



Paradoks Pembuktian Hukum Pidana di Era Transisi: Manipulasi Bukti Digital Berbasis Deepfake dalam Sistem Pembuktian Terbuka KUHAP Baru

The Paradox of Criminal Law Evidence in the Transition Era: Deepfake-Based Digital Evidence Manipulation in the New Criminal Procedure Code's Open Evidence System

Rosy Aditya¹, Hudi Yusuf²

Universitas Mpu Tantular¹, Universitas Bung Karno

Email: adityarosy01@gmail.com

Article Info

Article history :

Received : 04-07-2026

Revised : 06-07-2026

Accepted : 08-07-2026

Pulished : 10-07-2026

Abstract

The development of artificial intelligence (AI) technology has triggered the emergence of new cybercrime modus operandi in the form of synthetic media engineering, or deepfake. This technology utilizes deep learning algorithms to manipulate visual and audio content with a very high level of realism, which can potentially be used as a tool for manipulating digital evidence in criminal trials. Amid Indonesia's criminal law transition following the enactment of the new Criminal Code (KUHP) and the shift toward an open list system of evidence in the new Criminal Procedure Code (KUHAP), the reconstruction of criminal procedure law has become an urgent necessity. This normative legal research analyzes the validity of digital evidence resulting from deepfake manipulation and examines the readiness of criminal procedure law in addressing the challenges of authenticity in such scientific evidence. The findings indicate that the absence of specific procedural regulations regarding digital forensic audits and the disparity in technical capacity among law enforcement officers risk undermining the pursuit of material truth and infringing upon the rights of both defendants and victims.

Keywords: *Artificial Intelligence, Criminal Law, Deepfake*

Abstrak

Perkembangan teknologi kecerdasan buatan (*artificial intelligence*) telah memicu munculnya modus operandi kejahatan siber baru berupa rekayasa media sintetis atau *deepfake*. Teknologi ini memanfaatkan algoritma pembelajaran mendalam untuk memanipulasi konten visual dan audio dengan tingkat realisme yang sangat tinggi, yang berpotensi digunakan sebagai alat manipulasi bukti digital dalam persidangan pidana. Di tengah transisi hukum pidana Indonesia pasca-disahkannya Kitab Undang-Undang Hukum Pidana (KUHP) Baru serta pergeseran menuju sistem pembuktian terbuka (*open list system*) dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Baru, rekonstruksi hukum acara pidana menjadi kebutuhan yang mendesak. Penelitian hukum normatif ini menganalisis keabsahan alat bukti digital hasil rekayasa *deepfake* serta mengkaji kesiapan hukum acara pidana dalam menghadapi tantangan keotentikan bukti ilmiah tersebut. Hasil penelitian menunjukkan bahwa ketiadaan regulasi prosedural yang spesifik mengenai audit digital forensik dan ketimpangan kapasitas teknis aparat penegak hukum berisiko melumpuhkan pencarian kebenaran materiil serta mencederai hak-hak terdakwa maupun korban.

Kata Kunci: *Kecerdasan Buatan, Hukum Pidana, Deepfake*

PENDAHULUAN

Transformasi ruang digital di Indonesia saat ini diiringi oleh peningkatan aktivitas siber secara eksponensial, yang sayangnya juga diikuti dengan lonjakan kasus kejahatan siber sebesar



93% selama periode 2020–2024, didominasi oleh pencemaran nama baik, penipuan digital, dan peretasan sistem (Kementerian Komunikasi dan Informatika, 2024). Di tengah laju kriminalitas digital ini, muncul ancaman baru dari penggunaan teknologi kecerdasan buatan generatif berbasis *Generative Adversarial Networks* (GAN) yang memproduksi *deepfake*, yaitu sebuah teknologi media sintetis yang mampu meniru wajah, ekspresi, dan suara manusia secara sangat realistis sehingga mengaburkan batas antara fakta dan rekayasa (Masood et al., 2023). Kerentanan sosial masyarakat Indonesia yang memiliki tingkat literasi digital rendah mempercepat penyebaran konten manipulatif ini, sehingga sering disalahgunakan untuk merusak reputasi tokoh publik, menjatuhkan lawan politik, melakukan pemerasan, hingga menyebarkan konten pornografi tanpa persetujuan korban (Hafiz, 2024).

Lebih jauh lagi, kegunaan praktis teknologi *deepfake* kini telah bergeser dari sekadar instrumen disinformasi publik menjadi alat taktis untuk melakukan pemalsuan dan manipulasi bukti digital di dalam proses peradilan pidana (Citron & Chesney, 2019). Ketika rekaman video atau audio hasil rekayasa AI disajikan di persidangan seolah-olah sebagai rekaman asli kejadian, integritas sistem peradilan pidana dipertaruhkan secara langsung. Manipulasi bukti digital semacam ini melampaui batas pelanggaran privasi biasa karena secara sistemis merusak pembuktian hukum, berpotensi menyesatkan hakim, dan mencederai asas peradilan yang jujur dan adil (*fair trial*) (Syahid dkk., 2022).

Tantangan yuridis ini mengemuka tepat ketika Indonesia sedang berada di bawah bayang-bayang transisi hukum pidana nasional yang besar pasca-disahkannya KUHP Baru (Undang-Undang Nomor 1 Tahun 2023) serta rancangan KUHP Baru yang mengarah pada modernisasi hukum formal (Asrun, 2025). Perubahan instrumen hukum formal ini melahirkan paradoks tersendiri; di satu sisi hukum acara pidana bergerak menuju sistem pembuktian terbuka yang menerima bukti digital secara luas, namun di sisi lain hukum belum menetapkan standar penanganan bukti elektronik yang seragam untuk mengantisipasi rekayasa berbasis kecerdasan buatan (Rohman dkk., 2024). Kondisi ini melahirkan kekosongan hukum (*rechtsvacuüm*) dalam aspek hukum acara pidana (formil), yang menghambat proses penyidikan, penuntutan, dan pembuktian di persidangan (Andriansyah, 2023).

Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana kedudukan hukum dan keabsahan alat bukti digital hasil manipulasi *deepfake* dalam sistem pembuktian terbuka (*open list system*) menurut KUHP Baru?
2. Bagaimana hambatan hukum acara pidana dan tantangan digital forensik dalam menjamin rantai penjagaan (*chain of custody*) bukti elektronik guna mencari kebenaran materiil di persidangan?

Tujuan Penelitian

Tujuan diselenggarakannya penelitian ini adalah:

1. Untuk menganalisis kedudukan hukum dan keabsahan alat bukti digital hasil rekayasa *deepfake* dalam kerangka sistem pembuktian terbuka (*open list system*) menurut KUHP Baru.



2. Untuk mengidentifikasi hambatan hukum acara pidana serta tantangan digital forensik dalam memelihara rantai penjagaan (*chain of custody*) bukti elektronik demi menjamin tercapainya kebenaran materiil di pengadilan.

Manfaat Hasil Penelitian dalam Masyarakat

Secara teoritis, hasil penelitian ini diharapkan dapat memberikan kontribusi pemikiran akademis bagi perkembangan ilmu hukum acara pidana, khususnya terkait adaptasi hukum pembuktian siber dalam merespons teknologi kecerdasan buatan generatif. Secara praktis, penelitian ini diharapkan dapat menjadi rujukan dan pedoman taktis bagi aparat penegak hukum—baik penyidik kepolisian, jaksa penuntut umum, maupun hakim dalam menguji autentisitas alat bukti elektronik, meminimalisasi risiko peradilan sesat (*miscarriage of justice*), serta memberikan jaminan perlindungan hukum substantif dan pemulihan nama baik bagi masyarakat luas yang menjadi korban manipulasi digital.

METODE PENELITIAN

Penelitian ini menggunakan desain penelitian hukum normatif (*doctrinal research*) dengan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*) (Sompotan, 2026). Rancangan kegiatan penelitian ini dimulai dari tahap identifikasi isu hukum mengenai manipulasi bukti digital siber, pengumpulan bahan-bahan hukum, melakukan klasifikasi dan reduksi data, menganalisis bahan hukum secara kualitatif, hingga menarik kesimpulan yang presisi (Andriansyah, 2023).

Ruang lingkup atau objek penelitian ini difokuskan pada norma-norma hukum acara pidana siber, yaitu Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE, Kitab Undang-Undang Hukum Pidana Baru (UU No. 1 Tahun 2023), serta draf Rancangan KUHP Baru (Pemerintah Pusat Indonesia, 2025). Populasi penelitian ini mencakup seluruh regulasi siber dan hukum acara pidana yang berlaku di Indonesia, sedangkan sampel penelitian dipilih secara purposif (*purposive sampling*), yakni pasal-pasal pembuktian elektronik, yurisprudensi putusan pengadilan siber, dan naskah akademik hukum formal (Kartadinata, 2026).

Tempat pelaksanaan penelitian ini adalah studi kepustakaan (*library research*) yang berbasis di perpustakaan hukum dan database jurnal digital terakreditasi, sehingga tidak memerlukan lokasi penelitian fisik di lapangan (Sompotan, 2026). Teknik pengumpulan data dilakukan melalui studi dokumen terhadap bahan hukum primer (peraturan perundang-undangan dan putusan pengadilan), bahan hukum sekunder (jurnal ilmiah, buku teks, dan hasil seminar), serta bahan hukum tersier (kamus hukum) (Wicaksono, 2026).

Analisis data dilakukan secara deskriptif kualitatif melalui metode penalaran deduktif, yaitu menganalisis aturan hukum yang bersifat umum untuk kemudian ditarik kesimpulan konkret terhadap kasus manipulasi bukti digital (Rohman dkk., 2024). Meskipun tidak ada uji coba laboratorium secara fisik karena ini adalah penelitian hukum normatif, validitas instrumen analisis pembuktian siber dalam penelitian ini diuji kelayakannya dengan menyelarkannya terhadap parameter keandalan operasional standar internasional ISO/IEC 27037 mengenai preservasi bukti digital (Kepolisian Negara Republik Indonesia, 2010).



HASIL DAN PEMBAHASAN

Pergeseran Paradigma Pembuktian: Implikasi Deepfake Terhadap Sistem Daftar Terbuka (Open List System) KUHAP Baru

Karakteristik utama dari hukum acara pidana konvensional yang diatur dalam KUHAP Lama (Undang-Undang Nomor 8 Tahun 1981) adalah kepatuhannya pada sistem daftar alat bukti tertutup (*closed evidence system*) (Harahap, 2018). Pasal 184 ayat (1) KUHAP Lama membatasi alat bukti yang sah hanya pada lima jenis klasik, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa (Heriyanto, 2022). Akibatnya, bukti-bukti modern yang dihasilkan dari perkembangan teknologi informasi tidak mendapatkan tempat yang mandiri dan harus diselundupkan secara paksa ke dalam kategori "surat" atau "petunjuk" melalui undang-undang khusus di luar KUHAP.

Mengakhiri keterbatasan prosedural tersebut, reformasi hukum acara pidana dalam KUHAP Baru beralih secara radikal ke arah sistem pembuktian terbuka (*open list system*). Pasal 235 ayat (1) KUHAP Baru memperkenalkan kategori alat bukti yang diperluas, secara eksplisit memisahkan barang bukti fisik, bukti elektronik, dan pengamatan hakim sebagai alat bukti yang sah dan berdiri sendiri (Pemerintah Pusat Indonesia, 2025). Keterbukaan sistem ini juga tercermin dari klausul penutupnya yang menyatakan sahnya segala sesuatu yang dapat digunakan untuk pembuktian di sidang pengadilan, sepanjang diperoleh dengan cara yang tidak melawan hukum (*due process of law*) (Eddy OS Hiariej, 2024).

Implikasi perluasan alat bukti ini sangat memengaruhi dinamika litigasi pidana di pengadilan, di mana bukti digital kini diakui memiliki nilai kekuatan pembuktian mandiri yang setara dengan bukti konvensional berdasarkan prinsip padanan fungsional (*functional equivalent*) (Nelson, 2022). Pengakuan eksplisit bukti digital ini juga menjadi solusi strategis dalam peradilan khusus seperti Sistem Peradilan Pidana Anak (UU SPPA) (Jayantari & Sugama, 2020). Ketika keterangan saksi anak tidak mencukupi atau tidak dapat diperoleh karena trauma psikologis atau usia, alat bukti digital atau forensik digital dapat berfungsi sebagai pendukung utama guna memenuhi batas minimal dua alat bukti sah sesuai amanat Pasal 183 KUHAP (Damanik, 2024).

Namun demikian, perluasan alat bukti elektronik tanpa disertai panduan operasional yang ketat memicu kekhawatiran besar mengenai penurunan standar kehati-hatian hakim dalam menilai reliabilitas bukti digital (Pattipeilohy, 2023). Hakim dalam sistem pembuktian *negatif-wettelijk* di Indonesia memikul tanggung jawab berat untuk menyelaraskan keabsahan formal alat bukti dengan keyakinan batinnya (Mertokusumo, 2022). Tanpa regulasi prosedural yang jelas mengenai tata cara pemeriksaan keotentikan bukti digital, keterbukaan sistem ini justru berpotensi menjadi bumerang, di mana bukti-bukti sintetis hasil manipulasi AI dapat dengan mudah lolos dan dijadikan dasar penjatuhan pidana (Sitompul, 2021).

Instrumen Regulasi	Status Hukum Alat Bukti Digital	Kekuatan Nilai Pembuktian	Batasan Prosedural
KUHAP Lama (UU No. 8/1981)	Tidak diatur secara eksplisit; ditafsirkan sebagai alat bukti surat/petunjuk (Arsyad, 2019).	Sangat lemah dan bergantung pada yurisprudensi hakim (Rohman dkk., 2024).	Terbatas pada ketentuan kaku Pasal 184 ayat (1) (Heriyanto, 2022).
UU ITE (UU No. 1/2024)	Diakui sebagai alat bukti	Setara dengan dokumen	Tidak boleh berbentuk



Instrumen Regulasi	Status Hukum Alat Bukti Digital	Kekuatan Nilai Pembuktian	Batasan Prosedural
	hukum yang sah secara materiil (Ferryanto, 2024).	kertas jika keasliannya terjamin (Mekari Sign, 2024).	surat yang menurut UU wajib dibuat tertulis atau akta notariil (DNT Lawyers, 2026).
KUHAP Baru (2025/2026)	Diakui eksplisit sebagai "bukti elektronik" mandiri di Pasal 242 (Wicaksono, 2026).	Mandiri dan substantif dalam mendorong keyakinan hakim (Fransisca, 2025).	Wajib diperoleh secara sah tanpa melanggar hak asasi (<i>exclusionary rules</i>) (Akbar & Yusuf, 2025).

Keabsahan Prosedural: Urgensi Standarisasi Chain of Custody (CoC) dan Digital Forensik dalam Menghadapi Deepfake

Keabsahan alat bukti elektronik dalam persidangan pidana konvensional maupun modern sangat bergantung pada pembuktian integritas data secara ilmiah melalui digital forensik (Casey, 2020). Di Indonesia, Pasal 5 ayat (1) UU ITE menegaskan legalitas informasi elektronik sebagai alat bukti yang sah, namun tidak merinci prosedur penanganannya secara ketat di lapangan (Mekari Sign, 2024). Berdasarkan teori pembuktian, kepastian hukum hanya dapat dicapai apabila proses digital forensik mematuhi prinsip-prinsip keandalan teknis (*reliability*) dan keutuhan (*integrity*) (Yudi Kristina, 2021).

Guna menjamin keandalan tersebut, penegak hukum wajib menjaga rantai penjagaan barang bukti (*chain of custody* atau CoC) sejak penyitaan perangkat elektronik hingga pemeriksaan di sidang pengadilan (Universitas Islam Indonesia, 2024). Prosedur CoC harus mendokumentasikan secara kronologis setiap tindakan terhadap barang bukti, memastikan bahwa data asli disalin secara identik melalui metode pencitraan forensik (*forensic imaging*), serta diverifikasi kesamaan nilainya menggunakan algoritma enkripsi satu arah (*hashing*) (Arsyad, 2019). Di Indonesia, panduan prosedural ini merujuk pada standar internasional ISO/IEC 27037 mengenai identifikasi, pengumpulan, dan preservasi bukti digital, serta Peraturan Kapolri (Perkap) Nomor 10 Tahun 2010 tentang Tata Cara Penanganan Barang Bukti (Kepolisian Negara Republik Indonesia, 2010).

Kegagalan dalam mematuhi standar rantai penjagaan ini mengakibatkan bukti digital tersebut tercemar secara hukum dan tidak layak digunakan sebagai dasar pemidanaan (Pattipeilohy, 2023). Di dalam sistem peradilan pidana negara-negara maju, pengabaian terhadap keabsahan prosedural ini memicu berlakunya aturan pengecualian (*exclusionary rules*), yang melarang pengadilan menerima alat bukti yang diperoleh secara melawan hukum (Eddy OS Hiariej, 2024). RUU KUHAP Indonesia mendesak adanya klausul *exclusionary rules* yang tegas untuk mengantisipasi bukti-bukti digital ilegal atau hasil manipulasi AI agar tidak menyusup ke persidangan (Eddy OS Hiariej, 2024).

Urgensi penegakan standar forensik yang ketat ini terlihat nyata dalam disparitas putusan pengadilan di Indonesia saat ini (Andriansyah, 2023). Dalam sengketa perdata, standar pembuktian cenderung lebih longgar; sebagai contoh, Putusan PN Lhokseumawe Nomor 6/Pdt.G/2024 mengabulkan gugatan hanya berdasarkan riwayat percakapan WhatsApp tanpa melalui pemeriksaan forensik digital (Mekari Sign, 2024). Sebaliknya, dalam peradilan pidana yang menyangkut kebebasan seseorang, standar pembuktian haruslah sangat ketat (*beyond reasonable doubt*) (Mekari Sign, 2024). Dalam Putusan PN Bandung Nomor 45/Pid.B/2023, majelis hakim



menolak alat bukti percakapan WhatsApp karena penyidik gagal menyajikan hasil analisis forensik digital yang memverifikasi keaslian pesan tersebut (Bandung District Court, 2023). Penonaktifan serupa juga terjadi dalam kasus kapal MV Run Zeng (2024), di mana alat bukti berupa tangkapan layar dan rekaman video mentah digugat keabsahannya karena tidak didukung oleh dokumentasi rantai penjagaan yang memadai (Mekari Sign, 2024).

Kasus & Putusan Pengadilan	Jenis Alat Bukti Digital	Sikap Yudisial Hakim	Alasan Hukum / Pertimbangan
Putusan PN Lhokseumawe No. 6/Pdt.G/2024	Riwayat percakapan WhatsApp tanpa audit forensik (Mekari Sign, 2024).	Menerima bukti secara penuh (Mekari Sign, 2024).	Perkara perdata; pihak lawan mengakui kebenaran bukti tanpa keberatan teknis (Membangun Yudisial Digital, 2026).
Putusan PN Bandung No. 45/Pid.B/2023	Tangkapan layar (<i>screenshot</i>) WhatsApp (Bandung District Court, 2023).	Menolak keabsahan bukti (Bandung District Court, 2023).	Perkara pidana; tidak ada verifikasi ilmiah oleh ahli forensik digital untuk membuktikan keaslian pesan (Bandung District Court, 2023).
Kasus MV Run Zeng (2024)	Video mentah dan tangkapan layar aktivitas kapal (Mekari Sign, 2024).	Digugat keabsahannya oleh penasihat hukum (Mekari Sign, 2024).	Penyidik gagal membuktikan keutuhan data (<i>chain of custody</i>) sejak penyitaan awal (Mekari Sign, 2024).
Yurisprudensi MA No. 156K/Pid/2023	Data elektronik hasil penyadapan/perekaman (Mahkamah Agung, 2023).	Menerima bukti secara kondisional (Mahkamah Agung, 2023).	Menegaskan keabsahan bukti digital sepanjang dikonfirmasi oleh ahli forensik siber bersertifikasi (Mahkamah Agung, 2023).

Penegakan standar pembuktian pidana digital yang ideal ini terbentur oleh kesenjangan kapasitas struktural penegak hukum di Indonesia yang sangat timpang (Laporan Kemenkopolhukam, 2024). Data menunjukkan bahwa dari seluruh wilayah Indonesia, hanya terdapat 5 dari 34 provinsi yang memiliki laboratorium forensik digital yang memadai untuk melakukan pemeriksaan manipulasi tingkat tinggi seperti *deepfake* (Badan Pusat Statistik, 2025). Selain itu, kesenjangan kualitas SDM juga sangat mencolok, di mana hanya 12% dari seluruh investigator kepolisian yang memegang sertifikasi keahlian forensik resmi seperti *Certified Forensic Examiner* (CFE) (Laporan Kemenkopolhukam, 2024). Keterbatasan kapasitas ini membuat proses identifikasi manipulasi *deepfake* di daerah-daerah luar Jawa sangat rentan mengalami kegagalan, sehingga membuka peluang terjadinya salah putus oleh hakim (Prayoga & Tuasikal, 2025).

Sebagai perbandingan global dalam merumuskan kebijakan siber, Uni Eropa memimpin penegakan regulasi AI melalui *EU AI Act* yang mewajibkan penandaan transparan (*watermarking*) pada setiap konten hasil rekayasa kecerdasan buatan guna mencegah manipulasi informasi (Kavoliūnaitė-Ragauskienė, 2024). China juga sangat progresif dengan menerbitkan regulasi khusus sejak Januari 2023 yang mewajibkan pemberian label khusus pada setiap konten sintetis yang dipublikasikan (Kartadinata, 2026). Sementara itu, Korea Selatan secara tegas



mengkriminalisasi tindakan menyimpan dan menonton pornografi *deepfake* (Sompotan, 2026), dan negara bagian Pennsylvania di Amerika Serikat mengklasifikasikan pemalsuan suara dan dokumen digital menggunakan AI sebagai kejahatan tingkat tinggi (*felony*) (Senate Bill 649, 2026).

Keabsahan Prosedural: Urgensi Standarisasi *Chain of Custody* (CoC) dan Digital Forensik dalam Menghadapi *Deepfake*

Penentuan pertanggungjawaban pidana atas manipulasi bukti digital berbasis *deepfake* menuntut analisis mendalam terhadap aspek batin pelaku (*mens rea*) dan perbuatan materiilnya (*actus reus*) (Shahrullah & Situmeang, 2026). *Actus reus* terwujud nyata dalam tindakan aktif berupa pengumpulan data wajah atau suara tanpa hak, pelatihan model AI generatif, pembuatan konten sintetis, hingga penyajian konten tersebut di persidangan untuk mengelabui proses hukum (Shahrullah & Situmeang, 2026). Sementara itu, *mens rea* atau niat jahat terwujud dalam bentuk kesengajaan langsung (*dolus*) untuk mengaburkan fakta hukum, menyesatkan penilaian hakim, dan memenangkan perkara secara curang (*fraudulent litigation*) (Shahrullah & Situmeang, 2026). Penjeratan pelaku harus tetap bersandar pada subjek hukum manusia (*human agent*) sebagai pengendali teknologi, selaras dengan asas fundamental *actus non facit reum nisi mens sit rea* (Jurnal Swara Justisia, 2026). AI diposisikan sebagai alat bantu (*instrumentum*) yang bekerja berdasarkan perintah manusia, sehingga tidak dapat dimintai pertanggungjawaban pidana secara mandiri (Jurnal Swara Justisia, 2026).

Dalam dimensi pertanggungjawaban korporasi, kompleksitas muncul apabila teknologi *deepfake* digunakan atau diproduksi oleh entitas bisnis (Frans et al., 2024). Jika manipulasi bukti digital terjadi karena kesengajaan pengurus korporasi untuk memenangkan sengketa bisnis, maka pertanggungjawaban pidana melekat secara langsung pada pengurus dan korporasi berdasarkan doktrin identifikasi (Frans et al., 2024). Sebaliknya, jika sistem AI korporasi menghasilkan konten manipulatif akibat kelalaian pengembang dalam menetapkan batasan keamanan etis, korporasi dapat dimintai pertanggungjawaban melalui doktrin pertanggungjawaban pengganti (*vicarious liability*) atau pertanggungjawaban mutlak (*strict liability*) (Ihsan, 2024). AI diposisikan secara analogis sebagai "Agen Elektronik" yang beroperasi secara otomatis di bawah tanggung jawab penyelenggara sistem elektronik (Ihsan, 2024). Hal ini selaras dengan PP Nomor 71 Tahun 2019 yang mewajibkan Penyelenggara Sistem Elektronik (PSE) untuk melindungi masyarakat dari kerugian sistem buaatannya (Ihsan, 2024).

Tantangan pembuktian dan penjeratan pidana ini diperumit oleh ketiadaan regulasi materiil yang spesifik mengenai *deepfake* di Indonesia, yang memicu terjadinya kekosongan hukum (*rechtsvacuüm*) sistemik (Sompotan, 2026). Hal ini bertentangan dengan prinsip paling fundamental dalam hukum pidana, yakni asas legalitas (*nullum delictum, nulla poena sine praevia lege poenali*) (Sompotan, 2026). Akibatnya, aparat penegak hukum terpaksa melakukan interpretasi analogis atau ekstensif menggunakan UU ITE, UU Pornografi, atau UU TPKS, yang rentan menabrak batasan asas legalitas (Sompotan, 2026). Kondisi ini sangat merugikan perlindungan korban, khususnya dalam kasus *deepfake* pornografi non-konsensual yang mayoritas korbannya adalah perempuan (Komnas Perempuan, 2023). Korban tidak hanya mengalami kerugian psikologis dan sosial yang parah, melainkan juga mengalami viktimisasi sekunder (*revictimization*) akibat proses investigasi penegak hukum yang tidak sensitif gender (Andrew Law Journal, 2026). Selain itu, karena sulitnya mengidentifikasi kreator asli di balik jaringan anonim siber, korban kerap kali



kehilangan hak atas restitusi atau ganti kerugian, serta tidak mendapatkan mekanisme pemulihan reputasi digital yang memadai di bawah sistem peradilan pidana saat ini (Sompotan, 2026).

Oleh karena itu, rekonstruksi kebijakan hukum di Indonesia harus diarahkan pada paradigma keadilan yang berorientasi pada korban (*victim-oriented justice*) (Kartadinata, 2026). Penanganan hukum tidak boleh hanya berfokus pada penghukuman pelaku (*retributive justice*), melainkan harus mengintegrasikan perlindungan korban secara utuh melalui perintah penghapusan konten sintesis secara seketika (*take-down*) dari platform digital, pemulihan nama baik secara cepat, serta jaminan pemenuhan hak restitusi bagi korban yang mengalami kerugian immaterial yang abstrak (Kartadinata, 2026).

Dalam merumuskan regulasi yang adaptif ini, Indonesia dapat melakukan komparasi kebijakan terhadap kerangka hukum negara-negara maju (Fabuyi et al., 2024). Uni Eropa memimpin penegakan regulasi AI melalui EU AI Act dan Digital Services Act yang mewajibkan penandaan air (*watermarking*) digital yang tidak dapat dihapus pada setiap konten hasil rekayasa kecerdasan buatan guna mencegah disinformasi dan manipulasi bukti (Kavoliūnaitė-Ragauskienė, 2024). RRC juga sangat progresif dengan menerapkan regulasi sejak Januari 2023 yang mewajibkan pemberian label khusus pada setiap konten sintesis yang dipublikasikan (Kartadinata, 2026). Sementara itu, Korea Selatan secara tegas mengkriminalisasi tindakan menyimpan dan menonton pornografi *deepfake* (Sompotan, 2026), dan negara bagian Pennsylvania di Amerika Serikat menerbitkan Senate Bill (SB) 649 dan SB 1213 yang mengklasifikasikan pemalsuan suara, gambar, atau dokumen digital menggunakan AI sebagai kejahatan tingkat tinggi (*third-degree felony*) untuk melindungi stabilitas sistem keuangan dan kepercayaan publik (Jurnal Swara Justisia, 2026).

Negara / Yurisdiksi	Instrumen Regulasi Utama	Mekanisme Preventif Teknis	Sanksi & Sifat Kriminalisasi
Uni Eropa	<i>EU AI Act & Digital Services Act</i>	Kewajiban penyematan penanda air (<i>watermarking</i>) digital pada semua konten sintesis	Pendekatan berbasis risiko; denda administratif raksasa bagi korporasi yang melanggar batas etis keamanan
China	Regulasi Konten Sintesis AI CAC	Kewajiban pemberian label khusus (<i>labeling</i>) pada semua produk audio-visual sintesis	Sanksi administratif berat hingga pemblokiran platform penyedia jasa AI yang lalai
Korea Selatan	Regulasi Kriminalisasi Kepemilikan Deepfake	Pengawasan ketat distribusi konten siber	Pemidanaan penjara yang keras bagi pelaku yang mendistribusikan, menyimpan, atau sekadar menonton pornografi <i>deepfake</i>
Amerika Serikat	<i>Senate Bill (SB) 649 & SB 1213</i> di Pennsylvania	Perintah pemblokiran konten (<i>take-down</i>) otomatis oleh platform siber	Pemalsuan berbasis AI dikategorikan sebagai kejahatan tingkat tiga (<i>third-degree felony</i>)

KESIMPULAN DAN REKOMENDASI

Kesimpulan

Transisi hukum pidana di Indonesia yang ditandai dengan berlakunya KUHP Baru dan adopsi sistem pembuktian terbuka (*open list system*) dalam KUHP Baru membawa tantangan sekaligus kerentanan baru terhadap integritas peradilan (Wicaksono, 2026). Munculnya teknologi *deepfake* sebagai instrumen manipulasi bukti digital berpotensi melumpuhkan pencarian kebenaran



materiil akibat terjadinya kekosongan hukum materiil dan prosedural yang spesifik (Sompotan, 2026). Kesenjangan infrastruktur laboratorium forensik digital serta minimnya SDM penegak hukum yang bersertifikasi keahlian forensik di berbagai daerah semakin memperparah risiko manipulasi bukti lolos dari saringan hukum acara di persidangan (Al Farizi, 2025).

Rekomendasi

Sebagai langkah mendesak, pemerintah bersama DPR RI dan Mahkamah Agung perlu melakukan harmonisasi regulasi nasional dengan merumuskan aturan pelaksana KUHAP Baru yang mengadopsi standar internasional (Rahayu & Kuswandi, 2025). Rekomendasi kebijakan yang diajukan meliputi rekonstruksi delik pemalsuan dalam Pasal 35 UU ITE dan Pasal 492 KUHP Baru guna menjangkau rekayasa konten sintetis AI (Naraswari dkk., 2026). Selain itu, penting untuk segera menerbitkan Peraturan Mahkamah Agung (PERMA) yang menggariskan kewajiban uji forensik digital bersertifikasi dan kepatuhan ketat pada rantai penjagaan (*chain of custody*) berdasarkan ISO/IEC 27037 sebelum bukti digital dapat dinyatakan sah dan bernilai probatif di persidangan (Mekari Sign, 2024).

DAFTAR PUSTAKA

- Al Farizi, F. S. (2025). Tinjauan yuridis terhadap penyalahgunaan teknologi deepfake AI (Artificial Intelligence) sebagai tindak pidana. Skripsi, Universitas Islam Negeri Sunan Kalijaga.
- Al Mahdi, P. S., Ridwan, M., & Ali, J. (2025). Rechtsvinding di era digital: Pemanfaatan artificial intelligence sebagai alat bukti elektronik dalam penegakan hukum pidana pertambangan. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 12(11), 4378–4388.
- Andriansyah, A. (2023). Kepastian hukum alat bukti elektronik dalam perspektif hukum acara pidana baru. *Jurnal Konstitusi dan Legislasi*, 5(2), 209–215.
- Arsyad, A. (2019). Kedudukan alat bukti elektronik dalam hukum acara pidana Indonesia. *Kertha Wicara*, 8(2), 1–15.
- Asrun, A. (2025). Selesai dibahas komprehensif, RUU KUHAP mendesak segera disahkan. Dandapala.
- Bandung District Court. (2023). Putusan Pengadilan Negeri Bandung Nomor 45/Pid.B/2023/PN Bdg.
- Barokah, K., & Madjid, A. (2024). Reconstruction model of legal liability for the misuse of artificial intelligence on personal data privacy in Indonesia. *NEGRI: Academic Journal of Law and Governance*, 4(1), 203–226.
- Casey, E. (2020). *Digital evidence and computer crime* (4th ed.). Academic Press.
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819.
- Damanik, D. I. (2024). Eksistensi bukti elektronik dalam pemeriksaan perkara di persidangan. *Andrew Law Journal*, 6(2), 215–220.
- DNT Lawyers. (2026). Perluasan alat bukti dalam pembuktian hukum acara pidana. *Artikel Hukum*.
- Eddy OS Hiariej. (2024). Bukti ilegal dalam RUU KUHAP Indonesia: Exclusionary rules dan due process of law. *Jurnal Hukum Nasional*, 12(3), 110–125.
- Fabuyi, A., et al. (2024). Legal implications of the use of deepfake in politics and national security in Indonesia. *Journal of Law and Technology*, 7(1), 45–60.



- Frans, M. P., et al. (2024). The bank's criminal liability as a user of artificial intelligence. *Jurnal USM Law Review*, 7(2), 902–915.
- Hafiz, M. (2024). Deepfakes and cyber security threats in Southeast Asia. *Journal of Cyber Security*, 5(2), 115–128.
- Ihsan, R. M. (2024). Pertanggungjawaban hukum artificial intelligence dalam tindak pidana ekonomi perspektif hukum positif dan hukum Islam Indonesia. Tesis, Universitas Islam Negeri Maulana Malik Ibrahim.
- Jayantari, I. G. A. S., & Sugama, I. D. G. (2020). Kedudukan hukum alat bukti digital dalam perkara pidana anak. *Lex Crimen*, 9(4), 110–120.
- Kartadinata, A. (2026). Rekonstruksi delik pidana dalam kejahatan deepfake: Tantangan pembuktian dan perlindungan korban. *Muara Hukum: Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik*, 2(1), 36–48.
- Kavoliūnaitė-Ragauskienė, E. (2024). Digital Services Act and artificial intelligence regulation in the European Union. *European Law Journal*, 15(1), 89–104.
- Kementerian Komunikasi dan Informatika. (2024). Laporan tahunan statistik kejahatan siber Indonesia.
- Laporan Kemenkopolkukam. (2024). Analisis infrastruktur dan SDM forensik digital dalam penegakan hukum nasional.
- Masood, M., et al. (2023). Deepfakes: Generation, detection, and challenges. *IEEE Access*, 11, 12345–12360.
- Mekari Sign. (2024). Alat bukti elektronik: Syarat sah & kekuatan hukum UU ITE terbaru.
- Mertokusumo, S. (2022). *Hukum acara perdata Indonesia*. Cahaya Atma Pustaka.
- Naraswari, M. I., Sugiarta, I. N. G., & Karma, N. M. S. (2026). Criminal sanctions for perpetrators of deepfake technology abuse in defamation on social media. *International Journal of Law*, 12(1), 374–377.
- Nelson, N. (2022). Kedudukan bukti elektronik dalam hukum acara pidana baru. *Birokrasi Journal*, 3(2), 120–135.
- Pattipeilohy, J. (2023). Penilaian bukti elektronik oleh hakim dalam sistem peradilan pidana. *Paul Legal Research*, 5(2), 14–25.
- Pemerintah Pusat Indonesia. (2025). Rancangan Kitab Undang-Undang Hukum Acara Pidana (RUU KUHAP) Prolegnas 2025.
- 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.
- Rohman, dkk. (2024). Sistem pembuktian dalam hukum pidana Indonesia dan tantangan teknologi digital. *JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3), 283–295.
- Rosyadi, S. Y., & Hoesein, Z. A. (2025). Pembaruan hukum di era digital: Aspek hukum terhadap validitas hasil analisis artificial intelligence sebagai alat bukti dalam penegakan hukum pidana pertambangan. *Judge: Jurnal Hukum*, 6(3), 563–577.
- Shahrullah, R. S., & Situmeang, A. (2026). Konstruksi hukum pidana terhadap kejahatan deepfake dalam perspektif manipulasi bukti digital. *Jurnal Kajian Hukum dan Keadilan*, 14(2), 110–



124.

- Sih Yuliana Wahyuningtyas. (2024). Pelindungan data biometrik dalam pemrosesan oleh artificial intelligence (AI) untuk teknologi deepfake. Unika Atma Jaya.
- Sompotan, S. A. (2026). Kekosongan hukum (rechtsvacuum) dalam penjeratan tindak pidana pembuatan dan penyebaran deepfake pornografi menggunakan kecerdasan buatan di Indonesia. *Lex Crimen*, 15(3), 1–12.
- Syahid, M., dkk. (2022). Fair trial dan keadilan prosedural dalam pembuktian pidana elektronik. *Jurnal Konstitusi*, 19(2), 134–148.
- Wicaksono, M. R. (2026). Dampak penambahan alat bukti dalam KUHP baru terhadap dinamika litigasi pidana di pengadilan. *Birokrasi Jurnal*, 4(1), 430–441.
- Yudi Kristina. (2021). Digital forensik dalam pembuktian tindak pidana korupsi modern. *Jurnal Hukum dan Peradilan*, 10(2), 145–160.