INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 4 Tahun 2025 Page 386-398
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran *Deepfake* di Media Sosial

Desty Aster Yansen Basah[1]✉, Andika Wijaya[2], Ivans Januardy[3]
Universitas Palangka Raya
Email: destyaster20@gmail.com[1]✉

Abstrak

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/AI) telah melahirkan tantangan baru dalam ranah hukum pidana, salah satunya melalui fenomena *deepfake*. Teknologi ini memungkinkan penciptaan konten visual dan audio yang menyerupai kenyataan, namun bersifat manipulatif dan berpotensi menimbulkan kerugian serius, baik terhadap individu maupun terhadap tatanan hukum. Penelitian ini bertujuan untuk menganalisis urgensi pengaturan hukum pidana terhadap penyebaran konten *deepfake* di Indonesia. Metode yang digunakan adalah pendekatan yuridis normatif dengan analisis terhadap peraturan perundang-undangan, doktrin, dan putusan hukum yang relevan, serta ditunjang dengan studi komparatif dari regulasi internasional. Hasil penelitian menunjukkan bahwa sistem hukum Indonesia saat ini belum memiliki aturan eksplisit mengenai *deepfake*, sehingga menyebabkan kekosongan hukum (*legal vacuum*) yang berdampak pada kesulitan pembuktian dan lemahnya perlindungan terhadap korban. Beberapa ketentuan dalam KUHP dan UU ITE masih bersifat umum dan tidak mengakomodasi kompleksitas karakteristik *deepfake*. Oleh karena itu, diperlukan reformulasi hukum dalam bentuk undang-undang khusus atau amandemen terhadap regulasi yang ada guna mengklasifikasikan kejahatan *deepfake* sebagai tindak pidana tersendiri. Negara juga perlu memperkuat kapasitas penegak hukum serta mendorong kolaborasi lintas sektor dalam merespons tantangan teknologi manipulatif yang semakin masif di era digital.

Kata Kunci: *Deepfake, Hukum Pidana, Kecerdasan Buatan, UU ITE, KUHP, Kriminalisasi*.

Abstract

The advancement of Artificial Intelligence (AI) technology has posed new challenges to criminal law, particularly through the emergence of deepfake phenomena. Deepfake allows for the creation of visual and audio content that mimics reality but is in fact manipulated, potentially causing significant harm to individuals and the legal system. This study aims to analyze the urgency of criminal law regulation concerning the dissemination of deepfake content in Indonesia. A normative juridical method is applied, focusing on statutory analysis, doctrinal interpretation, and relevant jurisprudence, supported by comparative studies from international legal frameworks. The findings reveal that Indonesia's current legal system lacks explicit provisions governing deepfake, resulting in a legal vacuum that complicates evidentiary procedures and weakens victim protection. Existing provisions in the Indonesian Penal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) are still general and fail to accommodate the complexity of deepfake crimes. Therefore, legal reform is needed through a specific law or amendment to existing regulations to classify deepfake as a distinct criminal offense. The state must also enhance the capacity of law enforcement and encourage cross-sector collaboration in addressing the growing threat of manipulative technologies in the digital age.

Keywords: *Deepfake, Criminal Law, Artificial Intelligence, Electronic Information Law, Indonesian Penal Code, Criminalization*.

PENDAHULUAN

Kemajuan teknologi informasi telah memengaruhi hampir seluruh aspek kehidupan, termasuk dalam ranah hukum pidana. Salah satu bentuk kemajuan teknologi yang menimbulkan tantangan hukum tersendiri adalah *deepfake*. Teknologi ini berbasis kecerdasan buatan (*Artificial Intelligence*) yang memungkinkan manipulasi konten visual maupun audio dengan hasil yang sangat realistis, sehingga sulit dibedakan dengan konten asli. Keberadaan *deepfake* telah menciptakan kekhawatiran global karena potensinya untuk digunakan dalam kejahatan digital seperti penipuan, pencemaran nama baik, penyebaran pornografi, hingga manipulasi politik (Salvi, 2023).Fenomena *deepfake* telah menjadi instrumen baru dalam disinformasi digital. Penyebarannya kian meningkat di media sosial karena akses teknologi yang semakin mudah. Di Indonesia, penggunaan *deepfake* belum diatur secara eksplisit dalam undang-undang, meskipun praktiknya sudah nyata merugikan banyak pihak, baik individu maupun institusi. Regulasi hukum yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS), serta KUHP baru (Undang-Undang Nomor 1 Tahun 2023), belum secara spesifik mengatur tindak pidana berbasis konten manipulatif semacam ini (Novyanti & Astuti, 2021).

Dalam perspektif hukum pidana, keberadaan konten *deepfake* menimbulkan

tantangan pembuktian yang serius. Penyidik dan aparat penegak hukum harus dapat membuktikan keaslian konten dan niat pelaku dalam konteks hukum pidana. Namun demikian, instrumen hukum yang tersedia belum cukup akomodatif. Sementara *deepfake* dapat digunakan untuk menjatuhkan reputasi seseorang, misalnya melalui konten pornografi nonkonsensual atau fitnah politik, hukum yang berlaku masih menggunakan pasal-pasal umum seperti pencemaran nama baik atau pelanggaran kesusilaan yang cenderung multitafsir dan lemah dalam penerapan teknis (Prayoga & Tuasikal, 2025). Upaya kriminalisasi terhadap penyebaran konten *deepfake* sangat penting untuk mencegah berkembangnya kejahatan digital yang berbasis manipulasi visual. Dalam studi yang dilakukan oleh Delfino (2022), disebutkan bahwa sistem hukum pidana harus mampu mengembangkan peran hakim dalam mengidentifikasi dan mengevaluasi bukti digital manipulatif agar proses peradilan tidak dikompromikan. Pendekatan normatif dalam sistem hukum Indonesia saat ini belum memadai untuk menjawab tantangan tersebut.

Seiring perkembangan teknologi, muncul kebutuhan akan reformulasi hukum pidana yang mampu mengantisipasi kejahatan-kejahatan berbasis kecerdasan buatan. Jika tidak diantisipasi sejak awal, maka akan terjadi kekosongan hukum (*legal vacuum*) yang berisiko pada impunitas pelaku. Di Indonesia, aparat penegak hukum menghadapi kesulitan dalam mengklasifikasikan tindak pidana berbasis *deepfake*, sehingga sering kali perkara tersebut ditangani dengan pendekatan administratif atau perdata, bukan pidana (Putri et al., 2024).

Pentingnya reformulasi ini juga diperkuat oleh hasil kajian di jurnal *Crime Science* (Sandoval et al., 2024) yang mengidentifikasi bahwa ancaman terbesar *deepfake* bukan hanya pada individu, tetapi juga terhadap sistem peradilan pidana secara keseluruhan. Oleh karena itu, diperlukan penguatan pada aspek pembuktian dan legislasi yang secara khusus mengatur jenis kejahatan berbasis AI.

Dalam konteks Indonesia, UU ITE dan KUHP baru memang sudah mengalami sejumlah pembaruan, namun belum ada pasal yang secara eksplisit mengatur atau menyebutkan *deepfake* sebagai bentuk tindak pidana. KUHP baru yang disahkan pada 2023 masih bersifat general dan belum menyesuaikan dengan dinamika ancaman digital seperti *deepfake* (Syahirah & Prasetyo, 2025). Padahal, sifat destruktif *deepfake* terhadap reputasi dan kehormatan seseorang sangat besar, bahkan dapat menyebabkan tekanan psikis yang berujung pada gangguan mental berat. Bahkan dalam konteks internasional, berbagai negara telah mulai merespons bahaya *deepfake* dengan kebijakan pidana progresif. Beberapa negara bagian di Amerika Serikat telah mengkriminalisasi penyebaran *deepfake* yang bersifat politis atau seksual. Hal ini menunjukkan bahwa terdapat kebutuhan mendesak akan penyesuaian hukum pidana nasional terhadap ancaman yang bersifat transnasional

dan berbasis teknologi tinggi (Salvi, 2023).

Ketiadaan norma hukum yang eksplisit dan kekhususan jenis kejahatan ini membuat penegakan hukum di Indonesia cenderung berjalan lambat. Studi oleh Heny & Puji (Novyanti & Astuti, 2021) menunjukkan bahwa aparat penegak hukum masih gamang dalam menentukan pasal yang tepat untuk menjerat pelaku penyebaran *deepfake*. Hal ini menyebabkan banyak kasus tidak sampai pada tahap peradilan atau dihentikan di tahap penyelidikan karena kesulitan pembuktian. Dalam perspektif pertanggungjawaban pidana, penyebaran *deepfake* mengandung unsur kesengajaan dan niat jahat (*mens rea*) apabila dilakukan untuk mencemarkan nama baik, menyebarkan pornografi, atau menipu orang lain. Oleh karena itu, hukum pidana memiliki posisi strategis untuk menegakkan keadilan dan memberikan efek jera terhadap pelaku (Amelia et al., 2024). Penelitian yang dipublikasikan jurnal GLS Kalp ((Kothari & Tibrewala, 2024)) juga menggarisbawahi bahwa *deepfake* telah menjadi trojan horse dalam sistem keadilan pidana, karena ia mampu merusak integritas bukti dan memengaruhi persepsi publik secara masif. Hal ini berdampak serius terhadap kepercayaan publik terhadap institusi hukum dan pengadilan.

Sebagai respons terhadap tantangan tersebut, maka dibutuhkan pengaturan khusus dalam hukum pidana Indonesia yang tidak hanya bersifat reaktif tetapi juga preventif. Hal ini dapat dilakukan melalui amandemen undang-undang yang ada atau pembentukan undang-undang khusus yang mengatur kejahatan berbasis teknologi manipulatif seperti *deepfake*. Selain itu, perlu penguatan dari sisi teknologi forensik digital yang dapat mendeteksi konten *deepfake* dengan akurasi tinggi. Ketiadaan alat pembuktian yang memadai menyebabkan korban berada dalam posisi lemah dan aparat hukum cenderung mengabaikan kasus semacam ini karena proses pembuktian yang rumit dan mahal (Sandoval et al., 2024).

Kondisi tersebut menunjukkan bahwa *deepfake* bukan sekadar tantangan teknologi, melainkan juga ancaman terhadap struktur hukum dan perlindungan hak asasi manusia. Negara berkewajiban untuk menghadirkan perlindungan hukum yang memadai guna memastikan bahwa kejahatan digital tidak berkembang di luar kendali hukum..

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yakni suatu metode penelitian hukum yang bertumpu pada studi pustaka terhadap bahan-bahan hukum tertulis yang menjadi dasar dalam menganalisis persoalan hukum yang diangkat. Metode ini sering digunakan dalam kajian-kajian hukum positif, di mana permasalahan dikaji dengan menganalisis peraturan perundang-undangan yang relevan, doktrin, asas hukum, dan

yurisprudensi (Soekanto & Mamudji, 2015).

Pendekatan yuridis normatif dianggap tepat karena isu yang dikaji berkenaan dengan kriminalisasi penyebaran konten *deepfake* dalam kerangka hukum pidana nasional, khususnya dalam kaitannya dengan efektivitas peraturan perundang-undangan yang berlaku, seperti KUHP baru (UU No. 1 Tahun 2023), UU ITE, dan UU TPKS. Penelitian ini bertujuan untuk menelaah apakah hukum pidana positif Indonesia telah cukup memadai untuk menanggulangi kejahatan digital berbasis manipulasi konten seperti *deepfake*.

Bahan hukum Primer yang digunakan adalah Kitab Undang-Undang Hukum Pidana (KUHP) terbaru (UU No. 1 Tahun 2023), Undang-Undang Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016), Undang-Undang Tindak Pidana Kekerasan Seksual (UU No. 12 Tahun 2022), dan yurisprudensi yang terkait dengan tindak pidana digital. Bahan hukum sekunder, berupa hasil penelitian terdahulu dari jurnal hukum nasional dan internasional yang relevan, pendapat para pakar hukum pidana, buku teks hukum, serta hasil seminar atau diskusi akademik terkait regulasi *deepfake* dan kejahatan siber dan bahan hukum tersier, yaitu kamus hukum, ensiklopedia hukum, dan indeks hukum yang digunakan sebagai penunjang dan klarifikasi terhadap konsep-konsep tertentu yang digunakan dalam analisis.

Analisis data dilakukan secara deskriptif-analitis, yakni dengan menggambarkan peraturan hukum yang ada dan menganalisisnya secara kritis dalam konteks penyebaran konten *deepfake* di Indonesia. Data yang diperoleh disusun, diklasifikasikan, dan kemudian dianalisis secara sistematis untuk menjawab rumusan masalah dalam tulisan ini. Analisis tersebut bertujuan menemukan kekosongan hukum, disharmoni norma, atau ketidaksesuaian antara norma dengan perkembangan teknologi informasi (Firmanto et al., 2024).

Dalam konteks metodologi hukum, penelitian ini juga menggunakan pendekatan konseptual (conceptual approach) untuk memahami definisi, ruang lingkup, dan implikasi hukum dari *deepfake* dalam sistem hukum pidana. Pendekatan ini penting karena belum terdapat pengaturan eksplisit mengenai *deepfake* dalam hukum positif Indonesia, sehingga perlu dianalisis berdasarkan asas-asas hukum dan teori-teori hukum pidana modern (McCrudden, 2017).

Secara metodologis, penelitian ini bertumpu pada paradigma doktrinal dalam hukum, yang menempatkan hukum sebagai sistem normatif. Paradigma ini memungkinkan peneliti untuk menguji konsistensi norma, prinsip, dan logika hukum dalam menghadapi fenomena baru seperti kejahatan digital. Sebagaimana ditegaskan oleh Nasir dkk. (2023), penelitian hukum doktrinal bertujuan untuk menganalisis hubungan internal antara norma hukum dan

penggunaannya dalam praktik peradilan

HASIL DAN PEMBAHASAN

Konsep dan Karakteristik *Deepfake* dalam Perspektif Hukum Pidana

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/AI) telah menciptakan dimensi baru dalam dunia digital, salah satunya melalui kemunculan teknologi *deepfake*. *Deepfake* memungkinkan penciptaan konten audio-visual yang sangat menyerupai kenyataan, padahal secara faktual adalah rekayasa. Teknologi ini bekerja dengan memanfaatkan algoritma pembelajaran mendalam, khususnya Generative Adversarial Networks (GANs), yang mampu menyintesis gambar, suara, hingga ekspresi seseorang ke dalam format video maupun audio secara hampir sempurna (Masood et al., 2023).

Secara etimologis, istilah "*deepfake*" berasal dari gabungan kata deep learning dan fake, yang merujuk pada teknik pembelajaran mendalam untuk menciptakan konten palsu secara otomatis. Teknologi ini pertama kali mencuat ke permukaan publik pada tahun 2017 melalui platform Reddit, di mana pengguna mengunggah video manipulatif yang kemudian viral. Dalam waktu singkat, fenomena ini menyebar ke berbagai bidang: dari industri hiburan, media sosial, sampai ke area kejahatan digital seperti penipuan, eksploitasi seksual, dan pencemaran nama baik (Korshunov & Marcel, 2018). Ciri utama *deepfake* yang membuatnya problematik dalam konteks hukum adalah kemampuannya untuk menghasilkan konten yang sangat meyakinkan. Penelitian oleh Tolosana dkk. (2020) mengungkap bahwa konten *deepfake* seringkali sulit dibedakan dari aslinya, baik oleh publik awam maupun oleh sistem keamanan berbasis biometrik. Hal ini menimbulkan ancaman terhadap keandalan bukti visual dalam sistem peradilan pidana serta memunculkan potensi gangguan sosial seperti penyebaran hoaks atau fitnah secara masif.

Di Indonesia, fenomena ini belum memiliki pengaturan hukum yang bersifat spesifik. Meskipun berbagai ketentuan hukum dapat digunakan sebagai dasar penindakan, belum ada satu pun norma hukum yang secara eksplisit menyebutkan atau mendefinisikan *deepfake* sebagai bentuk kejahatan tertentu. Penelitian yang dilakukan oleh Heny & Pudji (Novyanti & Astuti, 2021) menyatakan bahwa penyalahgunaan *deepfake* dapat dikenakan sanksi pidana apabila memenuhi unsur pencemaran nama baik atau penyebaran berita bohong sebagaimana diatur dalam UU ITE. Namun, absennya definisi dan karakter hukum yang tegas menyebabkan interpretasi hukum bersifat lentur dan berpotensi menimbulkan ketidakpastian. Hal senada dikemukakan oleh Yolanda dkk. (Amelia et al., 2024), yang melalui pendekatan yuridis normatif menunjukkan bahwa pertanggungjawaban pidana

terhadap pelaku *deepfake* tidak dapat ditegakkan secara optimal apabila hanya berlandaskan pada pasal-pasal umum dalam KUHP atau UU ITE. Penelitian tersebut menyoroti kekosongan hukum yang nyata dalam struktur hukum pidana Indonesia, serta merekomendasikan agar kejahatan *deepfake* diklasifikasikan sebagai tindak pidana khusus yang memiliki karakter delik aduan dan unsur teknis yang spesifik.

Lebih jauh, dari perspektif hukum internasional, penelitian oleh Dalila dkk. (Durães et al., 2023) menyoroti urgensi sistem peradilan pidana untuk mengantisipasi penggunaan bukti *deepfake* dalam proses litigasi. Tantangan terbesar terletak pada pembuktian keaslian bukti digital, yang jika tidak didukung oleh perangkat deteksi yang memadai, dapat merusak integritas proses hukum. Penelitian ini merekomendasikan pembentukan regulasi prosedural baru untuk menangani bukti berbasis konten manipulatif. Sementara itu, Masood (Masood et al., 2023) dalam studi mereka tentang taksonomi teknologi *deepfake*, menekankan bahwa keberhasilan mendeteksi dan menindak *deepfake* tidak hanya bergantung pada regulasi, tetapi juga kesiapan infrastruktur teknologi, seperti perangkat lunak forensik digital dan sistem pelacakan metadata. Tanpa kolaborasi antara regulator, penyidik, dan teknologi, upaya penindakan akan selalu tertinggal dari inovasi pelaku.

Pavel & Sebastian (Korshunov & Marcel, 2018) menambahkan bahwa kerentanan sistem pengenalan wajah (facial recognition system) terhadap *deepfake* semakin memperparah risiko dalam penegakan hukum berbasis teknologi. Sistem biometrik yang selama ini menjadi alat validasi identitas justru dapat dimanipulasi, sehingga menyebabkan error dalam deteksi kejahatan atau bahkan kriminalisasi terhadap pihak yang tidak bersalah.

Dalam konteks Indonesia, Sarah & Diana (Sijabat & Lukitasari, 2024) menganalisis fenomena konten *deepfake* dalam bentuk pornografi digital, yang ternyata tidak mudah dijerat dengan pasal-pasal dalam UU Pornografi maupun KUHP karena tidak memenuhi unsur "perbuatan fisik" dari pelaku terhadap korban. *Deepfake* dalam hal ini menciptakan visual yang menyerupai korban tanpa keterlibatan fisik, sehingga memperumit aspek pertanggungjawaban.

Silvia dkk. (Putri et al., 2024) turut merekomendasikan kriminalisasi tegas terhadap pelaku penyebaran *deepfake* dalam konteks penipuan, pencemaran nama baik, dan serangan terhadap integritas personal. Mereka mengusulkan pembentukan norma hukum pidana baru yang mengatur secara spesifik bentuk delik, ancaman pidana, serta perlindungan bagi korban.

Secara umum, hasil pengkajian menunjukkan bahwa teknologi *deepfake* memiliki potensi ganda: di satu sisi sebagai sarana inovasi, namun di sisi lain sebagai alat kriminalitas. Apabila tidak segera diatur, maka penyebaran *deepfake* dapat menyebabkan kerugian besar

di masyarakat—baik secara psikis, sosial, maupun hukum. Kondisi ini menuntut langkah komprehensif dari negara. Regulasi hukum pidana yang bersifat preventif dan represif terhadap *deepfake* perlu dirumuskan segera, termasuk dalam bentuk rancangan undang-undang khusus, revisi UU ITE, atau penyisipan pasal baru dalam KUHP yang mengatur secara khusus mengenai manipulasi konten berbasis AI. Sebagai bagian dari strategi penanggulangan, diperlukan juga peningkatan kapasitas aparat penegak hukum dalam memahami struktur dan logika teknologi *deepfake*. Kolaborasi antara sektor akademik, lembaga keamanan digital, dan pengembang perangkat lunak menjadi penting dalam mendukung keberhasilan penegakan hukum yang adaptif dan akuntabel.

Negara-negara lain telah menunjukkan langkah progresif. Denmark, misalnya, melalui kebijakan hak cipta atas wajah dan suara warganya, mencoba menjamin bahwa penggunaan wajah seseorang dalam konten *deepfake* tanpa izin dapat dikenai sanksi hukum (Bryant, 2025). Kebijakan ini berbasis prinsip kontrol atas data biometrik dan martabat pribadi, yang dapat diadopsi secara kontekstual di Indonesia. Dengan demikian, temuan penelitian ini memperkuat argumentasi bahwa regulasi hukum pidana Indonesia saat ini belum cukup memadai untuk mengantisipasi kompleksitas kejahatan digital seperti *deepfake*. Diperlukan reformulasi hukum yang progresif dan antisipatif, agar hukum pidana dapat menjalankan fungsinya sebagai instrumen perlindungan terhadap hak individu dan keadilan sosial di era disrupsi teknologi.

Urgensi Pengaturan Hukum Pidana Indonesia Terkait *Deepfake*

Fenomena *deepfake* telah menjadi isu penting dalam lanskap hukum pidana modern, khususnya dalam konteks transformasi digital di Indonesia. Teknologi ini menciptakan konten visual dan audio yang menyerupai realitas, namun bersifat manipulatif dan dapat menimbulkan kerugian hukum bagi individu atau masyarakat. Dalam kerangka hukum Indonesia saat ini, belum terdapat pengaturan normatif yang secara spesifik mengatur *deepfake* sebagai objek kejahatan, meskipun sejumlah pasal dalam UU ITE dan KUHP baru mencoba menjangkau perilaku tersebut secara tidak langsung.

Hasil analisis terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU No. 19 Tahun 2016) menunjukkan bahwa ketentuan dalam Pasal 27 ayat (3) dapat digunakan untuk menjerat pelaku penyebaran konten *deepfake* yang berunsur penghinaan atau pencemaran nama baik. Namun, formulasi norma dalam pasal tersebut tidak menyebutkan secara eksplisit jenis konten manipulatif seperti *deepfake*, yang secara teknis memiliki karakteristik berbeda dari konten digital biasa (Novyanti & Astuti, 2021).

Kajian lebih lanjut terhadap KUHP baru (UU No. 1 Tahun 2023) menunjukkan bahwa meskipun terdapat pembaruan terhadap pendekatan pemidanaan atas kejahatan berbasis teknologi, tidak terdapat satu pun pasal yang secara eksplisit mendefinisikan atau mengkualifikasi *deepfake* sebagai bentuk tindak pidana tersendiri. Beberapa pasal yang dapat dikaitkan, seperti Pasal 310 tentang pencemaran nama baik dan Pasal 378 tentang penipuan, masih bersifat umum dan belum mengakomodasi dinamika kejahatan digital berbasis kecerdasan buatan (Amelia et al., 2024).

Sebagian besar norma hukum pidana yang ada masih bersandar pada delik konvensional, yang tidak mempertimbangkan elemen teknologis seperti autentikasi algoritmik atau rekayasa digital wajah. Akibatnya, penegakan hukum terhadap pelaku penyebaran *deepfake* menjadi tidak optimal, baik dalam aspek substansi hukum maupun teknis pembuktian. Hal ini juga diamini oleh Sarah & Diana (Sijabat & Lukitasari, 2024), yang menyatakan bahwa konten *deepfake* dalam bentuk pornografi digital sering kali tidak bisa dijerat secara efektif karena kurangnya kepastian hukum mengenai bentuk visual hasil rekayasa.

Penelitian yuridis menunjukkan bahwa dalam ketiadaan norma eksplisit, aparat penegak hukum cenderung melakukan interpretasi hukum secara ekstensif. Ini mengarah pada kemungkinan terjadinya ketidakadilan dalam praktik penegakan hukum karena pembuktian kejahatan *deepfake* memerlukan pendekatan teknologis yang kompleks, termasuk digital forensics dan verifikasi visual berbasis AI (Masood et al., 2021). Oleh sebab itu, ruang hukum yang ada saat ini belum cukup memberikan kepastian dan perlindungan hukum yang optimal bagi korban kejahatan *deepfake*.

Dalam konteks hukum pidana nasional, model delik formil yang digunakan oleh KUHP membuat banyak kasus penyebaran konten *deepfake* sulit untuk dikualifikasikan ke dalam tindak pidana. Apalagi apabila pelaku menyebarkan konten melalui platform yang server-nya berada di luar yurisdiksi hukum Indonesia. Keadaan ini menimbulkan tantangan bagi aparat penegak hukum untuk membuktikan intensi pelaku (mens rea) maupun keberadaan alat bukti digital yang sah.

Dari tinjauan perbandingan, ditemukan bahwa beberapa negara telah mengambil langkah proaktif dalam merespons bahaya *deepfake*. Penelitian oleh Dalila dkkl. (Durães et al., 2023) menunjukkan bahwa Amerika Serikat, melalui regulasi di tingkat negara bagian seperti Texas dan California, telah mulai menerapkan aturan pidana terhadap penyebaran *deepfake* untuk kepentingan politik dan pornografi nonkonsensual. Hal ini memberikan preseden positif bagi pembentukan regulasi serupa di Indonesia. Studi komparatif dari Pavel & Sebastian (Korshunov & Marcel, 2018) memperlihatkan bahwa sistem keamanan berbasis

pengenalan wajah yang selama ini digunakan oleh lembaga negara maupun sektor privat masih rentan terhadap serangan *deepfake*. Oleh karena itu, pembaruan terhadap regulasi harus dibarengi dengan strategi mitigasi teknologi, agar pembuktian dalam konteks hukum pidana dapat dilaksanakan secara adil dan efisien.

Selain itu, penelitian oleh Iskandar et al. (2024) merekomendasikan bahwa pengaturan hukum pidana terhadap *deepfake* sebaiknya ditempatkan sebagai delik khusus (specialis), mengingat karakteristiknya yang kompleks dan multidisipliner. Tanpa kategori khusus, pasal-pasal dalam hukum pidana umum dikhawatirkan tidak mampu mengakomodasi kerugian non-material seperti trauma psikis, kerusakan reputasi, dan pembunuhan karakter yang dihasilkan dari konten *deepfake*. Implikasi regulatif dari ketiadaan norma khusus terhadap *deepfake* terlihat pada lemahnya perlindungan terhadap korban. Hasil penelitian menunjukkan bahwa banyak korban merasa tidak memperoleh keadilan karena laporan mereka dihentikan pada tahap penyelidikan akibat minimnya alat bukti digital yang sah. Dalam banyak kasus, aparat penegak hukum mengalami kesulitan untuk menjustifikasi konten manipulatif sebagai tindak pidana murni (Sijabat & Lukitasari, 2024).

Penelitian Masood et al. (2023) juga menggarisbawahi pentingnya kolaborasi antara regulator, akademisi, dan pengembang teknologi dalam membentuk kerangka hukum yang adaptif. Tanpa partisipasi dari berbagai pihak, regulasi yang dibentuk akan bersifat elitis dan ketinggalan zaman, terutama di tengah laju perkembangan teknologi yang sangat cepat.

Dalam dokumen kebijakan internasional seperti GDPR (General Data Protection Regulation), prinsip hak atas identitas visual dan data biometrik mulai diperluas ke wilayah hukum. Hal ini dapat menjadi rujukan bagi Indonesia dalam merumuskan kerangka hukum berbasis hak digital yang lebih progresif. Penerapan hak atas wajah dan suara sebagai bagian dari hak personal yang dilindungi hukum pidana dapat menjadi arah pembaruan yang relevan dalam konteks nasional (Durães et al., 2023). Lebih lanjut, Denmark bahkan berinisiatif memberikan hak cipta atas wajah dan suara warganya untuk mencegah penyalahgunaan *deepfake*, suatu pendekatan hukum preventif berbasis privasi dan kekayaan intelektual yang menunjukkan potensi hibridisasi rezim hukum dalam menanggulangi kejahatan digital (Bryant, 2025). Model ini membuka peluang bagi Indonesia untuk mengembangkan norma baru yang bersifat lintas bidang.

Sebagai hasil dari kajian ini, ditemukan bahwa regulasi hukum pidana Indonesia masih bersifat reaktif dan fragmentaris dalam merespons ancaman *deepfake*. Upaya kriminalisasi yang dilakukan masih mengandalkan pasal-pasal lama yang kurang responsif terhadap perkembangan teknologi. Oleh karena itu, sangat mendesak bagi pemerintah Indonesia untuk menyusun rancangan undang-undang khusus yang secara eksplisit mengatur

mengenai produksi, penyebaran, dan pertanggungjawaban pidana terhadap konten *deepfake*.

SIMPULAN

Berdasarkan hasil analisis yuridis normatif terhadap fenomena *deepfake* dan kerangka hukum yang mengaturnya di Indonesia, dapat disimpulkan bahwa teknologi ini menghadirkan tantangan serius dalam sistem hukum pidana nasional. Absennya ketentuan hukum yang secara eksplisit mengatur mengenai *deepfake* menimbulkan kekosongan hukum (rechtsvacuum) yang berdampak pada ketidakpastian dalam penegakan hukum. Meskipun beberapa pasal dalam UU ITE dan KUHP dapat digunakan sebagai dasar pemidanaan, karakteristik manipulatif dan kompleksitas teknologis dari *deepfake* membuat pasal-pasal tersebut tidak cukup responsif. Dalam praktiknya, aparat penegak hukum mengalami kendala dalam aspek pembuktian, yurisdiksi, dan identifikasi intensi pelaku. Situasi ini memperkuat urgensi pembentukan norma hukum pidana khusus yang mengklasifikasikan penyebaran konten *deepfake* sebagai tindak pidana tersendiri dengan unsur-unsur yang lebih jelas dan terukur.

Di sisi lain, pengalaman beberapa negara seperti Amerika Serikat dan Denmark menunjukkan bahwa pendekatan progresif terhadap regulasi *deepfake*, baik melalui pengakuan hak atas identitas visual maupun kriminalisasi khusus, dapat memberikan arah bagi Indonesia dalam merumuskan kebijakan serupa. Kolaborasi lintas sektor antara pemerintah, akademisi, dan komunitas teknologi menjadi kunci dalam membentuk sistem hukum yang adaptif dan tanggap terhadap perkembangan teknologi. Oleh karena itu, diperlukan langkah konkret berupa penyusunan undang-undang khusus atau pembaruan norma dalam KUHP dan UU ITE yang mampu menjawab tantangan kejahatan digital masa kini. Dengan begitu, hukum pidana Indonesia akan mampu menjalankan fungsinya sebagai instrumen perlindungan terhadap martabat individu, keamanan sosial, dan keadilan di era disrupsi digital.

DAFTAR PUSTAKA

Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut Hukum positif Indonesia. *Dinamika*, *30*(1), 9675–9691.

Bryant, M. (2025). *Denmark to tackle deepfakes by giving people copyright to their own features*. Https://Www.Theguardian.Com/. https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence

Delfino, R. A. (2022). Deepfakes on trial: a call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *Hastings LJ*, *74*, 293.

Durães, D., Freitas, P. M., & Novais, P. (2023). The relevance of deepfakes in the administration of criminal justice. In *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (pp. 351–369). Springer International Publishing Cham.

Firmanto, T., Sufiarina, S., Reumi, F., & Saleh, I. N. S. (2024). *Metodologi Penelitian Hukum: Panduan Komprehensif Penulisan Ilmiah Bidang Hukum*. PT. Sonpedia Publishing Indonesia.

Korshunov, P., & Marcel, S. (2018). Deepfakes: a new threat to face recognition? assessment and detection. *ArXiv Preprint ArXiv:1812.08685*.

Kothari, S., & Tibrewala, S. (2024). AI's Trojan Horse: The Deepfake conundrum under the criminal justice system. *GLS KALP: Journal of Multidisciplinary Studies*, *4*(3), 45–53.

Majeed, N., Hilal, A., & Khan, A. N. (2023). Doctrinal Research in Law: Meaning, Scope and Methodology. *Bulletin of Business and Economics (BBE)*, *12*(4), 559–563.

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, *53*(4), 3974–4026.

McCrudden, C. (2017). Legal research and the social sciences. In *Legal Theory and the Social Sciences* (pp. 149–167). Routledge.

Novyanti, H., & Astuti, P. (2021). Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana. *Novum: Jurnal Hukum*, 31–40.

Prayoga, H., & Tuasikal, H. (2025). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. *Abdurrauf Law and Sharia*, *2*(1), 22–38.

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

Salvi, C. (2023). *Deepfake Evidence in Criminal Proceedings: Procedural hurdles and forensic challanges*. https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/SALVI-8.711-Deepfake-evidence-Salvi-Crim-AI.pdf

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, *13*(1), 41.

Sijabat, S. A. U., & Lukitasari, D. (2024). Konten Gambar dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik. *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *13*(2), 179–194.

Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada*. Jakarta: Rajawali Pers.

Syahirah, S. N., & Prasetyo, B. (2025). Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (Ai) Di Indonesia. *Jurnal Inovasi Hukum Dan Kebijakan*, *6*(1).

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, *64*, 131–148.