ISSN (P): (2580-8656)
ISSN (E): (2580-3883)

LEGAL STANDING
JURNAL ILMU HUKUM

Vol.9 Issue.5 (2025)

Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi *Deepfake* di Indonesia

***Supuan Sultan Al Alif[1], Anis Rindiani[2], Cik Marhayati[3]**
[1-3]Universitas Pertiba, Jl. Adhiyaksa No.9, Pangkal Pinang, Kepulauan Bangka Belitung, Indonesia
*supuansultan@gmail.com

ABSTRACT

The development of Deepfake technology presents new challenges for Indonesian criminal law, particularly in the field of cybercrime. Deepfake, as an artificial intelligence creation, can realistically manipulate audio and video, making it susceptible to misuse for fraud, non-consensual pornography, defamation, and digital identity theft. This study focuses on the construction of Indonesian criminal law in addressing Deepfake-based cybercrime. The research employs a normative juridical approach combined with a comparative study. The data consist of primary legal materials (the ITE Law, the Criminal Code, the Personal Data Protection Law, and court decisions), secondary legal materials (scholarly journals, books, research reports), and tertiary legal materials (legal dictionaries, encyclopedias). Data were collected through library research and documentation, and analyzed using descriptive-comparative techniques. Data validity was ensured through source triangulation and cross-verification. The findings show that the construction of Indonesian criminal law in handling Deepfake-related crimes still relies on extensive interpretation of the ITE Law (Articles 27, 28, 35) and relevant provisions of the Criminal Code on morality, fraud, and defamation. However, this construction remains inadequate, as there is no explicit provision regulating AI-based content manipulation, leading to legal uncertainty in terms of offense elements, evidentiary standards, and criminal liability. Nevertheless, there is potential for adaptation through analogical interpretation, the broad jurisdiction principle of the ITE Law, and general criminal sanctions. To strengthen this legal construction, it is necessary to establish specific regulations defining Deepfake in legal terms, provide graded sanctions based on impact, ensure victim protection (including the right to be forgotten), and impose preventive obligations on digital platforms.

Perkembangan teknologi *Deepfake* menimbulkan persoalan baru dalam hukum pidana Indonesia, khususnya dalam ranah kejahatan siber. *Deepfake*, sebagai hasil rekayasa artificial intelligence, mampu memanipulasi audio dan video secara realistis sehingga berpotensi disalahgunakan untuk penipuan, pornografi non-konsensual, pencemaran nama baik, maupun pencurian identitas digital. Penelitian ini berfokus pada konstruksi hukum pidana Indonesia dalam menanggulangi kejahatan siber berbasis *Deepfake*. Metode penelitian menggunakan pendekatan yuridis normatif dengan studi komparatif. Data terdiri atas bahan hukum primer (UU ITE, KUHP, UU Perlindungan Data Pribadi, putusan pengadilan), bahan hukum sekunder (jurnal ilmiah, buku, laporan penelitian), dan bahan hukum tersier (kamus hukum, ensiklopedia). Data dikumpulkan melalui studi kepustakaan dan dokumentasi, kemudian

dianalisis dengan teknik deskriptif-komparatif. Keabsahan data dijaga melalui triangulasi sumber dan verifikasi silang. Hasil penelitian menunjukkan bahwa konstruksi hukum pidana Indonesia terhadap kejahatan *Deepfake* masih bertumpu pada interpretasi ekstensif UU ITE (Pasal 27, 28, 35) dan pasal-pasal KUHP mengenai kesusilaan, penipuan, dan pencemaran nama baik. Namun, konstruksi tersebut belum memadai karena tidak ada norma eksplisit yang mengatur manipulasi konten berbasis AI, sehingga menimbulkan ketidakpastian hukum dalam aspek delik, pembuktian, dan pertanggungjawaban pidana. Meski demikian, terdapat potensi adaptasi melalui asas analogi, prinsip yurisdiksi luas UU ITE, serta sanksi pidana umum. Untuk memperkuat konstruksi hukum, diperlukan regulasi khusus yang mendefinisikan *Deepfake* secara yuridis, mengatur gradasi sanksi sesuai dampak, menjamin perlindungan korban (termasuk hak untuk dilupakan), serta mewajibkan peran preventif platform digital.

Kata Kunci: *Deepfake, Hukum Pidana Siber, Rekonstruksi Hukum.*

A. PENDAHULUAN

Perkembangan teknologi artificial intelligence (AI) dalam bentuk *Deepfake* telah menimbulkan persoalan hukum yang kompleks dan mendesak dalam sistem peradilan pidana Indonesia. Pada tahun 2023, Indonesia mengalami peningkatan signifikan kasus kejahatan siber berbasis *Deepfake*, termasuk kasus viral video *Deepfake* yang melibatkan tokoh publik dan kasus penipuan menggunakan suara sintetis yang merugikan korban hingga miliaran rupiah (Ananta et al., 2024). Kepolisian Republik Indonesia mencatat adanya kesulitan dalam menangani kasus-kasus tersebut karena keterbatasan regulasi yang spesifik mengatur teknologi *Deepfake*, sementara pelaku memanfaatkan celah hukum ini untuk menghindari jeratan pidana. Persoalan konkrit ini menunjukkan adanya legal vacuum dalam sistem hukum pidana Indonesia yang tidak mampu mengantisipasi karakteristik unik kejahatan berbasis *Deepfake*.

Deepfake, sebagai teknologi yang menggunakan algoritma machine learning untuk menciptakan atau memanipulasi konten video, audio, dan gambar secara realistis, telah berkembang dengan pesat dan semakin mudah diakses oleh masyarakat umum. Teknologi ini memungkinkan seseorang untuk "mengganti" wajah atau suara orang lain dalam konten digital dengan tingkat kemiripan yang sangat tinggi, sehingga sulit dibedakan dengan konten asli. Kemudahan akses terhadap aplikasi *Deepfake* melalui platform digital dan rendahnya biaya produksi telah menjadikan teknologi ini sebagai instrumen baru dalam berbagai bentuk kejahatan siber (Faridi, 2019). Di Indonesia, pemanfaatan *Deepfake* untuk tujuan kriminal mulai bermunculan dalam bentuk pornografi non-konsensual, penipuan identitas, manipulasi berita (*hoax*), pencemaran nama baik, dan penipuan finansial.

Kompleksitas permasalahan hukum *Deepfake* terletak pada karakteristik teknologinya yang berbeda dengan bentuk kejahatan siber konvensional. Pertama,

Deepfake menciptakan tantangan dalam aspek pembuktian karena teknologi ini menghasilkan konten palsu yang sangat menyerupai kenyataan, sehingga memerlukan analisis forensik digital yang canggih untuk mengidentifikasi keasliannya. Kedua, sifat lintas batas (*borderless*) teknologi *Deepfake* memungkinkan pelaku beroperasi dari yurisdiksi yang berbeda, menciptakan kompleksitas dalam proses penyelidikan dan penuntutan. Ketiga, kecepatan penyebaran konten *Deepfake* melalui media sosial dan platform digital dapat menimbulkan kerugian yang masif dalam waktu singkat, sementara proses hukum memerlukan waktu yang relatif lama (Novera & Fitri, 2024).

Dalam konteks hukum pidana Indonesia, pengaturan kejahatan siber saat ini masih mengandalkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) (Sujamawardi, 2018). Namun, kedua regulasi tersebut belum secara spesifik mengatur karakteristik khusus kejahatan *Deepfake*. UU ITE lebih berfokus pada kejahatan konvensional seperti pencemaran nama baik, pornografi, dan penipuan dalam konteks digital, namun tidak mengakomodasi aspek manipulasi konten berbasis AI yang memiliki tingkat sofistikasi tinggi (Harun & Nurhadiyanto, 2024). Demikian pula KUHP, meskipun memiliki pasal-pasal yang dapat diterapkan secara analogis, namun tidak mampu menangkap esensi kejahatan *Deepfake* yang memiliki modus operandi dan dampak yang berbeda.

Kekosongan hukum ini semakin problematik ketika melihat tren global penggunaan *Deepfake* untuk tujuan kriminal. Berdasarkan laporan Deeptrace tahun 2023, penggunaan *Deepfake* untuk kejahatan meningkat 900% dalam dua tahun terakhir, dengan mayoritas digunakan untuk pornografi non-konsensual (96%) dan penipuan (4%) (Kurniarullah et al., 2024). Sementara itu, berbagai negara seperti Amerika Serikat, Inggris, dan Singapura telah mulai mengembangkan regulasi khusus untuk menangani kejahatan *Deepfake*, termasuk melalui kriminalisasi spesifik terhadap pembuatan dan penyebaran konten *Deepfake* yang merugikan.

Tantangan implementasi hukum pidana terhadap kejahatan *Deepfake* juga berkaitan dengan kapasitas sumber daya manusia penegak hukum. Kompleksitas teknologi *Deepfake* memerlukan pemahaman mendalam tentang AI, machine learning, dan forensik digital yang belum sepenuhnya dikuasai oleh aparat penegak hukum Indonesia (Utara & Widyawati, 2025). Hal ini berdampak pada lemahnya proses penyelidikan, penyidikan, dan pembuktian di persidangan. Selain itu, keterbatasan infrastruktur teknologi dan peralatan forensik digital di berbagai daerah menjadi hambatan dalam penanganan kasus-kasus *Deepfake* secara efektif.

Dari perspektif korban, dampak kejahatan *Deepfake* memiliki dimensi yang lebih luas dibandingkan kejahatan siber konvensional. Korban tidak hanya mengalami kerugian materiil, tetapi juga kerugian psikologis, reputasi, dan sosial yang bersifat jangka panjang. Konten *Deepfake* yang bersifat pornografi non-konsensual, misalnya, dapat menimbulkan trauma psikologis yang berkelanjutan bagi korban, sementara

sistem hukum pidana Indonesia belum memiliki mekanisme perlindungan korban yang memadai untuk jenis kejahatan ini (Utara & Widyawati, 2025).

Urgensitas rekonstruksi hukum pidana untuk menangani kejahatan *Deepfake* juga didorong oleh potensi ancaman yang lebih besar terhadap stabilitas sosial dan politik. *Deepfake* dapat digunakan untuk memanipulasi informasi publik, menciptakan berita palsu yang dapat memicu konflik sosial, atau bahkan digunakan untuk tujuan terorisme dan subversi. Dalam konteks demokrasi, *Deepfake* berpotensi merusak integritas proses politik melalui manipulasi pidato atau pernyataan tokoh politik, yang dapat mempengaruhi opini publik dan hasil pemilihan umum (Kristiyenda et al., 2025).

Sejalan dengan urgensi tersebut, berbagai penelitian terdahulu turut menyoroti permasalahan hukum terkait penyalahgunaan *Deepfake*. Novera & Fitri (2024), misalnya, melalui penelitian "Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (*Deepfake*) dalam Penyebaran Konten Pornografi melalui Akun Media Sosial" menunjukkan bahwa penerapan pasal-pasal UU ITE masih bersifat analogis dan belum memberi perlindungan komprehensif bagi korban, sehingga diperlukan regulasi khusus yang mengatur secara eksplisit penggunaan *Deepfake* untuk tujuan kriminal.

Selanjutnya, Utara & Widyawati (2025) melalui penelitian "Analysis of Criminal Law Enforcement on Non-Consensual *Deepfake* Pornography in the Dissemination of Manipulative Content in Indonesia" menyoroti kendala teknis aparat penegak hukum dalam membuktikan keaslian konten *Deepfake* yang sangat realistis, serta merekomendasikan penguatan kapasitas forensik digital dan perlindungan korban.

Adapun Noerman & Ibrahim (2024) dalam penelitian "Kriminalisasi *Deepfake* di Indonesia sebagai Bentuk Pelindungan Negara" menegaskan adanya kekosongan hukum akibat ketiadaan definisi yuridis tentang *Deepfake*. Penelitian ini mengusulkan kriminalisasi khusus terhadap pembuatan dan penyebaran konten *Deepfake* yang merugikan, dengan tetap menjaga keseimbangan antara perlindungan hukum dan kebebasan berekspresi.

Berdasarkan kompleksitas permasalahan tersebut, diperlukan kajian mendalam mengenai konstruksi hukum pidana yang tepat untuk menanggulangi kejahatan siber berbasis teknologi *Deepfake* di Indonesia (Chandra et al., 2025). Penelitian ini menjadi penting untuk menganalisis kelemahan regulasi eksisting, mengidentifikasi tantangan yuridis dalam penerapannya, dan merumuskan rekomendasi rekonstruksi hukum yang dapat mengakomodasi karakteristik unik kejahatan *Deepfake*. Dengan demikian, diharapkan dapat tercipta sistem hukum pidana yang adaptif terhadap perkembangan teknologi dan mampu memberikan perlindungan hukum yang optimal bagi masyarakat di era digital (Prayuti, 2024).

B. METODE

Penelitian ini Penelitian ini menggunakan jenis penelitian hukum normatif (*normative legal research*), yaitu penelitian yang berfokus pada kajian peraturan perundang-undangan, putusan pengadilan, dan doktrin hukum yang relevan (Soekanto & Mamuji, 2013). Pendekatan yang digunakan adalah yuridis normatif dengan dikombinasikan pendekatan komparatif untuk menganalisis konstruksi hukum pidana Indonesia dalam menanggulangi kejahatan siber berbasis *Deepfake* sekaligus membandingkannya dengan regulasi di negara lain.

Sumber data terdiri dari: Bahan hukum primer: peraturan perundang-undangan terkait (UU ITE, KUHP, UU Perlindungan Data Pribadi, dan regulasi lain), putusan pengadilan yang relevan, serta regulasi mengenai *Deepfake* dari negara pembanding seperti Amerika Serikat, Uni Eropa, dan Singapura. Bahan hukum sekunder: buku ilmiah, jurnal hukum, artikel, laporan penelitian, serta working paper yang membahas kejahatan siber dan teknologi *Deepfake*. Bahan hukum tersier: kamus hukum, ensiklopedia, serta sumber referensi tambahan yang mendukung pemahaman konseptual.

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan metode dokumentasi terhadap peraturan, putusan pengadilan, dan literatur ilmiah. Selain itu, dilakukan penelusuran daring melalui database hukum, repositori jurnal, serta situs resmi lembaga terkait untuk memperoleh data terbaru mengenai perkembangan regulasi *Deepfake* (Marzuki, 2016).

Analisis data menggunakan analisis deskriptif-komparatif dengan pendekatan kualitatif. Data dianalisis secara sistematis melalui tahapan identifikasi norma, klasifikasi aturan, dan interpretasi terhadap ketentuan hukum yang relevan. Selanjutnya dilakukan perbandingan (*comparative analysis*) dengan regulasi dari negara lain untuk menemukan best practices dan mengidentifikasi adanya kekosongan hukum (*legal gap*) dalam sistem hukum pidana Indonesia. Keabsahan data dijamin melalui triangulasi sumber, yaitu dengan memverifikasi informasi dari peraturan, putusan, dan literatur akademik, serta melalui *cross-check* antar referensi agar hasil penelitian dapat dipertanggungjawabkan secara ilmiah (Moleong, 2018).

C. HASIL DAN PEMBAHASAN

1. Penerapan Hukum Pidana Terhadap Pelaku Yang Menggunakan *Deepfake* Untuk Kejahatan Siber

Penerapan hukum pidana Indonesia terhadap pelaku kejahatan siber yang menggunakan teknologi *Deepfake* menghadapi kompleksitas yuridis yang signifikan, mengingat belum adanya regulasi khusus yang secara spesifik mengatur teknologi artificial intelligence ini. Dalam praktik penegakan hukum, aparat kepolisian dan kejaksaan harus mengandalkan interpretasi ekstensif terhadap ketentuan-ketentuan

yang ada dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta pasal-pasal relevan dalam Kitab Undang-Undang Hukum Pidana (KUHP). Pendekatan analogis ini menciptakan ketidakpastian hukum dan berpotensi menimbulkan perbedaan penafsiran di antara penegak hukum, sehingga efektivitas penanganan kasus *Deepfake* menjadi tidak optimal (Meliana, 2025).

Dalam konteks UU ITE, beberapa pasal yang berpotensi diterapkan terhadap kejahatan *Deepfake* antara lain Pasal 27 ayat (1) yang mengatur tentang muatan yang melanggar kesusilaan, Pasal 27 ayat (3) mengenai pencemaran nama baik, Pasal 28 ayat (2) tentang informasi yang menimbulkan rasa kebencian berdasarkan SARA, dan Pasal 35 tentang manipulasi informasi elektronik. Namun, ketentuan-ketentuan tersebut tidak secara eksplisit mengakomodasi karakteristik unik *Deepfake* sebagai teknologi yang menggunakan algoritma machine learning untuk memanipulasi konten digital dengan tingkat realisme yang sangat tinggi. Pasal 35 UU ITE yang mengatur tentang manipulasi informasi elektronik merupakan ketentuan yang paling relevan, namun rumusannya masih bersifat umum dan tidak mencakup aspek-aspek teknis *Deepfake* seperti penggunaan artificial intelligence, tingkat sofistikasi manipulasi, dan dampak psiko-sosial yang ditimbulkan (Akmala, 2019).

Penerapan Pasal 27 ayat (1) UU ITE terhadap kasus *Deepfake* pornografi non-konsensual menghadapi tantangan dalam hal pembuktian unsur "melanggar kesusilaan" ketika konten yang disebarkan bukan merupakan gambar atau video asli korban, melainkan hasil manipulasi digital. Pertanyaan yuridis yang muncul adalah apakah konten *Deepfake* yang menampilkan wajah seseorang dalam situasi seksual dapat dikategorikan sebagai pelanggaran kesusilaan jika tubuh yang ditampilkan bukan milik orang yang wajahnya digunakan. Interpretasi yang sempit dapat menyebabkan lepasnya pelaku dari jeratan hukum, sementara interpretasi yang terlalu luas dapat menimbulkan ketidakadilan bagi pihak-pihak yang sebenarnya tidak bermaksud melakukan kejahatan (Utara & Widyawati, 2025).

Demikian pula dalam penerapan Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik, terdapat kompleksitas dalam membuktikan bahwa konten *Deepfake* telah mencemarkan nama baik seseorang, terutama ketika konten tersebut dibuat dengan tujuan hiburan atau parodi. Batas antara kebebasan berekspresi dan pencemaran nama baik menjadi kabur ketika melibatkan teknologi *Deepfake*, mengingat konten yang dihasilkan dapat ditafsirkan sebagai bentuk satire atau kritik sosial. Hal ini menimbulkan dilema bagi penegak hukum dalam menentukan threshold yang tepat untuk menetapkan kapan suatu konten *Deepfake* dapat dikategorikan sebagai pencemaran nama baik (Jayananda et al., 2021).

Aspek pembuktian dalam kasus kejahatan *Deepfake* menghadapi tantangan teknis yang fundamental. Berbeda dengan manipulasi konten digital konvensional yang relatif mudah dideteksi, *Deepfake* menggunakan teknologi *generative*

adversarial networks (GANs) yang menghasilkan manipulasi dengan tingkat kemiripan yang sangat tinggi dengan konten asli. Proses pembuktian memerlukan analisis forensik digital yang canggih menggunakan algoritma deteksi khusus, yang belum tentu tersedia di semua laboratorium forensik kepolisian. Keterbatasan infrastruktur teknologi ini dapat berdampak pada lemahnya alat bukti yang disajikan di persidangan, sehingga meningkatkan risiko pembebasan terdakwa karena tidak terbukti secara sah dan meyakinkan.

Dari perspektif unsur mens rea atau aspek psikologis pelaku, penerapan hukum pidana terhadap kejahatan *Deepfake* juga menghadapi kompleksitas. Teknologi *Deepfake* memungkinkan pembuatan konten manipulatif tanpa memerlukan keahlian teknis yang tinggi, sehingga banyak pelaku yang mungkin tidak sepenuhnya memahami konsekuensi hukum dari perbuatannya. Dalam konteks ini, perlu dibedakan antara pelaku yang sengaja menggunakan *Deepfake* untuk tujuan kriminal dengan mereka yang membuat konten *Deepfake* untuk tujuan hiburan atau eksperimen teknologi tanpa maksud jahat (Fernandes & Fatma, 2025). Ketiadaan regulasi yang spesifik membuat penegak hukum kesulitan dalam menentukan gradasi sanksi yang proporsional berdasarkan tingkat kesengajaan dan dampak yang ditimbulkan.

Penerapan KUHP terhadap kejahatan *Deepfake* juga menunjukkan keterbatasan yang signifikan. Pasal-pasal dalam KUHP seperti Pasal 310 tentang pencemaran nama baik, Pasal 311 tentang fitnah, Pasal 378 tentang penipuan, dan Pasal 282 tentang kejahatan terhadap kesusilaan dapat diterapkan secara analogis, namun unsur-unsur delik dalam pasal-pasal tersebut tidak dirancang untuk mengakomodasi karakteristik teknologi digital yang canggih. Misalnya, dalam kasus penipuan menggunakan *Deepfake* suara untuk mengecoh korban, pembuktian unsur "tipu muslihat" menjadi kompleks karena teknologi *Deepfake* menciptakan bentuk penipuan yang berbeda dari modus operandi konvensional.

Aspek yurisdiksi dalam kejahatan *Deepfake* menambah kompleksitas penerapan hukum pidana Indonesia. Teknologi *Deepfake* memungkinkan pelaku beroperasi dari luar wilayah Indonesia namun menargetkan korban di dalam negeri, atau sebaliknya. Server yang digunakan untuk menghosting konten *Deepfake* juga dapat berlokasi di berbagai negara, menciptakan tantangan dalam hal kewenangan penyidikan dan penegakan hukum. UU ITE telah mengadopsi prinsip yurisdiksi yang luas melalui Pasal 2, namun implementasinya dalam kasus *Deepfake* lintas batas masih menghadapi kendala teknis dan diplomatik (Cahyono et al., 2025).

Dari segi perlindungan korban, penerapan hukum pidana Indonesia terhadap kejahatan *Deepfake* menunjukkan kelemahan dalam memberikan remedial measures yang memadai. Berbeda dengan kejahatan konvensional yang dampaknya relatif terbatas, korban *Deepfake* mengalami kerugian yang bersifat multidimensional, meliputi kerugian psikologis, reputasi, sosial, dan ekonomi yang dapat berlangsung

dalam jangka panjang. Sistem pemidanaan dalam UU ITE dan KUHP lebih berorientasi pada aspek retributif dan deterrent, namun belum mengakomodasi kebutuhan korban akan pemulihan reputasi dan rehabilitasi psiko-sosial (Luthfi, 2021).

Penerapan hukum pidana terhadap korporasi atau platform digital yang memfasilitasi penyebaran konten *Deepfake* juga menghadapi tantangan yuridis. Meskipun UU ITE telah mengatur tentang tanggung jawab penyelenggara sistem elektronik, namun ketentuan tersebut belum secara spesifik mengatur kewajiban platform untuk mendeteksi dan menghapus konten *Deepfake*. Hal ini menciptakan celah hukum dimana platform dapat berdalih bahwa mereka tidak memiliki kewajiban khusus untuk melakukan moderasi konten *Deepfake*, terutama mengingat kompleksitas teknologi deteksi yang diperlukan (Nurfajri et al., 2025).

Dalam praktik peradilan, hakim juga menghadapi tantangan dalam menentukan sanksi yang proporsional terhadap pelaku kejahatan *Deepfake*. Ketiadaan pedoman pemidanaan yang spesifik untuk kejahatan berbasis AI dapat menyebabkan disparitas putusan antar pengadilan (Amalia & Prasetyo, 2021). Faktor-faktor seperti tingkat sofistikasi teknologi yang digunakan, jumlah korban, tingkat viralisasi konten, dan dampak sosial yang ditimbulkan perlu menjadi pertimbangan dalam penentuan sanksi, namun hal ini belum terintegrasi dalam sistem pemidanaan yang ada.

Berdasarkan analisis tersebut, dapat disimpulkan bahwa penerapan hukum pidana Indonesia terhadap pelaku kejahatan siber berbasis *Deepfake* masih menghadapi berbagai keterbatasan fundamental. Regulasi yang ada belum mampu mengakomodasi karakteristik unik teknologi *Deepfake*, proses pembuktian menghadapi kendala teknis yang signifikan, dan sistem pemidanaan belum memberikan perlindungan optimal bagi korban. Kondisi ini menunjukkan perlunya rekonstruksi hukum pidana yang lebih komprehensif dan adaptif terhadap perkembangan teknologi artificial intelligence, khususnya dalam konteks kejahatan siber yang semakin canggih dan merugikan Masyarakat (Septiawan et al., 2025).

2. Kendala Substansi Hukum Dalam Penegakan Hukum Pidana Terhadap Pelaku Kejahatan Siber Berbasis *Deepfake*

Kendala substansi hukum dalam penegakan hukum pidana terhadap pelaku kejahatan siber berbasis *Deepfake* mencerminkan ketidaksesuaian antara karakteristik teknologi artificial intelligence yang berkembang pesat dengan kerangka normatif hukum pidana Indonesia yang masih bersifat konvensional. Substansi hukum pidana Indonesia, yang terkodifikasi dalam KUHP dan UU ITE, dirumuskan dalam paradigma kejahatan tradisional yang belum mengantisipasi kompleksitas teknologi *Deepfake* sebagai instrumen kejahatan siber generasi baru. Ketidaksesuaian ini menciptakan gap substantif yang fundamental, dimana norma-norma hukum yang ada tidak mampu menangkap esensi kejahatan *Deepfake* secara

utuh, mulai dari aspek definisi, unsur-unsur delik, hingga mekanisme pertanggungjawaban pidana yang sesuai dengan karakteristik teknologi tersebut.

Kendala substansi hukum yang paling mendasar terletak pada ketiadaan definisi yuridis yang komprehensif mengenai *Deepfake* dalam peraturan perundang-undangan Indonesia. UU ITE hanya mendefinisikan "informasi elektronik" dan "dokumen elektronik" secara umum, tanpa membedakan antara konten digital asli dengan konten yang dihasilkan melalui teknologi artificial intelligence. Ketiadaan definisi khusus ini menciptakan ambiguitas dalam penerapan hukum, dimana penegak hukum harus melakukan interpretasi subjektif terhadap apa yang dimaksud dengan *Deepfake* dan bagaimana membedakannya dengan bentuk manipulasi digital lainnya (Noerman & Ibrahim, 2024). Ambiguitas definitional ini berimplikasi pada kesulitan dalam membuktikan unsur-unsur delik, mengingat tanpa definisi yang jelas, sulit untuk menetapkan threshold yang tepat untuk menentukan kapan suatu konten dapat dikategorikan sebagai *Deepfake* yang berpotensi kriminal.

Substansi hukum pidana Indonesia juga menghadapi kendala dalam hal perumusan unsur-unsur delik yang sesuai dengan modus operandi kejahatan *Deepfake*. Unsur-unsur delik dalam UU ITE seperti "mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan" sebagaimana diatur dalam Pasal 30 sampai dengan Pasal 37, tidak secara spesifik mengakomodasi proses pembuatan *Deepfake* yang melibatkan algoritma machine learning kompleks (Antonio & Adhari, 2024). Proses *Deepfake* tidak sekedar "mengubah" konten eksisting, melainkan "menciptakan" konten baru berdasarkan pembelajaran algoritma terhadap data training, sehingga kategorisasi yuridisnya menjadi tidak tepat jika hanya menggunakan unsur delik konvensional. Hal ini menciptakan celah hukum dimana pelaku dapat berargumen bahwa mereka tidak melakukan "perubahan" terhadap konten asli, melainkan menciptakan konten baru yang hanya mengambil referensi visual atau audio dari seseorang.

Kendala substansi hukum juga termanifestasi dalam aspek pertanggungjawaban pidana yang belum mengakomodasi karakteristik unik teknologi *Deepfake*. Dalam kejahatan *Deepfake*, terdapat multiple actors yang terlibat, mulai dari pengembang algoritma, penyedia platform, pengguna yang membuat konten, hingga pihak yang menyebarkan konten tersebut. Substansi hukum pidana Indonesia belum mengatur secara jelas bagaimana pembagian pertanggungjawaban pidana di antara para pihak tersebut, terutama dalam konteks chain of causation yang kompleks dalam teknologi AI. Misalnya, apakah pengembang algoritma *Deepfake* dapat dimintai pertanggungjawaban pidana jika teknologi yang dikembangkannya digunakan untuk tujuan kriminal, atau apakah tanggung jawab hanya terbatas pada end-user yang secara langsung menggunakan teknologi tersebut untuk melakukan kejahatan (Raharjo et al., 2025).

Aspek temporalitas dalam substansi hukum pidana juga menjadi kendala signifikan dalam penanganan kejahatan *Deepfake*. Ketentuan mengenai kapan suatu perbuatan dianggap selesai dilakukan (*vollendingdelict*) menjadi problematis dalam konteks *Deepfake* yang prosesnya melibatkan tahapan pembuatan, rendering, uploading, dan penyebaran melalui platform digital. Berbeda dengan kejahatan konvensional yang memiliki moment of completion yang jelas, kejahatan *Deepfake* memiliki kontinuitas temporal yang dapat berlangsung selama konten tersebut masih dapat diakses dan disebarkan melalui internet (Putri et al., 2024). Ketidakjelasan aspek temporalitas ini berimplikasi pada penentuan yurisdiksi, perhitungan masa daluwarsa, dan penetapan sanksi yang proporsional.

Kendala substansi hukum dalam hal gradasi sanksi juga menjadi permasalahan mendasar. Struktur pemidanaan dalam UU ITE tidak membedakan tingkat keseriusan kejahatan berdasarkan sofistikasi teknologi yang digunakan, jumlah korban, tingkat viralisasi konten, atau dampak sosial yang ditimbulkan. Sanksi pidana untuk manipulasi informasi elektronik diatur secara uniform tanpa mempertimbangkan bahwa *Deepfake* memiliki tingkat kompleksitas dan dampak yang berbeda dengan manipulasi digital konvensional (Maizuly et al., 2022). Hal ini dapat menghasilkan ketidakadilan dalam pemidanaan, dimana pelaku yang menggunakan teknologi *Deepfake* canggih untuk menimbulkan kerugian massal mendapat sanksi yang sama dengan pelaku yang melakukan manipulasi digital sederhana dengan dampak terbatas.

Substansi hukum pidana Indonesia juga belum mengakomodasi aspek preventif yang diperlukan dalam penanganan kejahatan *Deepfake*. Ketentuan yang ada lebih bersifat represif-kuratif, fokus pada penghukuman setelah kejahatan terjadi, namun tidak menyediakan mekanisme pencegahan yang efektif. Dalam konteks *Deepfake*, aspek preventif menjadi sangat penting mengingat damage yang ditimbulkan oleh konten *Deepfake* dapat bersifat irreversible, terutama dalam hal kerusakan reputasi dan trauma psikologis korban. Ketiadaan substansi hukum yang mengatur kewajiban preventif bagi platform digital, pengembang teknologi, dan stakeholder lainnya menciptakan vacum dalam upaya pencegahan kejahatan *Deepfake* (Kristiyenda et al., 2025).

Kendala substansi hukum juga termanifestasi dalam aspek pemulihan hak korban (*victim remediation*) yang belum memadai. Substansi hukum pidana Indonesia masih terfokus pada aspek punishment terhadap pelaku, namun belum menyediakan mekanisme comprehensive untuk pemulihan korban kejahatan *Deepfake*. Berbeda dengan korban kejahatan konvensional yang kerugiannya dapat dikuantifikasi dan dipulihkan melalui restitusi material, korban *Deepfake* mengalami kerugian immaterial yang kompleks, meliputi kerusakan reputasi, trauma psikologis, dan disruption sosial yang sulit dipulihkan melalui mekanisme konvensional. Ketiadaan substansi hukum yang mengatur right to be forgotten, right to correction,

dan mekanisme rehabilitasi reputasi menciptakan ketidakadilan bagi korban yang dampak viktimisasinya dapat berlangsung seumur hidup (Mutmainnah et al., 2024).

Aspek korporasi dan tanggung jawab platform digital juga menghadapi kendala substansi hukum yang signifikan. Meskipun UU ITE telah mengatur mengenai tanggung jawab penyelenggara sistem elektronik, namun substansi pengaturannya belum spesifik mengakomodasi karakteristik platform yang memfasilitasi teknologi *Deepfake*. Ketentuan mengenai kewajiban take-down, content moderation, dan user verification belum disesuaikan dengan kompleksitas deteksi *Deepfake* yang memerlukan teknologi khusus dan expertise yang tinggi. Hal ini menciptakan ketidakpastian hukum bagi platform digital mengenai standard of care yang harus dipenuhi dalam mencegah penyalahgunaan teknologi *Deepfake* di platform mereka.

Kendala substansi hukum dalam aspek lintas batas (transnational) juga menjadi permasalahan krusial. Substansi UU ITE belum mengatur secara komprehensif mekanisme kerjasama internasional dalam penanganan kejahatan *Deepfake* yang bersifat lintas negara. Ketentuan mengenai mutual legal assistance, extradition, dan digital evidence sharing masih bersifat umum dan belum disesuaikan dengan karakteristik khusus kejahatan *Deepfake* yang melibatkan transfer data digital, cloud computing, dan teknologi AI yang dapat dioperasikan dari multiple jurisdictions. Keterbatasan substansi hukum ini berdampak pada kesulitan penegakan hukum terhadap pelaku yang beroperasi dari luar negeri atau menggunakan infrastruktur teknologi yang tersebar di berbagai negara.

Dari perspektif constitutional law, substansi hukum pidana untuk kejahatan *Deepfake* juga menghadapi tension antara law enforcement needs dengan fundamental rights protection. Ketentuan yang terlalu luas dalam mendefinisikan *Deepfake* crime dapat berpotensi melanggar *freedom of expression, right to privacy*, dan *academic freedom*, terutama dalam konteks penggunaan *Deepfake* untuk tujuan legitimate seperti penelitian, pendidikan, atau artistic expression (Azka et al., 2025). Sebaliknya, ketentuan yang terlalu sempit dapat menciptakan loopholes yang dapat dieksploitasi oleh pelaku kejahatan. Substansi hukum pidana Indonesia belum menyediakan balancing mechanism yang tepat untuk mengatasi tension tersebut.

Kendala substansi hukum dalam hal evidentiary rules juga menjadi permasalahan fundamental. Ketentuan mengenai alat bukti dalam hukum acara pidana Indonesia belum secara spesifik mengakomodasi karakteristik digital evidence dalam kasus *Deepfake* yang memerlukan expert testimony, algorithm audit, dan technical analysis yang canggih. Substansi hukum belum mengatur standard untuk validasi alat bukti digital dalam kasus *Deepfake*, authentication procedures untuk AI-generated content, dan admissibility criteria untuk expert testimony mengenai *Deepfake* detection. Ketiadaan substansi hukum yang jelas dalam aspek evidentiary ini dapat mengakibatkan pembebasan terdakwa meskipun secara faktual telah melakukan kejahatan *Deepfake*.

Berdasarkan analisis komprehensif tersebut, dapat disimpulkan bahwa kendala substansi hukum dalam penegakan hukum pidana terhadap pelaku kejahatan siber berbasis *Deepfake* bersifat multidimensional dan fundamental. Kendala-kendala tersebut tidak hanya terbatas pada aspek teknis perumusan norma, melainkan mencakup philosophical foundations dari hukum pidana Indonesia yang belum sepenuhnya adaptif terhadap era artificial intelligence (Dinda, 2024). Rekonstruksi substansi hukum yang komprehensif menjadi kebutuhan mendesak untuk memastikan efektivitas penegakan hukum pidana di era digital yang semakin canggih.

D. SIMPULAN

Penerapan hukum pidana Indonesia terhadap kejahatan siber berbasis *Deepfake* masih menghadapi keterbatasan mendasar karena UU ITE dan KUHP tidak secara eksplisit mengatur karakteristik teknologi ini, sehingga penanganannya bergantung pada interpretasi analogis pasal-pasal yang ada dan menimbulkan ketidakpastian hukum. Tantangan utama meliputi kesulitan pembuktian forensik digital, penentuan yurisdiksi lintas batas, keterbatasan pemahaman aparat terhadap AI, serta ketidaksesuaian sanksi dengan dampak jangka panjang yang ditimbulkan. Selain itu, ketiadaan definisi legal mengenai *Deepfake* menciptakan kekosongan hukum, rumusan delik konvensional tidak mampu menangkap esensi "realitas sintetis", unsur kesengajaan menjadi lebih kompleks karena kemudahan akses teknologi, dan prosedur pembuktian belum memadai. Kondisi ini menunjukkan perlunya reformulasi substansial hukum pidana, baik materiil maupun formil, agar mampu merespons secara efektif, proporsional, dan pasti terhadap ancaman kejahatan *Deepfake* yang terus berkembang.

E. DAFTAR RUJUKAN

Akmala, S. (2019). Perkembangan Internet Pada Generasi Muda Di Indonesia Dengan Kaitan Undang-Undang Ite Yang Berlaku. *Cyber Security Dan Forensik Digital*, *1*(2), 45–49. https://doi.org/10.14421/csecurity.2018.1.2.1371

Amalia, D. A. R., & Prasetyo, M. H. (2021). Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism. *Jurnal Pembangunan Hukum Indonesia*, *3*(2), 228–239. https://doi.org/10.14710/jphi.v3i2.228-239

Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, *9*(2). https://doi.org/10.53429/iljs.v9i2.858

Antonio, A., & Adhari, A. (2024). Menilai Implementasi Undang Undang ITE dalam Menegakkan Kepastian Hukum Terhadap Kasus Pencemaran Nama Baik. *Ranah Research : Journal of Multidisciplinary Research and Development*, *6*(4), 1079–1087. https://doi.org/10.38035/rrj.v6i4.979

Azka, M. D. A., Aulia, N. F., Ananda, F., & Putra, P. (2025). Pengaruh *Deepfake*

terhadap Kepercayaan Publik pada Informasi Visual di Media Sosial. *Kajian Administrasi Publik Dan Ilmu Komunikasi*, *2*(2), 286–301. https://doi.org/10.62383/kajian.v2i2.401

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 1–23. https://doi.org/10.64344/djl.v1i1.6

Chandra, J., Tanaka, V., & Banke, R. (2025). Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia. *Peshum : Jurnal Pendidikan, Sosial Dan Humaniora*, *4*(3), 4710–4719. https://doi.org/10.56799/peshum.v4i3.9028

Dinda, A. L. S. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, Dan Hukum*, *2*(2), 69–77. https://doi.org/10.58707/aldalil.v2i2.777

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital*, *1*(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

Fernandes, Y. A., & Fatma, Y. (2025). Metode Deep Learning Dalam Teknologi *Deepfake*: Systematic Literature Review. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 3403–3410. https://doi.org/10.36040/jati.v9i2.12987

Harun, F. A., & Nurhadiyanto, L. (2024). Rekayasa Konten Pornografi Berbasis AI Image Generator dalam Perspektif Space Transition Theory. *Ranah Research : Journal of Multidisciplinary Research and Development*, *6*(3), 408–418. https://doi.org/10.38035/rrj.v6i3.826

Jayananda, I. M. V., Sugiartha, I. N. G., & Widiantara, M. M. (2021). Analisis Tentang Pencemaran Nama Baik dan Penyalahgunaan Hak Kebebasan Berpendapat di Media Sosial. *Jurnal Analogi Hukum*, *3*(2), 261–265. https://doi.org/10.22225/ah.3.2.2021.261-265

Kristiyenda, Y. S., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan *Deepfake*: Studi Kasus terhadap Modus Penipuan *Deepfake* Prabowo Subianto dalam Tawaran Bantuan Uang. *Al Adalah: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *3*(2), 149–164. https://doi.org/10.59246/aladalah.v3i2.1263

Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: *Deepfake* Pornografi dan Pencurian Data Pribadi. *Zenodo*. https://doi.org/10.5281/ZENODO.11448814

Luthfi, H. (2021). Penerapan Asas Ultimum Remidium Dalam Penegakan Hukum Tindak Pidana Undang-Undang Informasi Dan Transaksi Elektronik. *Yurispruden*, *4*(1), 29. https://doi.org/10.33474/yur.v4i1.9164

Maizuly, A. R., Hartono, B., & Satria, I. (2022). Penerapan Sanksi Pidana Terhadap Pelaku Tindak Pidana Manipulasi dan Penciptaan melalui Akun Media Sosial Facebook. *Ius Civile: Refleksi Penegakan Hukum Dan Keadilan*, *6*(1), 12. https://doi.org/10.35308/jic.v6i1.3794

Marzuki, P. M. (2016). *Penelitian Hukum*. Jakarta: Prenada Media.

Meliana, Y. (2025). Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana *Deepfake* dalam Sistem Hukum Pidana Nasional. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.1087

Moleong, L. J. (2018). *Metode Penelitian Kualitatif*. Bandung: PT Remaja Rosdakarya.

Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi *Deepfake* sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. *Upgrade : Jurnal Pendidikan Teknologi Informasi*, *1*(2), 67–72. https://doi.org/10.30812/upgrade.v1i2.3702

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara. *Jurnal USM Law Review*, *7*(2), 603–621. https://doi.org/10.26623/julr.v7i2.8995

Novera, O., & Fitri, Z. Y. (2024). Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (*Deepfake*) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial. *El-Faqih : Jurnal Pemikiran Dan Hukum Islam*, *10*(2), 460–474. https://doi.org/10.58401/faqih.v10i2.1539

Nurfajri, I., Pratama, E. T. H., Tupamahu, G. S., Saputra, R., & Erwina, Y. (2025). Dampak Algoritma AI terhadap Komunikasi Publik: Memahami Manipulasi Informasi dan Realitas. *Converse Journal Communication Science*, *1*(3), 13. https://doi.org/10.47134/converse.v1i3.3543

Prayuti, Y. (2024). Dinamika Perlindungan Hukum Konsumen di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce dan Perlindungan Data Konsumen di Indonesia. *Jurnal Interpretasi Hukum*, *5*(1), 903–913. https://doi.org/10.22225/juinhum.5.1.8482.903-913

Putri, S. M. I., Salsabila, N., & Hosnah, A. U. (2024). Kriminalisasi Penggunaan *Deepfake* dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum. *Jurnal Hukum Legalita*, *6*(2), 83–90. https://doi.org/10.47637/legalita.v6i2.1453

Raharjo, T., Irfan Adristi, F., Romadhona, F. Y., Syahputra, R. R., Halim, M. Y., Rachman, M. A., Marjianto, R. N., Santicho, D., Kusuma, P., & Ramadhani, E. (2025). Analisis Forensik *Deepfake* Berbasis Convolutional Neural Network (CNN) Untuk Deteksi Inkonsistensi Tekstur Dan Pola Pada Citra Wajah. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 2731–2738. https://doi.org/10.36040/jati.v9i2.13058

Septiawan, R., Anandatia, V., & Gustina, A. (2025). Pemanfaatan Artificial Intelligence dalam Hukum Acara Pidana: Tinjauan Yuridis dan Dampak Sosial. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *2*(4), 640–654. https://doi.org/10.51903/perkara.v2i4.2235

Soekanto, S., & Mamuji, S. (2013). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada.

Sujamawardi, L. H. (2018). Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor

19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*, *9*(2). https://doi.org/10.28932/di.v9i2.974

Utara, E. R., & Widyawati, A. (2025). Analysis of Criminal Law Enforcement on Non-Consensual *Deepfake* Pornography in the Dissemination of Manipulative Content in Indonesia: Analisis Penegakan Hukum Pidana *Deepfake* Pornografi Non-Konsensual dalam Penyebaran Konten Manipulatif di Indonesia. *Al-Jinayah : Jurnal Hukum Pidana Islam*, *11*(1), 125–153. https://doi.org/10.15642/aj.2025.11.1.125-153