PUNGGAWA
SOCIAL INQUIRY

Punggawa Social Inquiry
Volume 1, Number 3, 2026
E-ISSN: 3164-015X
Open Access: punggawajournal.com/psi

Pembaharuan Hukum Pidana Siber: Mengatasi Kesenjangan Normatif Pada Kejahatan Berbasis Kecerdasan Buatan (*Artificial Intelligence*)

Firda Suci Ramadhani[1], Nur Fadhillah Mappaselleng[2]
[1,2] Magister Ilmu Hukum, Pascasarjana Universitas Muslim Indonesia, Indonesia
Korespondensi: firdasuci1411@gmail.com

Informasi Artikel

Riwayat artikel:
Received Sept 30th, 2026
Revised Nov 5th, 2026
Accepted Nov 18th, 2026

Keyword:
Artificial Intelligence; Normative Gap; Cybercrime; Criminal Law Reform; Criminal Liability; Legal Reform.

ABSTRAK

Perkembangan kecerdasan buatan (Artificial Intelligence/AI), khususnya teknologi generatif, memperluas kemampuan produksi dan manipulasi teks, gambar, suara, serta video. Di satu sisi, teknologi tersebut mendukung inovasi dan efisiensi; di sisi lain, ia dapat dimanfaatkan untuk penipuan, pemalsuan identitas, pemerasan, penyebaran konten sintetis tanpa persetujuan, dan manipulasi informasi. Perkembangan ini menimbulkan tantangan terhadap hukum pidana, terutama mengenai kecukupan rumusan delik, atribusi perbuatan, pembuktian digital, dan pertanggungjawaban pihak yang terlibat. Artikel ini bertujuan menilai kemampuan hukum pidana Indonesia menjangkau kejahatan berbasis AI dan merumuskan arah pembaharuan yang menjaga legalitas serta perlindungan korban. Penelitian menggunakan metode hukum normatif melalui pendekatan perundang-undangan dan konseptual, dengan bahan hukum berupa KUHP, UU ITE, UU Perlindungan Data Pribadi, dan literatur ilmiah. Analisis menunjukkan bahwa sejumlah tindak pidana berbasis AI telah dapat dijangkau oleh norma yang ada, tetapi pengaturan tersebut masih tersebar dan tidak secara khusus merumuskan penyalahgunaan konten sintetis, impersonasi digital, serta standar penentuan tanggung jawab dalam ekosistem AI. Keterbatasan ini lebih tepat disebut kesenjangan normatif dan problem harmonisasi daripada kekosongan hukum total. Pembaharuan diperlukan melalui definisi yang presisi, penguatan pedoman penerapan norma, standar pembuktian digital, mekanisme pemulihan korban, dan kewajiban pencegahan yang proporsional bagi penyelenggara teknologi.

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Kemajuan kecerdasan buatan (Artificial Intelligence/AI) telah mengubah cara informasi diproduksi, diolah, disebarkan, dan digunakan dalam kehidupan sehari-hari. Model AI generatif mampu menghasilkan teks, gambar, suara, maupun video dengan tingkat kemiripan yang semakin tinggi terhadap materi autentik. Teknologi tersebut memberikan manfaat dalam berbagai bidang, seperti pendidikan, industri kreatif, layanan publik, dan aktivitas ekonomi (Sihombing & Syaputra, 2020), tetapi pada saat yang sama membuka ruang bagi penyalahgunaan teknologi. Konten sintetis dapat digunakan untuk meniru identitas seseorang, membuat komunikasi palsu yang meyakinkan, memanipulasi bukti visual, maupun menyebarkan informasi yang menyesatkan (Situmeang, 2021). Risiko tersebut semakin kompleks karena produksi konten berbasis AI dapat dilakukan secara cepat, berbiaya relatif rendah, dan disebarkan melalui platform digital yang melampaui batas wilayah hukum.

Salah satu bentuk penyalahgunaan AI yang semakin mendapat perhatian ialah deepfake, yaitu konten audio-visual sintetis atau manipulatif yang membuat seseorang tampak atau terdengar melakukan sesuatu yang sebenarnya tidak dilakukan. Teknologi deepfake dapat digunakan dalam berbagai bentuk kejahatan, antara lain penipuan berbasis suara, pemerasan, pencemaran reputasi,

pornografi nonkonsensual, disinformasi, serta penyalahgunaan identitas. Perbuatan tersebut pada dasarnya tidak selalu membentuk jenis tindak pidana yang sepenuhnya baru, karena teknologi AI dapat berfungsi sebagai alat, metode, atau sarana untuk melaksanakan tindak pidana yang telah dikenal dalam hukum pidana (Amboro & Komarhana, 2021; Jaya & Goh, 2021). Namun, karakteristik teknologi deepfake menimbulkan persoalan hukum baru, terutama berkaitan dengan keaslian konten elektronik, penelusuran sumber informasi, identifikasi pelaku, pembuktian hubungan antara tindakan manusia dan keluaran sistem AI, serta penentuan bentuk pertanggungjawaban pidana (Fadlian, 2020).

Dalam konteks hukum Indonesia, sejumlah ketentuan hukum pidana dan hukum siber telah memiliki relevansi terhadap penanggulangan penyalahgunaan AI dan deepfake. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik memuat ketentuan yang berkaitan dengan informasi dan dokumen elektronik, termasuk pengaturan mengenai konten tertentu serta manipulasi informasi elektronik (Budhijanto, 2017; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024, 2024). Di sisi lain, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana Nasional menyediakan kerangka umum mengenai tindak pidana, kesalahan, subjek hukum, dan pertanggungjawaban pidana yang mulai berlaku pada 2 Januari 2026 (Undang-Undang Republik Indonesia Nomor 1 Tahun 2023, 2023). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga memiliki relevansi ketika penggunaan teknologi AI melibatkan pemrosesan data identitas, foto, suara, maupun data biometrik (Disemadi, 2021; Undang-Undang Republik Indonesia Nomor 27 Tahun 2022, 2022; Yuniarti, 2019). Keberadaan berbagai ketentuan tersebut menunjukkan bahwa hukum Indonesia pada dasarnya telah memiliki sejumlah instrumen yang dapat digunakan untuk merespons penyalahgunaan AI. Akan tetapi, keberadaan norma tersebut belum serta-merta menunjukkan bahwa seluruh karakteristik kejahatan deepfake telah diatur secara jelas dan komprehensif.

Persoalan hukum tersebut semakin terlihat karena penyalahgunaan deepfake dapat bersinggungan dengan berbagai kepentingan hukum dan konstruksi tindak pidana. Manipulasi identitas dapat berkaitan dengan penipuan, pemalsuan atau manipulasi informasi elektronik, pelanggaran privasi, tindak pidana kesusilaan, maupun serangan terhadap kehormatan seseorang (Niffari, 2020; Priscyllia, 2019). Namun, tidak setiap perbuatan yang menggunakan teknologi deepfake secara otomatis memenuhi seluruh unsur tindak pidana tersebut. Demikian pula, tidak setiap keluaran sistem AI yang menimbulkan kerugian dapat langsung dibebankan sebagai tindak pidana kepada pengguna, pengembang, atau pihak lain tanpa terlebih dahulu menguji unsur perbuatan, kesalahan, hubungan kausal, dan keterlibatan subjek hukum (Fadlian, 2020). Kondisi tersebut menunjukkan adanya persoalan mengenai kecukupan dan kejelasan norma dalam menghadapi karakteristik kejahatan berbasis AI. Oleh karena itu, persoalan tersebut lebih tepat dipahami sebagai persoalan kesenjangan normatif, keterbatasan jangkauan norma, serta kemungkinan ketidakjelasan penerapan hukum daripada semata-mata sebagai kekosongan hukum.

Permasalahan tersebut menjadi penting dikaji melalui perspektif pembaharuan hukum pidana siber karena perkembangan teknologi berlangsung lebih cepat dibandingkan perubahan regulasi. Hukum pidana pada dasarnya dibatasi oleh prinsip legalitas yang menuntut agar suatu perbuatan dapat dipidana berdasarkan ketentuan hukum yang telah ada dan dirumuskan secara jelas (Arief, 2018). Pada saat yang sama, perkembangan teknologi menuntut hukum memiliki kemampuan untuk memberikan perlindungan yang efektif terhadap korban dan merespons bentuk kejahatan baru (Ali & Wibowo, 2018). Kondisi tersebut menimbulkan kebutuhan untuk menguji apakah norma hukum pidana dan hukum siber yang berlaku telah memadai untuk menjangkau karakteristik penyalahgunaan AI, khususnya deepfake, atau masih terdapat aspek yang memerlukan penyesuaian dan pembaharuan. Dengan demikian, pembaharuan hukum tidak hanya diarahkan pada pembentukan norma baru, tetapi juga pada harmonisasi dan penyempurnaan norma yang telah tersedia agar mampu memberikan kepastian hukum, perlindungan korban, serta efektivitas penegakan hukum.

Sejumlah penelitian terdahulu telah membahas berbagai persoalan hukum yang muncul akibat perkembangan teknologi *deepfake* di Indonesia. Nabilah dkk. (2026) mengkaji pertanggungjawaban pidana atas penyalahgunaan teknologi *deepfake* sebagai salah satu bentuk kejahatan digital. Sementara itu, Banfatin dkk. (2025) menganalisis pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi *artificial intelligence deepfake* dalam tindak pidana *cybercrime*, khususnya dengan menyoroti belum adanya regulasi yang secara khusus mengatur *deepfake* serta keterbatasan instrumen hukum yang dapat digunakan. Di sisi lain, Tekayadi dkk. (2026) membahas konstruksi hukum pidana terhadap

kejahatan *deepfake* dalam konteks manipulasi bukti digital melalui penafsiran terhadap unsur-unsur delik dalam UU ITE dan KUHP Nasional. Secara umum, penelitian-penelitian tersebut menunjukkan bahwa perkembangan teknologi *deepfake* menghadirkan sejumlah persoalan hukum, mulai dari pertanggungjawaban pidana, kecukupan regulasi siber, konstruksi norma pidana, hingga aspek pembuktian digital (Banfatin dkk., 2025; Nabilah dkk., 2026; Tekayadi dkk., 2026).

Meskipun demikian, penelitian terdahulu tersebut cenderung memberikan perhatian pada aspek tertentu dari persoalan deepfake, baik mengenai pertanggungjawaban pelaku, penerapan ketentuan hukum yang tersedia, tantangan pembuktian digital, maupun evaluasi kesiapan regulasi. Kajian yang secara khusus mengintegrasikan persoalan tersebut untuk menguji kecukupan hukum pidana siber sekaligus merumuskan kebutuhan pembaharuan hukum dalam menghadapi karakteristik kejahatan berbasis AI masih perlu dikembangkan. Kesenjangan tersebut menjadi penting karena penyalahgunaan deepfake tidak hanya menimbulkan persoalan mengenai siapa yang dapat dimintai pertanggungjawaban, tetapi juga mengenai apakah konstruksi norma yang tersedia mampu mengidentifikasi perbuatan yang dilarang, menentukan kepentingan hukum yang dilindungi, mengakomodasi karakteristik alat dan metode kejahatan berbasis AI, serta memberikan dasar hukum yang memadai bagi penegakan hukum.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan mengkaji pembaharuan hukum pidana siber di Indonesia dalam menghadapi perkembangan kejahatan berbasis kecerdasan buatan, khususnya penyalahgunaan teknologi deepfake. Penelitian ini secara khusus diarahkan untuk mengidentifikasi ketentuan hukum yang dapat digunakan untuk menanggulangi kejahatan berbasis AI, menganalisis kesenjangan normatif dan problem penerapannya, serta merumuskan arah pembaharuan hukum yang dapat memberikan kepastian hukum, perlindungan terhadap korban, dan efektivitas penegakan hukum terhadap kejahatan siber berbasis kecerdasan buatan. Dengan tujuan tersebut, penelitian tidak hanya berorientasi pada identifikasi ketentuan hukum yang telah tersedia, tetapi juga menguji kecukupan dan relevansinya terhadap karakteristik kejahatan deepfake.

Penelitian ini diharapkan memberikan kontribusi terhadap pengembangan ilmu hukum, khususnya hukum pidana dan hukum siber, melalui kajian mengenai relevansi, kecukupan, dan kebutuhan pembaharuan regulasi dalam menghadapi kejahatan berbasis kecerdasan buatan. Secara teoretis, penelitian ini diharapkan dapat memperkaya kajian hukum pidana siber mengenai hubungan antara perkembangan teknologi AI, prinsip legalitas, pertanggungjawaban pidana, dan perlindungan hukum terhadap korban. Secara praktis, hasil penelitian diharapkan dapat menjadi bahan pertimbangan bagi pembentuk undang-undang, aparat penegak hukum, dan pihak terkait dalam merumuskan serta menerapkan kebijakan hukum pidana siber yang adaptif terhadap perkembangan teknologi, tetapi tetap menjamin kepastian hukum, perlindungan hak, dan proporsionalitas penegakan hukum.

Kebaruan penelitian ini terletak pada pendekatan yang mengintegrasikan analisis terhadap kecukupan norma hukum yang berlaku dengan kebutuhan pembaharuan hukum pidana siber dalam menghadapi kejahatan berbasis kecerdasan buatan, khususnya deepfake. Berbeda dengan penelitian terdahulu yang lebih terfokus pada pertanggungjawaban pidana, konstruksi hukum, pembuktian, atau kesiapan regulasi secara parsial, penelitian ini menempatkan persoalan tersebut dalam satu kerangka analisis untuk menilai kemampuan hukum pidana siber Indonesia dalam menjangkau karakteristik kejahatan deepfake. Analisis diarahkan pada relevansi KUHP Nasional, UU ITE, serta ketentuan hukum terkait lainnya untuk mengidentifikasi kesenjangan normatif dan merumuskan arah pembaharuan hukum yang diperlukan. Dengan demikian, penelitian ini tidak berhenti pada identifikasi persoalan hukum, tetapi berupaya memberikan argumentasi normatif mengenai kebutuhan pengembangan hukum pidana siber yang lebih adaptif terhadap perkembangan kecerdasan buatan, memberikan kepastian hukum, serta menjamin perlindungan terhadap korban.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang menempatkan peraturan perundang-undangan, asas hukum, dan doktrin sebagai objek analisis. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach) (Tan, 2021). Pendekatan perundang-undangan dilakukan dengan mengkaji UU Nomor 1 Tahun 2023 tentang KUHP, UU Nomor 1 Tahun 2024 tentang perubahan kedua UU ITE, UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta ketentuan lain yang relevan. Pendekatan konseptual

digunakan untuk membahas asas legalitas, kesalahan, pertanggungjawaban pidana, kejahatan siber, konten sintetis, dan pembaharuan hukum.

Bahan hukum primer terdiri atas peraturan perundang-undangan. Bahan hukum sekunder meliputi artikel jurnal, karya ilmiah, dan literatur yang membahas deepfake, AI, penegakan hukum pidana, dan bukti digital (Tan, 2021). Bahan dikumpulkan melalui studi kepustakaan dan penelusuran pada portal peraturan resmi serta laman jurnal. Analisis dilakukan secara kualitatif-preskriptif, yaitu mengidentifikasi norma, menguji kecocokannya dengan karakter perbuatan berbasis AI, mengevaluasi batas penerapan berdasarkan unsur delik, dan menyusun rekomendasi reformasi (Tan, 2021). Penelitian ini tidak menggunakan data empiris lapangan, sehingga kesimpulan mengenai efektivitas penegakan hukum dibatasi pada analisis normatif, bukan klaim mengenai kinerja faktual aparat atau prevalensi kasus.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa perkembangan kecerdasan buatan (Artificial Intelligence/AI), khususnya teknologi generatif dan deepfake, telah menimbulkan persoalan baru dalam penerapan hukum pidana siber di Indonesia. AI pada dasarnya tidak dapat diposisikan secara otomatis sebagai pelaku tindak pidana, melainkan sebagai sarana, alat, atau metode yang digunakan oleh manusia atau badan hukum untuk melakukan suatu perbuatan (Amboro & Komarhana, 2021; Jaya & Goh, 2021). Dalam konteks tersebut, hukum pidana Indonesia melalui UU ITE, KUHP Nasional, dan UU Perlindungan Data Pribadi telah menyediakan sejumlah norma yang dapat digunakan untuk menanggulangi berbagai bentuk penyalahgunaan AI. Namun, penerapan norma tersebut masih bergantung pada terpenuhinya unsur delik masing-masing dan belum membentuk kerangka hukum yang secara khusus mengatur keseluruhan karakteristik kejahatan berbasis AI, khususnya deepfake. Kondisi tersebut menunjukkan adanya kesenjangan normatif, fragmentasi pengaturan, serta persoalan atribusi, pembuktian, pertanggungjawaban, dan perlindungan korban.

Tabel 1 Hasil Analisis Pengaturan Hukum terhadap Kejahatan Berbasis AI

No.	Aspek Pembahasan	Dasar Hukum/Kajian	Hasil Analisis
1	AI sebagai sarana tindak pidana	Konsep pertanggungjawaban pidana	AI pada dasarnya merupakan alat atau sarana. Pertanggungjawaban pidana diarahkan kepada manusia atau korporasi yang memenuhi unsur tindak pidana dan syarat kesalahan.
2	Penyebaran konten bermuatan melanggar kesusilaan	Pasal 27 ayat (1) UU ITE	Dapat diterapkan terhadap penyebaran konten seksual sintetis apabila unsur perbuatan dan muatan dalam pasal terpenuhi.
3	Manipulasi kehormatan dan nama baik	Pasal 27A UU ITE	Dapat menjangkau konten deepfake yang menyerang kehormatan atau nama baik melalui tuduhan, sepanjang seluruh unsur delik terpenuhi.
4	Informasi bohong dalam transaksi elektronik	Pasal 28 ayat (1) UU ITE	Relevan terhadap penggunaan AI untuk menyebarkan informasi bohong yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

5	Informasi bohong yang menimbulkan kerusuhan	Pasal 28 ayat (3) UU ITE	Dapat diterapkan apabila pemberitahuan bohong yang disebarkan memenuhi unsur dan akibat berupa kerusuhan di masyarakat.
6	Manipulasi informasi elektronik	Pasal 35 jo. Pasal 51 ayat (1) UU ITE	Relevan terhadap pembuatan atau perubahan informasi elektronik secara melawan hukum dengan tujuan agar dianggap autentik.
7	Pertanggungjawaban pelaku dan korporasi	KUHP Nasional, Pasal 45–49 serta ketentuan penyertaan	Pertanggungjawaban ditentukan berdasarkan peran, kontribusi, kesalahan, dan keterlibatan masing-masing pihak.
8	Penyalahgunaan identitas digital	Pasal 65 UU PDP	Dapat menjangkau perolehan, pengungkapan, atau penggunaan data pribadi secara melawan hukum.
9	Kesenjangan normatif	Analisis UU ITE, KUHP, dan UU PDP	Belum terdapat pengaturan khusus yang secara menyeluruh mengakomodasi pembuatan, penggunaan, distribusi, dan pemulihan akibat konten sintetis.
10	Arah pembaharuan hukum	Reformulasi kebijakan hukum pidana siber	Diperlukan kejelasan definisi dan unsur delik, pengaturan pertanggungjawaban berdasarkan peran, penguatan pembuktian digital, serta perlindungan korban.

Berdasarkan Tabel 1, dapat diketahui bahwa hukum Indonesia pada dasarnya telah memiliki sejumlah instrumen hukum yang dapat digunakan untuk menanggulangi penyalahgunaan teknologi kecerdasan buatan. Akan tetapi, daya jangkau setiap ketentuan berbeda-beda dan sangat bergantung pada terpenuhi atau tidaknya unsur delik. Dengan demikian, keberadaan norma hukum yang dapat diterapkan terhadap sebagian bentuk penyalahgunaan AI tidak berarti bahwa seluruh karakteristik kejahatan deepfake telah memperoleh pengaturan yang komprehensif. Persoalan tersebut selanjutnya dapat dianalisis melalui beberapa aspek berikut.

1. AI sebagai Sarana, Metode, dan Konteks Tindak Pidana Siber

AI tidak secara otomatis diposisikan sebagai pelaku tindak pidana, melainkan sebagai sarana yang digunakan manusia atau badan hukum. Pertanggungjawaban pidana tetap ditentukan berdasarkan tindakan, kesalahan, dan keterlibatan subjek hukum. Dalam praktiknya, AI dapat digunakan untuk meningkatkan skala kejahatan, memanipulasi identitas melalui *deepfake*, maupun memproses data pribadi secara melawan hukum.

Tantangan penegakan hukum muncul karena konten sintetis dapat menyerupai materi autentik, melibatkan banyak pihak, dan tersebar melalui berbagai platform. Oleh karena itu, penggunaan AI harus dianalisis sebagai bagian dari modus operandi tindak pidana, sedangkan pertanggungjawaban tetap didasarkan pada peran dan kesalahan masing-masing pihak.

2. UU ITE: Norma yang Dapat Diterapkan dan Batas Jangkauannya

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE menyediakan sejumlah ketentuan yang dapat diterapkan terhadap penyalahgunaan AI sepanjang unsur deliknya terpenuhi. Pasal 27 ayat (1) dapat relevan terhadap penyebaran konten *deepfake* bermuatan melanggar kesusilaan, sedangkan Pasal 27A berkaitan dengan serangan terhadap kehormatan atau nama baik melalui konten manipulatif. Pasal 28 ayat (1) dapat diterapkan terhadap penyebaran informasi bohong yang merugikan konsumen dalam transaksi elektronik, sementara Pasal 28 ayat (3) berkaitan dengan pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat. Adapun Pasal 35 jo. Pasal 51 ayat (1) memiliki relevansi terhadap manipulasi atau penciptaan informasi elektronik secara sengaja dan melawan hukum dengan tujuan agar dianggap seolah-olah autentik. Namun, tidak seluruh konten sintetis dapat dipidana karena penerapannya harus memenuhi unsur delik, termasuk tujuan dan konteks perbuatannya.

Dengan demikian, UU ITE telah menjangkau beberapa bentuk penyalahgunaan AI, tetapi belum mengatur secara khusus keseluruhan siklus *deepfake*, mulai dari pembuatan hingga pemulihan dampak terhadap korban. Kondisi ini menunjukkan perlunya harmonisasi dan penguatan norma hukum yang proporsional.

3. KUHP Nasional: Kesalahan, Penyertaan, dan Pertanggungjawaban Korporasi dalam Ekosistem AI

KUHP Nasional melalui Undang-Undang Nomor 1 Tahun 2023 berlaku sejak 2 Januari 2026. Ketentuan ini memberikan kerangka umum mengenai tindak pidana dan pertanggungjawaban, tetapi belum membentuk delik khusus mengenai AI. Apabila AI digunakan untuk melakukan penipuan, pemerasan, atau tindak pidana lainnya, pertanggungjawaban tetap didasarkan pada unsur delik, perbuatan, dan kesalahan pelaku. Dalam kejahatan yang melibatkan beberapa pihak, ketentuan penyertaan menjadi penting untuk menilai kontribusi masing-masing pihak, termasuk pengguna, operator, dan pihak yang menyebarkan konten.

Pengembang maupun penyedia platform tidak dapat dipidana semata-mata karena teknologinya disalahgunakan. Pertanggungjawaban harus didasarkan pada keterlibatan dan unsur hukum yang dapat dibuktikan. Hal serupa berlaku terhadap korporasi, dengan mempertimbangkan kebijakan, perintah, manfaat, pengawasan, dan hubungan aktivitas korporasi dengan tindak pidana. Dengan demikian, KUHP Nasional berfungsi sebagai dasar penentuan kesalahan dan pertanggungjawaban pelaku, yang penerapannya perlu diharmonisasikan dengan UU ITE dan UU PDP.

4. UU Perlindungan Data Pribadi dan Perlindungan Identitas Digital

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi relevan terhadap penggunaan AI yang melibatkan data pribadi, termasuk foto, rekaman suara, dan data biometrik. Penggunaan data tersebut untuk membentuk identitas sintetis dapat menimbulkan persoalan terkait dasar pemrosesan, tujuan penggunaan, dan penggunaan data secara melawan hukum. Pasal 65 UU PDP mengatur larangan memperoleh, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya secara melawan hukum. Ketentuan ini dapat diterapkan apabila data seseorang digunakan sebagai bahan pembuatan identitas sintetis tanpa dasar yang sah. Namun, penggunaan wajah atau suara dalam konten *deepfake* tidak otomatis merupakan pelanggaran UU PDP. Penilaiannya bergantung pada sifat data, cara memperolehnya, dasar pemrosesan, dan tujuan penggunaannya.

Oleh karena itu, perlindungan korban *deepfake* memerlukan harmonisasi UU PDP, UU ITE, dan KUHP. UU PDP melindungi pemrosesan data pribadi, UU ITE mengatur manipulasi informasi elektronik, sedangkan KUHP menjadi dasar pertanggungjawaban pidana.

5. Letak Kesenjangan Normatif: Bukan Kekosongan Hukum Total

Berdasarkan ketiga instrumen hukum tersebut, persoalan penyalahgunaan AI lebih tepat dikategorikan sebagai kesenjangan normatif daripada kekosongan hukum secara total. Kesenjangan tersebut meliputi empat aspek. Pertama, kesenjangan definisi, yaitu belum adanya pengaturan khusus yang membedakan manipulasi sintetis, impersonasi digital, dan penggunaan AI yang sah. Kedua, kesenjangan unsur perbuatan, karena norma yang tersedia lebih menitikberatkan pada distribusi, akibat, atau tujuan tertentu sehingga belum seluruh tahapan pembuatan dan pemanfaatan konten sintetis dapat dijangkau. Ketiga, kesenjangan atribusi dan pertanggungjawaban, mengingat kejahatan berbasis AI dapat melibatkan pengguna, pengembang, penyedia platform, dan korporasi dengan kontribusi yang berbeda. Keempat, kesenjangan pemulihan korban, terutama terkait mekanisme pengamanan bukti, penghentian distribusi, penghapusan konten ilegal, pencegahan pengunggahan ulang, dan pemulihan reputasi.

Kesenjangan tersebut tidak dapat dijadikan dasar untuk memperluas kriminalisasi melalui analogi. Penerapan hukum tetap harus berpedoman pada asas legalitas, kepastian hukum, dan pemenuhan unsur tindak pidana.

6. Model Pembaharuan Hukum Pidana Siber yang Proporsional

Pembaharuan hukum pidana siber perlu diarahkan pada penguatan norma dan perlindungan korban. Secara normatif, diperlukan pertimbangan mengenai definisi konten sintetis dan impersonasi digital serta rumusan delik yang secara jelas mengatur manipulasi identitas tanpa persetujuan untuk tujuan melawan hukum. Rumusan tersebut harus memperhatikan asas legalitas, unsur kesalahan, tujuan atau akibat perbuatan, serta perlindungan terhadap penggunaan AI yang sah, seperti seni, pendidikan, penelitian, dan kritik. Pertanggungjawaban juga harus didasarkan pada peran dan kendali masing-masing pihak, bukan semata-mata status sebagai pengguna atau penyedia teknologi. Selain itu, penguatan pembuktian digital diperlukan melalui pelestarian metadata, autentikasi, pencatatan *hash*, dan dokumentasi *chain of custody*.

Dari sisi perlindungan korban, diperlukan mekanisme pelaporan, penanganan dan penghapusan konten ilegal secara cepat, serta pencegahan pengunggahan ulang. Upaya tersebut perlu disertai penguatan kapasitas aparat dalam memahami AI generatif dan forensik digital.

Dengan demikian, pembaharuan hukum harus menyeimbangkan penanggulangan kejahatan, perlindungan korban, kepastian hukum, kebebasan berekspresi, dan perkembangan teknologi.

KESIMPULAN

Kejahatan berbasis kecerdasan buatan menimbulkan tantangan terhadap hukum pidana siber karena teknologi generatif memungkinkan manipulasi identitas, konten, dan komunikasi digital dengan tingkat realisme tinggi. Hukum Indonesia telah menyediakan norma yang dapat digunakan terhadap sejumlah perbuatan tersebut melalui UU ITE, KUHP Nasional, dan UU Perlindungan Data Pribadi. Pasal 27 ayat (1), Pasal 27A, Pasal 28 ayat (1) dan ayat (3), serta Pasal 35 UU ITE dapat relevan dalam konteks tertentu, tetapi penerapannya bergantung pada pemenuhan unsur delik. KUHP menyediakan kerangka pertanggungjawaban individual dan korporasi, sedangkan UU PDP memberikan perlindungan terhadap pemrosesan data pribadi yang melawan hukum.

Dengan demikian, persoalan hukum AI lebih tepat dipahami sebagai kesenjangan normatif, fragmentasi regulasi, dan tantangan penerapan serta pembuktian, bukan kekosongan hukum total. Pembaharuan diperlukan melalui definisi dan rumusan norma yang lebih presisi terhadap penyalahgunaan konten sintetis, penguatan standar bukti digital, pembagian tanggung jawab berdasarkan peran dan kesalahan, kewajiban pencegahan yang proporsional, serta mekanisme perlindungan dan pemulihan korban. Pembaharuan tersebut harus mempertahankan asas legalitas, proporsionalitas, dan perlindungan kebebasan berekspresi. Dengan pendekatan yang harmonis dan adaptif, hukum pidana siber Indonesia dapat menjangkau penyalahgunaan AI secara lebih efektif tanpa menghambat penggunaan teknologi yang sah.

DAFTAR PUSTAKA

Ali, M., & Wibowo, A. (2018). Kompensasi dan restitusi yang berorientasi pada korban tindak pidana. Yuridika, 33(2), 260–289. https://doi.org/10.20473/ydk.v33i2.7414

Amboro, Y. P., & Komarhana, K. (2021). Prospek kecerdasan buatan sebagai subjek hukum perdata di Indonesia. Law Review, 21(2), 145–172. https://doi.org/10.19166/lr.v0i2.3513

Arief, B. N. (2018). Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan. Prenada Media.

Banfatin, P. M., Medan, K. K., & Fallo, D. F. N. (2025). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. *Pemuliaan Keadilan*, *2*(1), 60–73. https://doi.org/10.62383/pk.v2i1.402

Budhijanto, D. (2017). Revolusi cyberlaw Indonesia: Pembaruan dan revisi Undang-Undang Informasi dan Transaksi Elektronik 2016. Refleksi Hukum: Jurnal Ilmu Hukum, 1(2), 115–130. https://doi.org/10.24246/jrh.2017.v1.i2.p115-130

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. Jurnal Wawasan Yuridika, 5(2), 177–199. https://doi.org/10.25072/jwy.v5i2.460

Fadlian, A. (2020). Pertanggungjawaban pidana dalam suatu kerangka teoretis. Jurnal Hukum Positum, 5(2), 10–19. https://doi.org/10.35706/positum.v5i2.5556

Jaya, F., & Goh, W. (2021). Analisis yuridis terhadap kedudukan kecerdasan buatan atau artificial intelligence sebagai subjek hukum pada hukum positif Indonesia. Supremasi Hukum: Jurnal Penelitian Hukum, 30(2), 1–11. https://doi.org/10.33592/jsh.v17i2.1287

Nabilah, A., Feriandref, A., & Ballan, O. (2026). Pertanggungjawaban pidana terhadap penyalahgunaan teknologi deepfake sebagai bentuk kejahatan digital. *Wajah Hukum*, *10*(2), 1035. https://doi.org/10.33087/wjh.v10i2.2220

Niffari, H. (2020). Perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi: Suatu tinjauan komparatif dengan peraturan perundang-undangan di negara lain. Jurnal Yuridis, 7(1), 105–119. https://doi.org/10.35586/jyur.v7i1.1846

Priscyllia, F. (2019). Perlindungan privasi data pribadi dalam perspektif perbandingan hukum. Jatiswara, 34(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218

Sari, I. (2020). Perbuatan melawan hukum (PMH) dalam hukum pidana dan hukum perdata. Jurnal Ilmiah Hukum Dirgantara, 11(1), 53–70. https://doi.org/10.35968/jh.v11i1.651

Sihombing, E. N. A. M., & Syaputra, M. Y. A. (2020). Implementasi penggunaan kecerdasan buatan dalam pembentukan peraturan daerah. Jurnal Ilmiah Kebijakan Hukum, 14(3), 419–434. https://doi.org/10.30641/kebijakan.2020.V14.419-434

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. Sasi, 27(1), 38–52. https://doi.org/10.47268/sasi.v27i1.394

Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. Nusantara: Jurnal Ilmu Pengetahuan Sosial, 8(8), 2463–2478. https://doi.org/10.31604/jips.v8i8.2021.2463-2478

Tekayadi, S. K., Efendi, S., & Rosikhu, M. (2026). Konstruksi hukum pidana terhadap kejahatan deepfake dalam perspektif manipulasi bukti digital. *Justice Voice*, *5*(1), 47–59. https://doi.org/10.37893/jv.v5i1.1367

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. (2023). Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2024). Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. Business Economic, Communication, and Social Sciences (BECOSS) Journal, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030