergantung pada pasal-pasal yang tidak dirancang secara eksplisit untuk menangani kejahatan digital berbasis AI, seperti pasal pencemaran nama baik atau pasal penyebaran konten asusila dalam UU ITE. Ketidadaan definisi juga menyulitkan penerapan asas *lex certa* (kepastian hukum), yang mensyaratkan bahwa suatu norma pidana harus dirumuskan secara jelas dan tegas agar masyarakat dapat memahami apa yang dilarang. Tanpa definisi teknis tentang apa itu AI, deepfake, atau sistem otonom, penafsiran terhadap pasal-pasal yang ada menjadi sangat luas dan rentan digugat. Sebagai ilustrasi, dalam kasus deepfake pornografi non-konsensual, penegak hukum harus memilih antara menggunakan UU ITE (pasal tentang konten asusila), UU TPKS (kekerasan seksual berbasis elektronik), atau KUHP (pasal tentang pencemaran nama baik atau pemerasan). Namun, tidak satu pun dari regulasi ini yang secara spesifik mendefinisikan deepfake sebagai bentuk manipulasi digital berbasis AI, sehingga pembuktian unsur delik menjadi sangat bergantung pada interpretasi hakim yang dapat bervariasi.¹⁶

Tantangan pembuktian digital dan forensik juga menjadi hambatan signifikan, mengingat kejahatan AI sering meninggalkan jejak digital yang terenkripsi, terdistribusi di berbagai server, atau bahkan dihapus secara otomatis oleh sistem. Membutuhkan keahlian forensik digital tingkat tinggi untuk melacak log algoritma, data pelatihan, dan proses pengambilan keputusan sistem AI, yang sering kali bersifat rahasia dagang (proprietary) dan

¹³ Eka Nanda Ravizki dan Lintang Yudhantaka, “Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia,” *Notaire* 5, no. 3 (2022): 351–376.

¹⁴ Budi Kristian dan Tubagus Ahmad Ramadan, “The Deterrence Dilemma: Assessing Criminal Liability Standards for Emerging Digital Offenses in the AI Era,” *Realism: Law Review* 3, no. 3 (Desember 2025).

¹⁵ Riska Fitriya et al., “Melacak Jejak Pidana AI...,” *As-Syar’i* 8, no. 1 (2026).

¹⁶ Siti Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia,” *Jurnal USM Law Review* 8, no. 3 (2025): 2421–2445.

tidak mudah diakses oleh penyidik. Banyak lembaga penegak hukum di Indonesia masih terbatas dalam hal kapasitas teknis, sumber daya manusia, dan infrastruktur untuk melakukan investigasi forensik digital yang kompleks semacam ini. Penelitian oleh tim dari Jurnal De Jure (2024) menegaskan bahwa penggunaan AI dalam sistem peradilan memerlukan pemahaman teknis yang mendalam tentang cara kerja algoritma, struktur sistem elektronik, dan karakter bukti digital. Beberapa hambatan spesifik dalam pembuktian kejahatan AI meliputi kompleksitas bukti algoritmik di mana bukti tidak lagi hanya berupa file statis seperti foto atau dokumen, melainkan berupa log sistem, parameter model, bobot neural network, dan data pelatihan yang dinamis dan sulit direkonstruksi, kemudian enkripsi dan distribusi data di mana data sering tersimpan di cloud lintas negara, dienkripsi end-to-end, atau dipecah menjadi shard yang tersebar di berbagai lokasi, sehingga menyulitkan proses pengumpulan bukti yang utuh, keterbatasan alat forensik di mana alat forensik konvensional sering kali tidak dirancang untuk menganalisis artefak AI seperti deepfake, voice clone, atau manipulated media, sehingga memerlukan pengembangan tool khusus yang mahal dan langka, serta kerahasiaan dagang di mana perusahaan pengembang AI sering menolak memberikan akses ke log algoritma atau data pelatihan dengan alasan perlindungan intellectual property, sehingga menghambat proses penyidikan. Kondisi ini menuntut investasi besar-besaran dalam pelatihan forensik digital bagi aparat penegak hukum, serta kerja sama dengan sektor swasta dan akademisi untuk mengembangkan metode dan alat forensik yang adaptif terhadap teknologi AI.¹⁷

Aspek yurisdiksi dan dimensi transnasional juga menjadi tantangan serius, karena sistem AI sering kali di-hosting di server luar negeri, dilatih menggunakan data dari berbagai negara, dan dioperasikan secara lintas batas tanpa mengenal teritori fisik. Hal ini menimbulkan pertanyaan kompleks mengenai hukum negara mana yang berlaku dan bagaimana mekanisme kerja sama internasional untuk penyidikan, penuntutan, dan eksekusi putusan. Meskipun UU PDP dan UU ITE mengatur tentang kerja sama internasional dalam penanganan tindak pidana terkait data dan sistem elektronik, implementasinya di lapangan masih terbatas dan sering kali terhambat oleh prosedur birokratis yang rumit. Penelitian oleh tim dari Jurnal Causa Justa (2025) menunjukkan bahwa sistem hukum pidana Indonesia yang masih berorientasi pada pelaku manusia dan korporasi belum secara memadai mengantisipasi aktivitas sistem digital yang mampu mengambil keputusan sendiri. Beberapa isu yurisdiksi yang muncul antara lain locus delicti yang ambigu di mana dalam kejahatan AI, tempat terjadinya tindak pidana bisa di mana saja, tempat server berada, tempat data dikumpulkan, tempat algoritma dilatih, atau tempat korban berada, sehingga menyulitkan penentuan yurisdiksi yang tepat, konflik hukum antar negara di mana suatu tindakan mungkin legal di satu negara tetapi ilegal di negara lain, sehingga menimbulkan konflik norma yang sulit diselesaikan tanpa harmonisasi regulasi internasional, serta keterbatasan ekstradisi dan mutual legal assistance (MLA) di mana proses MLA sering kali lambat dan rumit, sementara bukti digital dapat dengan mudah dipindahkan atau dihapus sebelum permintaan bantuan hukum saling diterima. Untuk mengatasi hal ini, diperlukan penguatan kerja sama bilateral dan multilateral dalam bidang cybercrime, termasuk ratifikasi konvensi internasional seperti Budapest Convention on Cybercrime (meskipun Indonesia belum meratifikasinya) dan pengembangan protokol MLA yang lebih cepat dan efisien untuk kasus-kasus berbasis AI.¹⁸

Terakhir, terdapat kesenjangan yang lebar antara kecepatan inovasi teknologi AI dan lambatnya proses pembentukan hukum di Indonesia. Teknologi AI berkembang secara eksponensial dan terus menghasilkan varian baru yang lebih canggih, sementara proses legislasi membutuhkan waktu yang panjang dan sering kali tertinggal dari perkembangan

¹⁷ Adrian Bima Putra, "The Legal Standing of Deepfake Digital Evidence in Criminal Proceedings: Challenges of Evidentiary Integrity in the AI Era," *Fox Just: Jurnal Ilmu Hukum* 16, no. 1 (2026).

¹⁸ Nabila Aprillia, Dian Ratu Ayu Uswatun Khasanah, dan Ronald Jolly Pongantung, "Implikasi Hukum tentang Penyalahgunaan Teknologi Deepfake terhadap Kejahatan Identitas Digital," *Dinamika Hukum* 26, no. 2 (2025).

teknologi. Akibatnya, regulasi yang ada berisiko menjadi tidak relevan atau mudah dicari celahnya (regulatory arbitrage) oleh pelaku kejahatan yang memanfaatkan kelemahan dalam interpretasi hukum. Kondisi ini menuntut adanya pendekatan regulasi yang lebih adaptif, seperti penggunaan regulasi berbasis prinsip (principle-based regulation) atau mekanisme sandbox regulasi, agar hukum dapat tetap efektif menghadapi dinamika kejahatan berbasis AI di masa depan. Penelitian oleh Putri, Hartono, dan Yudiawan (2024) menegaskan bahwa diperlukan rekonstruksi delik khusus deepfake dan perluasan corporate criminal liability melalui Pasal 45–47 KUHP 2023 untuk mengatasi keterbatasan pengaturan saat ini. Beberapa rekomendasi konkret yang dapat dipertimbangkan antara lain pembentukan *lex specialis* tentang AI yaitu regulasi khusus yang mendefinisikan AI, mengklasifikasikan risiko, dan mengatur tanggung jawab masing-masing pihak dalam rantai nilai AI, penerapan strict liability untuk sistem AI berisiko tinggi di mana untuk kasus-kasus di mana pembuktian *mens rea* sangat sulit, dapat diterapkan tanggung jawab mutlak bagi pengembang atau operator sistem AI yang menimbulkan kerugian, kewajiban transparansi dan auditabilitas di mana pengembang AI diwajibkan untuk menyimpan log sistem, dokumentasi algoritma, dan hasil uji risiko yang dapat diakses oleh aparat penegak hukum dalam rangka penyidikan, serta sandbox regulasi yaitu mekanisme uji coba regulasi dalam lingkungan terbatas yang memungkinkan regulator untuk belajar dari implementasi nyata sebelum memberlakukan aturan secara nasional.¹⁹

Selain tantangan teknis dan yurisdiksional, penegakan hukum terhadap kejahatan AI juga harus memperhatikan implikasi terhadap hak asasi manusia dan perlindungan korban. Penggunaan AI dalam kejahatan seperti deepfake pornografi non-konsensual, penipuan finansial, atau disinformasi politik dapat menimbulkan dampak psikologis, sosial, dan ekonomi yang sangat serius bagi korban. Namun, karena keterbatasan regulasi dan kapasitas penegakan hukum, banyak korban tidak mendapatkan keadilan yang memadai. Proses pembuktian yang rumit, biaya forensik digital yang tinggi, serta stigma sosial terhadap korban (terutama dalam kasus deepfake pornografi) sering kali membuat korban enggan melaporkan atau melanjutkan proses hukum. Oleh karena itu, strategi penanganan kejahatan AI harus mencakup pula mekanisme perlindungan korban yang lebih kuat, termasuk akses cepat ke layanan psikologis, hukum, dan teknis untuk menghapus konten ilegal, peningkatan literasi digital masyarakat agar dapat mengenali dan menghindari berbagai bentuk penipuan dan manipulasi berbasis AI, serta kewajiban proaktif platform digital untuk mendeteksi, membatasi penyebaran, dan menghapus konten deepfake atau manipulated media yang melanggar hukum.²⁰

Berdasarkan uraian tersebut, dapat dipahami bahwa tantangan penegakan hukum terhadap kejahatan berbasis AI bukan hanya terletak pada kekurangan aturan pidana. Persoalan yang lebih mendalam mencakup kesulitan menentukan pihak yang bertanggung jawab, pembuktian unsur kesalahan, keterbatasan keahlian forensik digital, karakter kejahatan lintas negara, ketimpangan antara perkembangan teknologi dan pembentukan hukum, serta kebutuhan untuk menjaga hak asasi manusia. Oleh sebab itu, penanganan kejahatan AI harus dilakukan melalui strategi yang terpadu. Strategi tersebut dapat meliputi pembaruan regulasi, penguatan kapasitas aparat, penyediaan fasilitas forensik digital, kerja sama internasional, kewajiban transparansi bagi penyedia AI, serta peningkatan literasi masyarakat agar mampu mengenali berbagai bentuk penipuan dan manipulasi digital. Dengan pendekatan yang komprehensif dan adaptif, sistem hukum pidana Indonesia dapat lebih siap menghadapi dinamika kejahatan berbasis AI di masa depan, sekaligus memastikan bahwa keadilan tetap dapat ditegakkan bagi para korban dan bahwa inovasi teknologi tidak terhambat oleh ketidakpastian hukum.

¹⁹ Tri Nurwahid, Sri Amlinawati Muin, dan Rizki Ramadhani, "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia," *LEGAL DIALOGICA* 1, no. 2 (2026).

²⁰ Supuan Sultan Al Alif, Anis Rindiani, dan Cik Marhayati, "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia," *Legal Standing: Jurnal Ilmu Hukum* 9, no. 5 (2025).

KESIMPULAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa pengaturan hukum pidana di Indonesia dalam menghadapi kejahatan yang dilakukan dengan memanfaatkan Artificial Intelligence (AI) pada dasarnya telah memiliki landasan hukum, meskipun belum terdapat peraturan khusus yang secara komprehensif mengatur kejahatan berbasis AI. Pengaturan yang ada masih tersebar dalam beberapa instrumen hukum, terutama Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Ketentuan tersebut dapat diterapkan terhadap berbagai bentuk penyalahgunaan AI berdasarkan perbuatan dan akibat yang ditimbulkan, seperti penipuan, pemalsuan, pencemaran nama baik, pemerasan, penyebaran informasi palsu, akses ilegal, gangguan sistem elektronik, dan penyalahgunaan data pribadi. Dalam hal ini, AI pada prinsipnya tidak dipandang sebagai subjek hukum pidana, melainkan sebagai alat atau sarana yang digunakan oleh manusia atau korporasi dalam melakukan tindak pidana. Namun, pendekatan pengaturan yang masih bersifat sektoral menunjukkan adanya kebutuhan untuk membangun pengaturan yang lebih jelas, terpadu, dan adaptif terhadap perkembangan teknologi AI.

Penegakan hukum terhadap kejahatan berbasis AI juga menghadapi berbagai tantangan. Tantangan tersebut meliputi kesulitan menentukan pihak yang dapat dimintai pertanggungjawaban pidana, terutama ketika dalam pengembangan dan penggunaan AI melibatkan banyak pihak. Selain itu, pembuktian unsur kesalahan dan hubungan antara tindakan manusia dengan keluaran yang dihasilkan oleh AI juga menjadi persoalan penting. Tantangan lainnya adalah keterbatasan pengaturan khusus mengenai AI, kesulitan pembuktian dan forensik digital, keterbatasan kemampuan aparat penegak hukum dalam memahami teknologi AI, serta karakter kejahatan yang dapat dilakukan secara lintas negara. Perkembangan teknologi AI yang berlangsung sangat cepat juga menimbulkan kesenjangan dengan proses pembentukan hukum yang cenderung membutuhkan waktu lebih lama.

Oleh karena itu, penanganan kejahatan berbasis AI di Indonesia tidak cukup hanya dengan mengandalkan ketentuan hukum pidana yang telah ada. Diperlukan pembaruan hukum yang lebih adaptif, disertai penguatan kapasitas aparat penegak hukum dan fasilitas forensik digital. Selain itu, perlu adanya kejelasan mengenai bentuk pertanggungjawaban para pihak yang terlibat dalam pengembangan dan penggunaan AI, peningkatan kerja sama internasional dalam penanganan kejahatan lintas negara, serta penguatan perlindungan terhadap korban. Dengan langkah tersebut, sistem hukum pidana Indonesia diharapkan mampu menghadapi perkembangan dan penyalahgunaan AI secara lebih efektif tanpa mengabaikan asas legalitas, asas kesalahan, kepastian hukum, serta perlindungan hak asasi manusia.

Saran

Berdasarkan hasil pembahasan dan kesimpulan penelitian, terdapat beberapa saran yang dapat diberikan. Pertama, pemerintah dan pembentuk undang-undang perlu melakukan pembaruan serta penguatan regulasi terkait pemanfaatan Artificial Intelligence (AI). Pengaturan tersebut perlu memberikan kejelasan mengenai definisi dan ruang lingkup AI, bentuk-bentuk penyalahgunaan AI yang berpotensi menimbulkan tindak pidana, serta batas dan bentuk pertanggungjawaban bagi pihak yang terlibat dalam pengembangan, penyediaan, dan penggunaan sistem AI. Pembentukan regulasi juga perlu dilakukan secara adaptif agar mampu mengikuti perkembangan teknologi tanpa menghambat inovasi dan pemanfaatan AI untuk kepentingan yang positif.

Kedua, aparat penegak hukum perlu meningkatkan kemampuan dan pemahaman dalam menghadapi perkembangan kejahatan berbasis AI. Peningkatan kapasitas tersebut dapat dilakukan melalui pendidikan dan pelatihan mengenai teknologi AI, kejahatan siber, pembuktian elektronik, dan forensik digital. Selain peningkatan sumber daya manusia,

diperlukan pula dukungan sarana dan prasarana yang memadai untuk mendeteksi, mengidentifikasi, dan menganalisis bukti digital yang telah dimanipulasi menggunakan teknologi AI, termasuk teknologi deepfake dan bentuk manipulasi digital lainnya.

Ketiga, pemerintah perlu memperkuat kerja sama antara aparat penegak hukum, lembaga pemerintah, akademisi, penyedia teknologi, dan masyarakat dalam menghadapi penyalahgunaan AI. Kerja sama internasional juga perlu ditingkatkan karena kejahatan berbasis AI memiliki karakter yang dapat melintasi batas negara. Melalui kerja sama tersebut, proses pertukaran informasi, pengumpulan bukti digital, pelacakan pelaku, dan penanganan kejahatan lintas negara dapat dilakukan secara lebih efektif.

Keempat, penyedia dan pengembang sistem AI perlu didorong untuk menerapkan prinsip transparansi, keamanan, dan akuntabilitas dalam pengembangan serta penggunaan teknologi AI. Penyedia sistem AI juga perlu memiliki mekanisme pengawasan dan pencegahan terhadap penyalahgunaan layanan, khususnya terhadap penggunaan AI untuk penipuan, pemalsuan identitas, penyebaran konten ilegal, dan manipulasi digital yang merugikan masyarakat.

Terakhir, peningkatan literasi digital masyarakat juga perlu menjadi bagian penting dalam upaya pencegahan kejahatan berbasis AI. Masyarakat perlu diberikan pemahaman mengenai risiko penggunaan teknologi AI serta kemampuan untuk mengenali berbagai bentuk manipulasi digital, penipuan berbasis suara atau video palsu, dan penyalahgunaan data pribadi. Dengan adanya pembaruan regulasi, peningkatan kapasitas aparat penegak hukum, kerja sama antarinstansi dan lintas negara, serta peningkatan kesadaran masyarakat, diharapkan Indonesia dapat membangun sistem hukum pidana yang lebih siap dan efektif dalam menghadapi perkembangan kejahatan berbasis Artificial Intelligence di masa mendatang.

DAFTAR PUSTAKA

- Aldin, Jumanudin, dan Anugrah Ryandra Fahlevi. "Pertanggungjawaban Pidana Dalam Tindak Pidana Berbasis *Artificial Intelligence*." *RIGGS: Journal of Artificial Intelligence and Digital Business* 5, no. 1 (2026): 6033–6042.
- Al Alif, Supuan Sultan, Anis Rindiani, dan Cik Marhayati. "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi *Deepfake* di Indonesia." *Legal Standing: Jurnal Ilmu Hukum* 9, no. 5 (2025): 1169–1183.
- Aprillia, Nabila, Dian Ratu Ayu Uswatun Khasanah, dan Ronald Jolly Pongantung. "Implikasi Hukum tentang Penyalahgunaan Teknologi *Deepfake* terhadap Kejahatan Identitas Digital." *Dinamika Hukum* 26, no. 2 (2025): 148–157.
- Fitriya, Riska, et al. "Melacak Jejak Pidana AI: Status Subjek Hukum dan Model Pertanggungjawaban di Indonesia." *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga* 8, no. 1 (2026).
- Kristian, Budi, dan Tubagus Ahmad Ramadan. "The Deterrence Dilemma: Assessing Criminal Liability Standards for Emerging Digital Offenses in the AI Era." *Realism: Law Review* 3, no. 3 (Desember 2025).
- Nurkholisah, Siti, Daud Rismana, Afrizal Eko Nugroho, Amrina Munjiyah, dan Qurota Ayunisa. "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia." *Jurnal USM Law Review* 8, no. 3 (2025): 2421–2445.
- Nurwahid, Tri, Sri Amlinawati Muin, dan Rizki Ramadhani. "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia." *LEGAL DIALOGICA* 1, no. 2 (2026).
- Putra, Adrian Bima. "The Legal Standing of Deepfake Digital Evidence in Criminal Proceedings: Challenges of Evidentiary Integrity in the AI Era." *Fox Justi: Jurnal Ilmu Hukum* 16, no. 1 (2026).

Ravizki, Eka Nanda, dan Lintang Yudhantaka. “Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia.” *Notaire* 5, no. 3 (2022): 351–376.