



Rekonstruksi Delik Pidana dalam Kejahatan Deepfake: Tantangan Pembuktian dan Perlindungan Korban

Andriansyah Kartadinata

Universitas Sang Bumi Ruwa Jurai, Indonesia

Alamat: Jl. Imam Bonjol No.486, Langkapura, Kec. Langkapura, Kota Bandar Lampung, Lampung

Korespondensi penulis: andri.fhunsab@gmail.com

Abstract. *The rapid development of artificial intelligence has led to the emergence of deepfake technology, which poses significant challenges to criminal law enforcement. Deepfake crimes involve the manipulation of audio-visual content that can harm individual dignity, privacy, and legal interests, while existing criminal law regulations in Indonesia have not explicitly addressed this phenomenon. This research aims to analyze the adequacy of current criminal law in dealing with deepfake crimes and to reconstruct the formulation of criminal offenses by focusing on evidentiary challenges and victim protection. This study employs normative legal research using statutory and conceptual approaches, supported by qualitative analysis of legal norms and recent scholarly works. The findings indicate that the absence of specific criminal provisions on deepfake results in legal uncertainty, difficulties in proving criminal intent, and inadequate protection for victims. Therefore, this research suggests the need for an adaptive reconstruction of criminal offenses that accommodates digital evidence and integrates victim-oriented protection mechanisms. The study contributes theoretically to the development of contemporary criminal law and practically to policymaking in addressing technology-based crimes.*

Keywords: *Artificial Intelligence; Criminal Law Reform; Deepfake; Digital Evidence; Victim Protection*

Abstrak. Perkembangan pesat teknologi kecerdasan buatan telah melahirkan fenomena *deepfake* yang menimbulkan tantangan serius dalam penegakan hukum pidana. Kejahatan *deepfake* melibatkan manipulasi konten audio-visual yang berpotensi merugikan kehormatan, privasi, dan kepentingan hukum seseorang, sementara hukum pidana Indonesia belum mengaturnya secara spesifik. Penelitian ini bertujuan untuk menganalisis kecukupan hukum pidana dalam menangani kejahatan *deepfake* serta merekonstruksi perumusan delik pidana dengan menitikberatkan pada tantangan pembuktian dan perlindungan korban. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual, yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa ketiadaan delik pidana khusus *deepfake* menyebabkan ketidakpastian hukum, kesulitan pembuktian unsur kesalahan, dan belum optimalnya perlindungan korban. Oleh karena itu, diperlukan rekonstruksi delik pidana yang adaptif terhadap perkembangan teknologi dan berorientasi pada perlindungan korban. Penelitian ini diharapkan memberikan kontribusi teoretis dan praktis bagi pembaruan hukum pidana nasional.

Kata kunci: Deepfake; Hukum Pidana; Kecerdasan Buatan; Pembuktian Digital; Perlindungan Korban

1. LATAR BELAKANG

Perkembangan teknologi digital berbasis *artificial intelligence* (AI) telah membawa transformasi besar dalam masyarakat modern, termasuk dalam produksi konten media digital yang semakin realistis melalui teknologi *deepfake*. Teknologi ini memanfaatkan algoritma pembelajaran mesin untuk menciptakan atau memodifikasi gambar, suara, maupun video sehingga tampak nyata, meskipun bukan representasi dari fakta objektif (Prayoga & Tuasikal, 2025). Fenomena *deepfake* telah menyebar luas di ruang siber dengan berbagai dampak sosial dan hukum, mulai dari pencemaran nama baik, penipuan, sampai penyebaran konten pornografi tanpa persetujuan korban (Isnawan, 2024; Wicaksana & Dewi, 2024).

Dalam konteks hukum pidana di Indonesia, kejahatan *deepfake* masih merupakan wilayah yang belum sepenuhnya terakomodasi dalam peraturan perundang-undangan. Beberapa kajian menyatakan bahwa meskipun UU Informasi dan Transaksi Elektronik (UU ITE), KUHP, UU Pornografi dan UU Perlindungan Data Pribadi menawarkan payung normatif terhadap berbagai bentuk penyalahgunaan konten digital, belum terdapat perumusan delik pidana yang secara eksplisit mencakup kejahatan *deepfake* sebagai bentuk delik baru (Isnawan, 2024; Putra & Dewi, 2024). Kondisi ini mencerminkan adanya *legal vacuum* yang berpotensi menghambat efektivitas penegakan hukum dalam menangani kasus-kasus *deepfake* (Afif, 2025).

Permasalahan tersebut juga berimplikasi pada prinsip asas legalitas dalam hukum pidana, bahwa suatu perbuatan hanya dapat dipidana jika telah jelas diatur dalam norma hukum yang berlaku (*nullum crimen sine lege*). Ketika teknologi *deepfake* berkembang lebih cepat dibanding peraturan yang menyertainya, aparat penegak hukum dihadapkan pada tantangan untuk menafsirkan norma yang ada secara ekstensif, yang berisiko menimbulkan ketidakpastian hukum (Isnawan, 2024). Hal ini diperparah oleh fakta bahwa konten *deepfake* sering kali memiliki karakteristik teknis yang kompleks dan dinamis sehingga sulit diidentifikasi dengan metode pembuktian konvensional (Prayoga & Tuasikal, 2025).

Permasalahan pembuktian menjadi salah satu isu sentral dalam penegakan hukum terhadap *deepfake*. Bukti digital dalam kasus *deepfake* cenderung sangat rawan manipulasi dan sering kali memerlukan keahlian forensik digital untuk dapat menentukan apakah suatu konten memang palsu secara teknologi atau merupakan hasil rekayasa AI (Prayoga & Tuasikal, 2025; Rahayu & Kuswandi, 2025). Ketiadaan mekanisme pembuktian yang memadai dapat menyebabkan aparat penegak hukum kesulitan menunjukkan keterkaitan pelaku dengan konten *deepfake*, khususnya dalam hal niat jahat (*mens rea*) dan keterlibatan langsung dalam proses pembuatan konten tersebut.

Lebih lanjut, aspek perlindungan korban menjadi isu yang mendesak namun masih kurang mendapat perhatian dalam kajian hukum pidana Indonesia. Korban *deepfake* sering menghadapi dampak psikologis, reputasi sosial yang rusak, dan pelanggaran privasi yang berkepanjangan, terutama pada konten pornografi yang dibuat tanpa persetujuan mereka (Alfathoni, Pratama & Lubis, 2025; Syaputra & Nuriyatman, 2025). Perlindungan hukum terhadap korban ini perlu dikaji secara mendalam agar sistem pidana tidak hanya berorientasi pada penghukuman pelaku tetapi juga perlindungan hak korban secara substantif.

Berbagai negara telah mulai merespon tantangan hukum *deepfake* melalui pembaruan regulasi pidana. Misalnya, beberapa legislator di Korea Selatan telah mengesahkan aturan yang

mengkriminalisasi kepemilikan dan tontonan pornografi *deepfake* dengan pidana penjara atau denda berat, sebagai bentuk antisipasi penyalahgunaan teknologi yang meluas (Reuters, 2024). Di Amerika Serikat, legislator federal juga mendorong pengaturan khusus terhadap konten *deepfake* non-konsensual dengan kewajiban penghapusan konten dalam waktu tertentu setelah pemberitahuan (Time, 2025). Perkembangan internasional ini menunjukkan arah normatif yang potensial untuk diadopsi secara selektif dalam pembaruan hukum pidana nasional.

Kajian akademik yang ada sejauh ini sebagian besar masih berfokus pada aspek peraturan normatif atau studi kasus tertentu tentang penyalahgunaan *deepfake* tanpa mengupas tuntas tantangan pembuktian dan rekonstruksi delik pidana yang komprehensif. Misalnya, studi tentang urgensi pengaturan *deepfake* pornografi di Indonesia menegaskan perlunya norma yang jelas untuk mengatasi celah hukum saat ini (Putra & Dewi, 2024). Namun, masih diperlukan penelitian yang memetakan secara holistik bagaimana delik pidana dapat direkonstruksi untuk mencerminkan karakteristik *deepfake* sekaligus mempertimbangkan tantangan pembuktian dan perlindungan korban secara efektif.

Dengan latar belakang tersebut, penelitian ini hadir untuk mengisi gap antara fenomena *deepfake* sebagai kejahatan baru dan ketertinggalan sistem hukum pidana nasional dalam meresponnya. Fokus penelitian ini adalah merekonstruksi perumusan delik pidana *deepfake* yang tepat, mengidentifikasi hambatan dalam pembuktian digital di ranah peradilan, dan mengusulkan mekanisme perlindungan hukum yang lebih kuat bagi korban. Diharapkan hasil penelitian ini dapat memberikan kontribusi teoritis untuk pengembangan hukum pidana kontemporer serta rekomendasi praktis bagi pembuat kebijakan dan aparat penegak hukum dalam menghadapi kejahatan *deepfake* di era digital.

2. KAJIAN TEORITIS

Kajian teoretis dalam penelitian ini bertumpu pada teori hukum pidana modern yang menempatkan hukum pidana sebagai instrumen perlindungan kepentingan hukum (*rechtsbelangen*) masyarakat dan individu di tengah perkembangan teknologi digital. Dalam konteks ini, hukum pidana tidak hanya berfungsi sebagai sarana represif, tetapi juga sebagai mekanisme preventif terhadap bentuk-bentuk kejahatan baru yang muncul akibat kemajuan teknologi informasi dan kecerdasan buatan (*artificial intelligence*) (Ashworth & Horder, 2022).

Teori kriminalisasi menjadi landasan penting dalam menganalisis kejahatan *deepfake*. Kriminalisasi dipahami sebagai proses penetapan suatu perbuatan sebagai tindak pidana berdasarkan pertimbangan bahaya sosial, kebutuhan perlindungan hukum, serta

proporsionalitas sanksi pidana. Beberapa ahli menegaskan bahwa kriminalisasi terhadap perbuatan berbasis teknologi harus didasarkan pada *harm principle*, yakni sejauh mana perbuatan tersebut menimbulkan kerugian nyata terhadap individu atau masyarakat (Duff et al., 2019; Simester & Sullivan, 2021). Dalam konteks *deepfake*, kerugian tersebut tampak nyata dalam bentuk pelanggaran privasi, kehormatan, dan integritas personal korban.

Teori asas legalitas juga menjadi kerangka utama dalam kajian ini, mengingat kejahatan *deepfake* belum dirumuskan secara eksplisit dalam hukum pidana positif Indonesia. Asas legalitas menuntut adanya kejelasan rumusan delik, unsur perbuatan, dan ancaman pidana agar tidak terjadi kesewenang-wenangan dalam penegakan hukum. Dalam perkembangan hukum pidana kontemporer, asas legalitas tidak lagi dipahami secara kaku, tetapi tetap menekankan kepastian dan prediktabilitas hukum dalam menghadapi kejahatan berbasis teknologi (Husak, 2020; Ambos, 2021).

Selain itu, teori pertanggungjawaban pidana relevan untuk menganalisis subjek hukum dalam kejahatan *deepfake*. Kejahatan ini tidak selalu dilakukan oleh individu secara langsung, melainkan dapat melibatkan penggunaan sistem AI, platform digital, atau bahkan jaringan anonim. Oleh karena itu, konsep *mens rea* dan *actus reus* dalam hukum pidana klasik perlu dikaji ulang agar mampu mengakomodasi perbuatan pidana yang dilakukan dengan perantara teknologi otomatis atau semi-otomatis (Brenner, 2021; Gless, Silverman & Weigend, 2023).

Dari perspektif pembuktian, teori pembuktian pidana dan *digital evidence* menjadi sangat relevan. Bukti digital memiliki karakteristik mudah dimodifikasi, direplikasi, dan dihapus, sehingga membutuhkan pendekatan khusus dalam proses pembuktian. Teori *chain of custody* dan *forensic reliability* menjadi penting untuk menjamin keabsahan alat bukti digital dalam perkara *deepfake* (Casey, 2020; Rahayu & Kuswandi, 2025). Tantangan pembuktian ini menunjukkan bahwa hukum acara pidana harus beradaptasi dengan kompleksitas teknologi AI.

Kajian ini juga menggunakan teori viktimologi modern, khususnya pendekatan *victim-oriented justice*, yang menempatkan korban sebagai subjek utama dalam sistem peradilan pidana. Kejahatan *deepfake* sering kali menimbulkan penderitaan non-material yang mendalam bagi korban, termasuk trauma psikologis dan kerusakan reputasi jangka panjang. Teori viktimologi kontemporer menekankan pentingnya pemulihan korban melalui perlindungan hukum, penghapusan konten, dan restitusi, bukan sekadar penghukuman pelaku (Walklate, 2021; Syaputra & Nuriyatman, 2025).

Sejumlah penelitian terdahulu menunjukkan bahwa pengaturan hukum terhadap *deepfake* masih berada pada tahap awal. Penelitian Prayoga dan Tuasikal (2025) menyoroti kesulitan

pembuktian kejahatan *deepfake* dalam sistem hukum Indonesia akibat keterbatasan regulasi dan sumber daya forensik digital. Putra dan Dewi (2024) menegaskan adanya kekosongan norma dalam UU ITE terkait manipulasi konten berbasis AI, yang menyebabkan aparat penegak hukum harus menggunakan pendekatan analogi pasal.

Penelitian lain menekankan urgensi perlindungan korban *deepfake*, terutama dalam kasus pornografi non-konsensual. Alfathoni, Pratama, dan Lubis (2025) menunjukkan bahwa kerangka hukum yang ada belum mampu memberikan pemulihan efektif bagi korban, sehingga banyak korban memilih tidak melaporkan kasusnya. Sementara itu, studi komparatif yang dilakukan oleh Gless et al. (2023) menunjukkan bahwa beberapa negara mulai merumuskan delik khusus *deepfake* sebagai respon terhadap ancaman teknologi AI terhadap sistem hukum pidana.

Berdasarkan kajian teori dan penelitian terdahulu tersebut, dapat dipahami bahwa kejahatan *deepfake* menuntut pendekatan hukum pidana yang adaptif dan progresif. Rekonstruksi delik pidana menjadi kebutuhan mendesak untuk menjamin kepastian hukum, efektivitas pembuktian, serta perlindungan korban. Secara implisit, penelitian ini berangkat dari asumsi bahwa hukum pidana Indonesia saat ini belum sepenuhnya mampu merespon karakteristik kejahatan *deepfake*, sehingga diperlukan perumusan konsep hukum pidana yang lebih responsif terhadap perkembangan teknologi AI dan dinamika kejahatan digital.

3. METODE PENELITIAN

Penelitian ini menggunakan desain penelitian hukum normatif dengan pendekatan konseptual dan peraturan perundang-undangan (*statute approach*). Desain ini dipilih karena fokus penelitian adalah menganalisis norma hukum pidana yang mengatur atau berkaitan dengan kejahatan *deepfake*, serta merekonstruksi perumusan delik pidana yang relevan dengan perkembangan teknologi *artificial intelligence*. Selain itu, pendekatan konseptual digunakan untuk mengkaji doktrin, asas, dan teori hukum pidana yang mendasari pembentukan delik serta sistem pembuktian dalam perkara pidana berbasis teknologi digital.

Populasi dalam penelitian ini berupa keseluruhan norma hukum pidana yang relevan dengan kejahatan *deepfake*, baik yang bersumber dari Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi, maupun peraturan perundang-undangan lain yang berkaitan dengan kejahatan siber dan perlindungan korban. Sampel penelitian ditentukan secara purposif, yaitu

norma-norma hukum yang memiliki keterkaitan langsung dengan unsur perbuatan, pertanggungjawaban pidana, pembuktian, dan perlindungan korban dalam kejahatan *deepfake*.

Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan, putusan pengadilan yang relevan, serta dokumen kebijakan hukum pidana. Bahan hukum sekunder mencakup hasil penelitian terdahulu, jurnal ilmiah, buku teks hukum pidana, dan publikasi akademik lima tahun terakhir yang membahas *deepfake*, kejahatan siber, pembuktian digital, dan perlindungan korban. Adapun bahan hukum tersier digunakan sebagai penunjang berupa kamus hukum dan ensiklopedia hukum.

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*), dengan cara menelusuri, menginventarisasi, dan mengkaji bahan-bahan hukum yang relevan secara sistematis. Instrumen pengumpulan data berupa daftar telaah dokumen yang digunakan untuk mengidentifikasi kesesuaian norma hukum yang ada dengan karakteristik kejahatan *deepfake*, khususnya dalam aspek perumusan delik dan pembuktian. Metode pengumpulan data yang bersifat umum dalam penelitian hukum normatif digunakan sebagaimana dirujuk dalam metodologi penelitian hukum (Soekanto & Mamudji, 2021).

Analisis data dilakukan secara kualitatif dengan menggunakan metode analisis yuridis normatif. Data yang telah dikumpulkan dianalisis melalui penafsiran hukum, baik secara gramatikal, sistematis, maupun teleologis, untuk menilai kecukupan norma hukum pidana dalam mengakomodasi kejahatan *deepfake*. Selain itu, analisis konseptual digunakan untuk membandingkan doktrin dan teori hukum pidana dengan praktik penegakan hukum, khususnya terkait pembuktian digital dan perlindungan korban. Metode analisis yang bersifat umum tidak diuraikan secara rinci dan merujuk pada teknik analisis kualitatif dalam penelitian hukum.

Model penelitian yang digunakan dalam penelitian ini bersifat deskriptif-analitis dan preskriptif. Secara deskriptif, penelitian ini memetakan karakteristik kejahatan *deepfake* serta ketentuan hukum pidana yang relevan. Secara analitis, penelitian ini mengkaji kesenjangan antara norma hukum yang ada dan kebutuhan pengaturan terhadap *deepfake*. Selanjutnya, secara preskriptif, penelitian ini merumuskan model rekonstruksi delik pidana yang ideal dengan memperhatikan unsur perbuatan, kesalahan, pembuktian, dan perlindungan korban. Dalam model ini, kejahatan *deepfake* diposisikan sebagai variabel utama yang mempengaruhi kebutuhan pembaruan norma delik pidana, sementara sistem pembuktian dan perlindungan korban dipahami sebagai konsekuensi yuridis yang harus diakomodasi dalam perumusan delik tersebut.

4. HASIL DAN PEMBAHASAN

Penelitian ini dilaksanakan melalui studi kepustakaan terhadap berbagai sumber hukum dan literatur ilmiah yang relevan dengan kejahatan *deepfake* dalam perspektif hukum pidana. Proses pengumpulan data dilakukan dalam rentang waktu Januari hingga Juni 2025 dengan lokasi penelitian berbasis studi dokumen, tanpa keterikatan pada wilayah geografis tertentu, mengingat karakter penelitian hukum normatif. Data diperoleh dari peraturan perundang-undangan nasional, putusan pengadilan yang relevan, jurnal ilmiah lima tahun terakhir, serta dokumen kebijakan dan laporan institusi terkait kejahatan siber dan teknologi kecerdasan buatan.

1. Bentuk dan Pola Kejahatan Deepfake

a) Deepfake sebagai Modus Operandi Kejahatan Digital

Hasil analisis menunjukkan bahwa *deepfake* tidak dapat dipahami semata-mata sebagai produk teknologi berupa konten palsu, melainkan telah berkembang menjadi modus operandi baru dalam berbagai bentuk kejahatan digital. Penggunaan teknologi kecerdasan buatan dalam pembuatan *deepfake* memungkinkan pelaku menciptakan representasi visual atau audio yang sangat menyerupai korban, sehingga memperkuat daya tipu dan meningkatkan efektivitas kejahatan yang dilakukan. Dalam konteks ini, *deepfake* berfungsi sebagai sarana utama yang mendukung terwujudnya tindak pidana.

Dalam praktiknya, *deepfake* banyak dimanfaatkan dalam tindak pidana penipuan daring, khususnya dengan cara meniru suara atau wajah pihak tertentu yang memiliki otoritas atau kedekatan dengan korban. Modus ini kerap digunakan untuk menipu korban agar mentransfer uang atau memberikan akses terhadap data pribadi. Tingginya tingkat realisme konten *deepfake* menyebabkan korban sulit membedakan antara komunikasi asli dan hasil rekayasa teknologi, sehingga memperbesar potensi kerugian yang ditimbulkan.

Selain penipuan, *deepfake* juga digunakan sebagai sarana pemerasan dan pencemaran nama baik. Pelaku dapat menciptakan konten palsu yang menampilkan korban seolah-olah melakukan perbuatan tercela, kemudian mengancam akan menyebarkan konten tersebut jika korban tidak memenuhi tuntutan tertentu. Dalam konteks ini, *deepfake* berperan sebagai alat yang memperparah kerugian immaterial korban, seperti rusaknya reputasi, kehormatan, dan kepercayaan sosial.

Modus operandi *deepfake* juga banyak ditemukan dalam kejahatan pornografi non-konsensual, di mana wajah korban ditempelkan pada tubuh orang lain dalam konten pornografi tanpa persetujuan. Kejahatan ini menimbulkan penderitaan psikologis yang mendalam dan berkepanjangan bagi korban, terutama karena konten tersebut dapat tersebar secara masif dan

sulit dihapus dari ruang digital. Karakteristik ini menunjukkan bahwa *deepfake* tidak hanya memperluas jenis kejahatan, tetapi juga meningkatkan tingkat keparahan dampak yang ditimbulkan.

Karakteristik utama *deepfake* sebagai modus operandi kejahatan digital terletak pada realisme yang tinggi, kemudahan distribusi melalui berbagai platform digital, serta kesulitan dalam mengidentifikasi pelaku dan sumber pembuatan konten. Faktor-faktor tersebut membedakan *deepfake* dari bentuk manipulasi digital konvensional dan menimbulkan tantangan tersendiri bagi hukum pidana, khususnya dalam menentukan konstruksi delik, pembuktian, dan pertanggungjawaban pidana pelaku.

b) Posisi Deepfake dalam Tipologi Kejahatan Siber

Berdasarkan hasil kajian normatif, *deepfake* belum memiliki posisi yang jelas dalam tipologi kejahatan siber dalam hukum pidana Indonesia. Tidak terdapat delik pidana yang secara eksplisit merumuskan perbuatan pembuatan, penggunaan, atau penyebaran konten *deepfake* sebagai tindak pidana tersendiri. Akibatnya, penanganan kasus *deepfake* masih bergantung pada konstruksi delik yang bersifat umum dan tidak dirancang untuk menghadapi karakteristik kejahatan berbasis kecerdasan buatan.

Dalam praktik penegakan hukum, *deepfake* sering dikualifikasikan melalui delik analogi, seperti pencemaran nama baik, penyebaran konten melanggar kesusilaan, atau penyebaran berita bohong. Pendekatan ini menunjukkan adanya upaya adaptasi aparat penegak hukum terhadap fenomena baru, namun sekaligus mengungkap keterbatasan norma hukum yang ada. Delik-delik tersebut pada dasarnya tidak dirancang untuk menangani manipulasi realitas digital yang kompleks seperti *deepfake*.

Ketidaktepatan klasifikasi *deepfake* dalam tipologi kejahatan siber berdampak pada ketidakjelasan unsur delik yang harus dibuktikan. Misalnya, unsur kesengajaan, perbuatan melawan hukum, dan akibat yang ditimbulkan sering kali sulit disesuaikan dengan karakteristik *deepfake* yang melibatkan teknologi otomatis dan penyebaran lintas platform. Kondisi ini berpotensi menimbulkan perbedaan penafsiran hukum dan inkonsistensi putusan pengadilan.

Selain itu, absennya klasifikasi delik khusus *deepfake* juga berdampak pada aspek perlindungan korban. Ketika *deepfake* dipaksakan masuk ke dalam delik konvensional, kebutuhan khusus korban, seperti penghapusan cepat konten dan pemulihan reputasi, sering kali tidak terakomodasi secara optimal. Hal ini menunjukkan bahwa tipologi kejahatan siber yang ada belum sepenuhnya responsif terhadap bentuk kejahatan berbasis kecerdasan buatan.

Dengan demikian, hasil penelitian ini menegaskan bahwa *deepfake* memerlukan posisi tersendiri dalam tipologi kejahatan siber dan hukum pidana nasional. Penempatan *deepfake* sebagai delik khusus akan memberikan kepastian hukum, mempermudah pembuktian, serta memungkinkan perumusan mekanisme perlindungan korban yang lebih komprehensif. Temuan ini sekaligus memperkuat urgensi rekonstruksi delik pidana *deepfake* sebagai bagian dari pembaruan hukum pidana di era digital.

2. Pembuktian Unsur Perbuatan dan Kesalahan

a) Kompleksitas Alat Bukti Digital

Hasil penelitian menunjukkan bahwa pembuktian dalam perkara *deepfake* menghadapi hambatan serius, terutama dalam menentukan keaslian atau kepalsuan konten digital yang dijadikan alat bukti. Teknologi *deepfake* dirancang untuk menghasilkan konten yang sangat realistis sehingga sulit dibedakan dari rekaman asli, bahkan dengan pengamatan visual biasa. Kondisi ini menyebabkan alat bukti elektronik dalam perkara *deepfake* memiliki tingkat kerentanan yang tinggi terhadap kesalahan interpretasi.

Kerentanan alat bukti digital semakin meningkat karena sifat data elektronik yang mudah dimodifikasi, disalin, dan disebarluaskan tanpa meninggalkan jejak yang jelas. Dalam konteks hukum acara pidana, karakteristik tersebut menimbulkan persoalan serius terkait keandalan (*reliability*) dan keabsahan (*authenticity*) alat bukti elektronik. Tanpa mekanisme verifikasi yang memadai, risiko terjadinya kesalahan pembuktian menjadi semakin besar.

Analisis forensik digital menjadi instrumen kunci dalam pembuktian perkara *deepfake*. Proses ini melibatkan pemeriksaan metadata, pola piksel, artefak audio-visual, serta penggunaan perangkat lunak khusus untuk mendeteksi rekayasa berbasis kecerdasan buatan. Namun demikian, hasil penelitian menunjukkan bahwa ketergantungan pada ahli forensik digital sangat tinggi, sementara ketersediaan tenaga ahli dan sarana pendukung belum merata di seluruh wilayah Indonesia.

Kondisi tersebut berdampak pada kesenjangan kualitas pembuktian antar perkara dan antar daerah. Perkara *deepfake* yang ditangani oleh aparat penegak hukum dengan akses terbatas terhadap teknologi forensik digital berpotensi mengalami kegagalan pembuktian, meskipun secara faktual kejahatan telah terjadi. Hal ini menunjukkan bahwa efektivitas pembuktian dalam perkara *deepfake* tidak hanya bergantung pada norma hukum, tetapi juga pada kapasitas institusional penegak hukum.

Dengan demikian, kompleksitas alat bukti digital dalam perkara *deepfake* menuntut pembaruan pendekatan pembuktian dalam hukum pidana. Pengakuan eksplisit terhadap alat

bukti forensik digital, peningkatan standar keahlian, serta penguatan infrastruktur teknologi menjadi prasyarat penting agar sistem peradilan pidana mampu merespons tantangan pembuktian kejahatan berbasis kecerdasan buatan secara efektif.

b) Pembuktian Mens Rea Pelaku

Selain persoalan teknis alat bukti, pembuktian unsur kesalahan (*mens rea*) pelaku dalam perkara *deepfake* merupakan tantangan fundamental dalam hukum pidana. *Mens rea* sebagai unsur subjektif tindak pidana menuntut pembuktian adanya niat, kesengajaan, atau setidaknya kelalaian pelaku dalam melakukan perbuatan yang dilarang. Dalam kejahatan *deepfake*, pembuktian unsur ini menjadi kompleks karena perbuatan dilakukan dengan bantuan teknologi otomatis.

Hasil penelitian menunjukkan bahwa pelaku *deepfake* kerap menggunakan identitas anonim, akun palsu, atau jaringan virtual untuk menyamarkan keterlibatannya. Selain itu, penggunaan platform pihak ketiga dan layanan berbasis *cloud* semakin mempersulit pelacakan jejak digital pelaku. Kondisi ini menyebabkan keterkaitan langsung antara pelaku dan konten *deepfake* sering kali sulit dibuktikan secara meyakinkan di pengadilan.

Kompleksitas pembuktian *mens rea* juga berkaitan dengan sifat teknologi *deepfake* yang dapat dioperasikan secara otomatis atau semi-otomatis. Dalam beberapa kasus, pelaku cukup memasukkan data tertentu ke dalam sistem AI, sementara proses pembuatan konten dilakukan oleh algoritma. Situasi ini menimbulkan pertanyaan yuridis mengenai sejauh mana niat pelaku dapat dilekatkan pada hasil kerja sistem teknologi yang digunakan.

Akibat kesulitan pembuktian tersebut, terdapat risiko bahwa pelaku *deepfake* tidak dapat dimintai pertanggungjawaban pidana secara optimal. Kegagalan membuktikan *mens rea* berpotensi menyebabkan terdakwa dibebaskan, meskipun secara objektif perbuatan yang dilakukan telah menimbulkan kerugian serius bagi korban. Hal ini pada akhirnya melemahkan fungsi preventif dan represif hukum pidana.

Hasil penelitian ini menunjukkan perlunya penyesuaian konsep pembuktian *mens rea* dalam perkara *deepfake*. Pendekatan yang lebih fleksibel, seperti pengakuan terhadap *dolus eventualis* atau perluasan pembuktian berbasis pola perilaku digital, dapat menjadi alternatif untuk menjembatani kesenjangan antara konsep klasik *mens rea* dan realitas kejahatan berbasis kecerdasan buatan. Penyesuaian ini penting untuk menjamin efektivitas pertanggungjawaban pidana tanpa mengabaikan prinsip kehati-hatian dalam penegakan hukum.

3. Dampak Kejahatan Deepfake terhadap Korban

a) Kerugian Psikologis dan Sosial

Hasil analisis menunjukkan bahwa kejahatan *deepfake* menimbulkan kerugian yang bersifat multidimensional bagi korban, terutama dalam aspek psikologis dan sosial. Korban sering mengalami tekanan mental, kecemasan, rasa malu, serta trauma berkepanjangan akibat penyebaran konten palsu yang mencemarkan martabat dan identitas personal. Dampak ini semakin berat ketika konten *deepfake* berkaitan dengan pornografi atau perbuatan tercela, karena stigma sosial yang melekat sulit dipulihkan meskipun konten tersebut kemudian dibantah atau dihapus.

Selain dampak psikologis, korban *deepfake* juga mengalami kerusakan reputasi dan pelanggaran privasi yang berkelanjutan. Karakteristik ruang digital yang memungkinkan distribusi konten secara cepat dan masif menyebabkan korban kehilangan kendali atas citra dirinya. Ketika sistem hukum tidak mampu memberikan pemulihan yang cepat dan efektif, penderitaan korban menjadi semakin kompleks dan berpotensi menimbulkan ketidakpercayaan terhadap mekanisme perlindungan hukum yang tersedia.

b) Keterbatasan Mekanisme Perlindungan Hukum

Penelitian ini menemukan bahwa mekanisme perlindungan korban dalam kejahatan *deepfake* masih bersifat parsial dan belum terintegrasi secara komprehensif dalam sistem hukum pidana Indonesia. Penanganan perkara *deepfake* cenderung berfokus pada pembuktian kesalahan dan pemidanaan pelaku, sementara kebutuhan korban untuk memperoleh perlindungan segera dan pemulihan jangka panjang belum menjadi prioritas utama dalam proses peradilan pidana.

Keterbatasan tersebut terlihat dari belum adanya pengaturan yang jelas mengenai kewajiban penghapusan konten *deepfake*, pemberian restitusi, maupun rehabilitasi psikologis bagi korban. Kondisi ini menguatkan kritik terhadap pendekatan *offender-oriented* yang masih dominan dalam hukum pidana Indonesia, sehingga kepentingan dan hak korban belum mendapatkan perlindungan yang seimbang. Oleh karena itu, diperlukan pergeseran paradigma menuju sistem peradilan pidana yang lebih berorientasi pada korban.

4. Rekonstruksi Delik Pidana dalam Kejahatan Deepfake

a) Perumusan Unsur Delik yang Adaptif

Berdasarkan hasil analisis, penelitian ini mengusulkan rekonstruksi delik pidana *deepfake* dengan merumuskan unsur perbuatan secara eksplisit, meliputi pembuatan, penggunaan, dan penyebaran konten palsu berbasis kecerdasan buatan yang menimbulkan

kerugian terhadap kepentingan hukum orang lain. Perumusan unsur delik yang jelas diperlukan untuk memberikan kepastian hukum serta membedakan *deepfake* dari bentuk manipulasi digital konvensional.

Selain unsur perbuatan, unsur kesalahan dalam delik *deepfake* perlu dirumuskan secara adaptif dengan mengakomodasi kesengajaan maupun kelalaian yang relevan dalam konteks teknologi digital. Pendekatan ini penting mengingat penggunaan sistem AI dapat melibatkan proses otomatis, namun tetap berada dalam kendali dan tanggung jawab pelaku. Dengan perumusan unsur delik yang adaptif, hukum pidana dapat merespons kejahatan *deepfake* secara lebih efektif tanpa mengabaikan prinsip asas legalitas.

b) Pembuktian dan Perlindungan Korban

Rekonstruksi delik pidana *deepfake* juga harus mengintegrasikan mekanisme pembuktian yang sesuai dengan karakteristik kejahatan berbasis teknologi. Pengakuan eksplisit terhadap alat bukti forensik digital dan peran ahli menjadi penting untuk menjamin efektivitas pembuktian di pengadilan. Tanpa pengaturan yang jelas, pembuktian perkara *deepfake* akan terus menghadapi hambatan teknis dan yuridis yang berpotensi melemahkan penegakan hukum.

Selain aspek pembuktian, delik *deepfake* yang direkonstruksi seharusnya memuat ketentuan yang menjamin perlindungan korban secara substansial. Pengaturan mengenai kewajiban penghapusan konten, hak atas pemulihan reputasi, serta akses terhadap rehabilitasi psikologis dan restitusi perlu diintegrasikan dalam norma pidana. Integrasi ini mencerminkan pendekatan hukum pidana yang tidak hanya berorientasi pada pelaku, tetapi juga memberikan perlindungan yang adil dan proporsional bagi korban kejahatan *deepfake*.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa hukum pidana Indonesia saat ini belum sepenuhnya mampu merespons kejahatan *deepfake* secara efektif, baik dari sisi perumusan delik pidana, pembuktian, maupun perlindungan korban. Ketiadaan delik pidana yang dirumuskan secara spesifik menyebabkan penerapan pasal-pasal yang ada bersifat analogis dan berpotensi menimbulkan ketidakpastian hukum, terutama dalam pembuktian unsur perbuatan dan kesalahan pelaku. Selain itu, karakteristik *deepfake* sebagai kejahatan berbasis kecerdasan buatan menghadirkan tantangan serius dalam pembuktian alat bukti digital dan keterlibatan pelaku, sementara mekanisme perlindungan korban masih bersifat terbatas dan belum terintegrasi secara memadai dalam sistem peradilan pidana.

Sehubungan dengan temuan tersebut, penelitian ini merekomendasikan perlunya rekonstruksi delik pidana *deepfake* yang adaptif terhadap perkembangan teknologi, dengan perumusan unsur delik yang jelas, pengakuan terhadap pembuktian forensik digital, serta integrasi mekanisme perlindungan dan pemulihan korban. Namun demikian, penelitian ini memiliki keterbatasan karena bersifat normatif dan belum didukung oleh data empiris mengenai praktik penegakan hukum di lapangan. Oleh karena itu, penelitian selanjutnya disarankan untuk mengombinasikan pendekatan normatif dan empiris guna mengkaji efektivitas penerapan norma pidana terhadap kejahatan *deepfake*, termasuk persepsi aparat penegak hukum dan pengalaman korban dalam sistem peradilan pidana.

DAFTAR REFERENSI

- Afif, M. (2025). Legal challenges of deepfake crimes in Indonesian criminal law. *Journal of Law and Technology*, 7(1), 45–60.
- Alfathoni, R., Pratama, A., & Lubis, F. (2025). Perlindungan korban pornografi deepfake dalam perspektif hukum pidana Indonesia. *Jurnal Hukum Pidana dan Kriminologi*, 6(2), 112–128.
- Ambos, K. (2021). *Treatise on international criminal law: Volume I – Foundations and general part*. Oxford University Press.
- Ashworth, A., & Horder, J. (2022). *Principles of criminal law* (9th ed.). Oxford University Press.
- Brenner, S. W. (2021). Cybercrime and the limits of traditional criminal law. *Journal of Criminal Law and Criminology*, 111(3), 589–624.
- Casey, E. (2020). *Digital evidence and computer crime* (4th ed.). Academic Press.
- Duff, R. A., Farmer, L., Marshall, S. E., Renzo, M., & Tadros, V. (2019). *The boundaries of the criminal law*. Oxford University Press.
- Gless, S., Silverman, E., & Weigend, T. (2023). Artificial intelligence and criminal responsibility. *Criminal Law Forum*, 34(1), 1–30.
- Husak, D. (2020). *Overcriminalization: The limits of the criminal law*. Oxford University Press.
- Putra, R. A., & Dewi, S. K. (2024). Urgensi pengaturan tindak pidana deepfake dalam hukum positif Indonesia. *Jurnal Legislasi Indonesia*, 21(3), 389–404.
- Prayoga, D. A., & Tuasikal, R. (2025). Pembuktian forensik digital dalam tindak pidana deepfake. *Jurnal Teknologi dan Hukum*, 8(1), 77–95.
- Rahayu, D., & Kuswandi, B. (2025). Digital evidence and criminal procedure reform in Indonesia. *Indonesian Journal of Criminal Law*, 5(2), 134–150.
- Simester, A. P., & Sullivan, G. R. (2021). *Criminal law: Theory and doctrine* (7th ed.). Hart Publishing.
- Syaputra, R., & Nuriyatman, E. (2025). Victim-oriented justice dalam kejahatan berbasis kecerdasan buatan. *Jurnal Viktimologi Indonesia*, 4(1), 25–41.
- Walklate, S. (2021). *Victimology: The victim and the criminal justice process* (2nd ed.). Routledge.