e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 13 No 1 Tahun 2026 Hal. : 29-36

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

EVALUASI KEDUDUKAN BARANG BUKTI DIGITAL DALAM PERKARA PIDANA DI ERA KECERDASAN BUATAN DAN DEEPFAKE DI INDONESIA

Urbanisasi, Atalla Mufid

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Tarumanagara

Abstrak

Perkembangan teknologi kecerdasan buatan dan kemunculan deepfake telah mengubah karakter pembuktian dalam perkara pidana, karena rekaman digital kini dapat dimodifikasi secara sangat realistis sehingga menimbulkan tantangan baru bagi sistem peradilan. Dalam konteks Indonesia, peningkatan penggunaan barang bukti digital tidak diimbangi dengan kepastian hukum yang memadai terkait keabsahan, autentikasi, dan kekuatan pembuktian data elektronik. Penelitian ini bertujuan untuk mengevaluasi kedudukan barang bukti digital dalam sistem pembuktian pidana Indonesia di tengah perkembangan AI dan deepfake. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa pengaturan mengenai alat bukti elektronik masih tersebar di berbagai undang-undang sehingga menimbulkan ketidaksinkronan antara KUHAP, UU ITE, UU PDP, dan KUHP baru. Selain itu, teknologi deepfake menyebabkan meningkatnya risiko manipulasi data digital sekaligus menimbulkan fenomena liar's dividend, yaitu ketika pelaku menyangkal bukti autentik dengan alasan rekayasa AI. Temuan lain menunjukkan bahwa proses autentikasi dan chain of custody barang bukti digital masih lemah akibat keterbatasan tenaga ahli forensik digital dan belum adanya standar nasional yang secara tegas merujuk pada praktik internasional. Dalam sistem negatief wettelijk, kelemahan autentikasi dapat mengganggu pembentukan keyakinan hakim karena bukti digital sangat mudah dimodifikasi tanpa deteksi kasat mata. Dengan demikian, penelitian ini menyimpulkan bahwa Indonesia perlu memperbarui kerangka regulasi dan memperkuat kapasitas forensik digital agar barang bukti digital memiliki kepastian hukum dan keandalan dalam proses pembuktian pidana.

Kata Kunci: Barang Bukti Digital, Deepfake, AI, Autentikasi, Pembuktian Pidana.

*Correspondence Address : urbanisasi@fh.untar.ac.id
DOI : 10.31604/jips.v13i1.2026. 29-36

PENDAHULUAN

Transformasi digital yang didorong oleh kemajuan internet, komputasi awan, dan kecerdasan buatan ("AI") telah mengubah cara manusia berkomunikasi, bekerja, dan bertransaksi, sekaligus menghadirkan bentuk-bentuk kejahatan baru yang sangat bergantung pada data dan sistem elektronik (Kerr & Earle, 2023). Salah satu perkembangan teknologi paling disruptif adalah munculnya deepfake, yaitu konten audio-visual yang dimanipulasi menggunakan teknik deep learning sehingga sanggup meniru wajah, suara, dan gestur seseorang secara sangat meyakinkan (Chesney & Citron, 2019). Di Indonesia, penggunaan barang bukti digital dalam perkara pidana meningkat seiring merebaknya kejahatan berbasis siber dan media sosial, seperti pencemaran nama baik online, penyebaran konten asusila, penipuan dalam jaringan, dan eksploitasi seksual berbasis digital. Informasi elektronik, percakapan di aplikasi pesan instan, rekaman CCTV, *log server*, dan metadata kini kerap menjadi bukti utama yang diajukan di pengadilan, meskipun Kitab Undang-Undang Hukum Acara Pidana ("KUHAP") sendiri tidak secara eksplisit mengenal istilah "alat bukti elektronik". Untuk mengisi kekosongan tersebut, Undang-Undang Informasi dan Transaksi Elektronik ("UU ITE") kemudian mengakui informasi elektronik dan/atau dokumen elektronik beserta cetakannya sebagai alat bukti hukum yang sah, sehingga menciptakan perluasan konseptual atas kategori "surat" dan "petunjuk" dalam Pasal 184 KUHAP.

Namun, kemunculan teknologi *deepfake* dan *voice cloning* membuat isu keabsahan, autentikasi, serta nilai pembuktian barang bukti digital menjadi jauh lebih kompleks. *Deepfake* dapat dipergunakan untuk membentuk rekaman palsu yang menggambarkan seolah-olah seseorang melakukan suatu perbuatan tertentu, padahal konten tersebut hanyalah hasil komposit algoritmik yang tidak pernah terjadi di dunia nyata, sehingga berpotensi menjerat individu yang tidak bersalah atau merusak reputasi dan privasi korban. Di sisi lain, maraknya fenomena *deepfake* juga menimbulkan apa yang dikenal sebagai "*liar's dividend*", yaitu fenomena ketika pelaku sesungguhnya justru memanfaatkan keberadaan deepfake untuk menyangkal rekaman yang sebenarnya autentik dengan dalih bahwa video atau audio tersebut juga merupakan hasil rekayasa AI.

Literatur hukum di Indonesia menunjukkan bahwa belum terdapat regulasi yang secara spesifik mengatur *deepfake* sebagai suatu tindak pidana tersendiri maupun sebagai kategori khusus barang bukti digital, sehingga penegak hukum cenderung mengandalkan ketentuan umum dalam UU ITE, UU Perlindungan Data Pribadi ("UU PDP"), Kitab Undang-Undang Hukum Pidana ("KUHP") lama, dan KUHP baru. Kekosongan pengaturan ini menimbulkan ketidakpastian hukum dalam hal: (1) bagaimana mengkualifikasi perbuatan menyebarkan *deepfake*; (2) bagaimana standar autentikasi dan verifikasi ketika *deepfake* diajukan sebagai barang bukti; dan (3) sejauh mana korban memperoleh perlindungan efektif terhadap pelanggaran privasi dan martabatnya.

Dalam konteks penegakan hukum, aparat penegak hukum di Indonesia menghadapi keterbatasan kapasitas digital forensics, baik dari segi jumlah tenaga ahli, ketersediaan laboratorium forensik, maupun standar operasional prosedur yang secara rinci mengatur tata cara penanganan barang bukti digital. Beberapa kajian menyoroti bahwa proses identifikasi, pelestarian, pengumpulan, analisis, dan pelaporan bukti digital kerap belum mengikuti *best practices* internasional, sehingga

berpotensi melemahkan integritas dan nilai pembuktian barang bukti yang diajukan ke persidangan. Tantangan ini diperberat oleh sifat bukti digital yang mudah dimodifikasi, mudah digandakan, dan sangat bergantung pada infrastruktur teknis yang sering kali tidak merata di berbagai wilayah Indonesia.

Di sisi lain, sistem pembuktian Indonesia menganut asas *negatif-wettelijk,* yang mensyaratkan bahwa keyakinan hakim dibangun atas dasar sekurang-kurangnya dua alat bukti yang sah menurut undang-undang dan keyakinan hakim yang logis. Penerapan asas ini dalam konteks barang bukti digital dan deepfake menimbulkan persoalan serius: bagaimana hakim dapat membangun keyakinan yang rasional jika alat bukti visual dan audio yang diajukan berpotensi merupakan hasil rekayasa algoritmik yang sulit terdeteksi, sementara ketentuan normatif belum menyediakan panduan autentikasi yang memadai. Berdasarkan uraian tersebut, tampak adanya kebutuhan mendesak untuk mengevaluasi kedudukan barang bukti digital dalam perkara pidana di Indonesia di tengah kemajuan teknologi AI dan *deepfake*, baik dari perspektif normatif, teoretis, maupun praktik peradilan.

Berdasarkan latar belakang di atas, penelitian ini merumuskan beberapa pertanyaan sebagai berikut:

1. Bagaimana pengaturan normatif mengenai alat bukti elektronik dan barang bukti digital dalam sistem hukum acara pidana Indonesia, terutama dalam kaitannya dengan KUHAP, UU ITE, UU PDP, KUHP baru, dan perkembangan RUU KUHAP?
2. Bagaimana tantangan autentikasi, verifikasi, dan penilaian barang bukti digital dalam perkara pidana yang melibatkan teknologi AI dan *deepfake* di Indonesia?
3. Bagaimana kedudukan barang bukti digital dalam sistem pembuktian *negatif-wettelijk* dan sejauh mana standar forensik digital internasional dapat dijadikan rujukan untuk memperkuat sistem pembuktian pidana Indonesia di era AI dan *deepfake*?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (*legal research*) dengan pendekatan perundang-undangan (*statute approach*), pendekatan kasus (*case approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk mengkaji KUHAP, UU ITE, UU PDP, KUHP baru, serta rancangan perubahan KUHAP dan peraturan teknis terkait barang bukti digital dan pembuktian elektronik. Pendekatan kasus dilakukan melalui analisis putusan pengadilan yang relevan dengan penggunaan alat bukti elektronik, rekaman video, rekaman suara, dan bukti digital lain dalam perkara pidana, termasuk kasus yang menyinggung keabsahan konten yang berpotensi hasil manipulasi digital. Pendekatan konseptual digunakan untuk menelaah doktrin hukum pembuktian, konsep *digital evidence*, *deepfake*, dan standar forensik digital internasional.

Bahan hukum primer dalam penelitian ini meliputi peraturan perundang-undangan, putusan pengadilan, dan dokumen kebijakan resmi yang berkaitan dengan alat bukti elektronik, perlindungan data pribadi, dan sistem pembuktian pidana. Bahan hukum sekunder mencakup artikel jurnal ilmiah nasional dan internasional, buku, laporan lembaga internasional tentang *digital forensics*, serta tulisan akademik yang membahas *deepfake* dan *AI-generated evidence*. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan indeks bibliografis yang membantu penelusuran referensi.

Data dianalisis secara kualitatif dengan menafsirkan ketentuan normatif, mengidentifikasi pola dalam putusan pengadilan, dan memadukan temuan-temuan tersebut dengan kerangka teori pembuktian dan forensik digital, sehingga diperoleh argumentasi yang sistematis untuk menjawab rumusan masalah.

HASIL DAN PEMBAHASAN

Pengaturan Normatif Alat Bukti Elektronik dan Barang Bukti Digital

Secara normatif, pengakuan terhadap bukti elektronik di Indonesia terutama bersumber dari UU ITE yang menyatakan bahwa informasi elektronik dan/atau dokumen elektronik beserta cetakannya merupakan alat bukti hukum yang sah dalam proses peradilan pidana. Ketentuan tersebut mendorong perluasan tafsir kategori alat bukti dalam KUHAP agar mampu mengakomodasi berbagai bentuk baru, seperti rekaman digital, email, pesan instan, transaksi keuangan elektronik, *log* sistem, dan rekaman jejak digital lainnya yang semakin lazim menjadi barang bukti dalam perkara siber maupun kejahatan konvensional (Kerr, 2005). Dalam praktik peradilan, interpretasi ini penting agar bukti digital tidak terpinggirkan akibat ketiadaan redaksi eksplisit dalam KUHAP, sehingga memastikan proses pembuktian responsif terhadap perkembangan teknologi.

UU PDP menambah dimensi baru dalam aspek pemrosesan bukti digital, dengan memperkuat regulasi terhadap data pribadi (Matheus & Gunadi, 2024), termasuk larangan pembuatan dan penyebaran data palsu, identitas digital palsu, serta penyalahgunaan biometrik yang relevan dalam konteks *deepfake* (Kusnadi, 2025). Ketentuan ini menjadi krusial dalam kasus ketika wajah, suara, atau data personal seseorang dimanipulasi tanpa persetujuan, menimbulkan potensi kerugian dan pelanggaran terhadap hak privasi yang dapat dianggap sebagai tindak pidana tambahan dalam proses litigasi digital (Vaccari & Chadwick, 2020).

KUHP terbaru mulai memasukkan pasal-pasal yang mengakui perkembangan kejahatan digital, dengan menyediakan ruang untuk pengaturan tindak pidana berbasis teknologi, namun masih terdapat kekosongan hukum mengenai definisi dan unsur-unsur spesifik dari tindak pidana deepfake (Maras & Alexandrou, 2019). Akibatnya, para penegak hukum hingga kini masih mengandalkan kategori pemalsuan, penghinaan, atau pelanggaran kesusilaan sebagai dasar penanganan kasus *deepfake*, yang dinilai oleh sejumlah kajian sebagai keadaan kekosongan hukum parsial (*rechtsvacuum*) yaitu ketidakpastian regulasi khusus yang dapat menyulitkan proses penegakan hukum dan pembuktian, serta mengurangi efektivitas perlindungan korban *deepfake* baik dalam aspek privat maupun dalam pembuktian tindak pidana.

Kondisi ini menuntut pembaruan dan harmonisasi peraturan perundang-undangan nasional agar dapat lebih responsif terhadap tantangan pembuktian digital evidence di era AI dan *deepfake*, termasuk perlunya pengakuan eksplisit kategori bukti digital dan rancangan mekanisme pemeriksaan, validasi, serta perlindungan hak korban dalam proses litigasi digital. Dengan pembaruan ini, proses pembuktian dan perlindungan korban *deepfake* diharapkan tidak lagi terhambat oleh ketidakjelasan hukum dan dapat berjalan efektif dalam sistem peradilan pidana nasional.

Tantangan Autentikasi dan Chain of Custody Barang Bukti Digital

Autentikasi barang bukti digital merupakan tahapan krusial dalam

proses pembuktian pidana, di mana penegak hukum harus memastikan bahwa data elektronik yang diajukan benarbenar berasal dari sumber yang diklaim, tidak mengalami perubahan, dan merupakan representasi akurat dari peristiwa hukum yang relevan (Pollitt & Whitcomb, 2021). Tantangan besar muncul dengan kehadiran teknologi *deepfake* dan rekayasa AI, karena pemalsuan konten digital dapat dilakukan dengan tingkat presisi tinggi sehingga rekaman video maupun suara sulit dikenali keasliannya oleh mata telanjang, bahkan oleh pengacara atau hakim yang berpengalaman (Chesney & Citron, 2019). Dalam banyak kasus, *deepfake* menuntut penerapan metode verifikasi tingkat lanjut yang menggabungkan analisis metadata, pemeriksaan *hash value*, deteksi artefak digital, serta pemeriksaan lintas platform untuk mengidentifikasi manipulasi algoritmik secara forensik (Maras & Alexandrou, 2019).

Praktik pembuktian di tingkat internasional hampir selalu mensyaratkan kolaborasi antara analisis teknis yang mendalam dan keterangan ahli forensik digital, ditambah konfirmasi melalui saksi atau evidensi digital lain yang bersifat *corroborative* (Brill et al., 2006). Namun, di Indonesia, keterbatasan jumlah ahli forensik digital, minimnya fasilitas laboratorium siber yang terakreditasi serta absennya regulasi standar membuat proses autentikasi kurang sistematis, sehingga potensi penerimaan barang bukti digital yang kualitasnya diragukan sangat tinggi (Manggala et al., 2024). Jika pengadilan menerima barang bukti digital tanpa verifikasi yang ketat, ada risiko tinggi kesalahan interpretasi dan salah putusan, khususnya dalam perkara berbasis rekaman audio-visual.

Chain of custody sebagai rangkaian dokumentasi yang menjamin integritas dan keamanan barang bukti digital semakin penting di era kejahatan siber yang melibatkan berbagai tahap perpindahan data ((Akmal et al., 2022); (Kerr, 2005)). Di negara-negara dengan regulasi matang, *chain of custody* sudah menjadi syarat formil, di mana setiap penyitaan, pemindahan, penyimpanan, hingga pengujian forensik wajib didokumentasikan secara detail dan dapat dipertanggungjawabkan di pengadilan (Brill et al., 2006). Di Indonesia, meskipun kepolisian dan kejaksaan telah mulai mengembangkan prosedur internal, absennya pengaturan eksplisit dalam undang-undang menyebabkan sebagian hakim kesulitan menilai apakah integritas bukti digital benar-benar terjaga sepanjang proses litigasi; terlebih jika ada keberatan dari pihak pembela terhadap keaslian dan keutuhan data digital yang diajukan sebagai bukti.

Penegakan standar *chain of custody* dan autentikasi bukan hanya soal prosedur administrasi, tetapi juga menentukan nilai, kedudukan, dan kekuatan barang bukti digital dalam memastikan keadilan proses peradilan pidana, terutama jika barang bukti tersebut digunakan sebagai penentu utama dalam sebuah kasus. Untuk itu, harmonisasi regulasi nasional dengan standar internasional secara mendesak diperlukan agar keadilan substansial benar-benar terwujud dalam proses pembuktian berbasis teknologi di era AI.

Kedudukan Barang Bukti Digital dalam Sistem Pembuktian *Negatif-Wettelijk*

Dalam sistem *negatif-wettelijk*, barang bukti digital dapat berfungsi sebagai salah satu dari minimal dua alat bukti yang diperlukan, asalkan diklasifikasikan ke dalam kategori alat bukti yang diakui dan dinilai layak oleh hakim. Misalnya, rekaman video dapat diperlakukan sebagai surat atau petunjuk, sementara laporan analisis

forensik digital dapat berada dalam ranah keterangan ahli. Dalam perkara yang banyak bergantung pada bukti digital, seperti kejahatan siber atau penyebaran konten *deepfake*, nilai pembuktian barang bukti digital sering kali sangat dominan, sehingga kualitas dan keandalannya menentukan arah putusan.

Masalah muncul ketika hakim membangun keyakinan terutama berdasarkan satu jenis bukti digital yang tampak meyakinkan secara visual atau audio, padahal secara teknis bukti tersebut belum teruji autentisitasnya secara memadai. Risiko salah putusan (*miscarriage of justice*) menjadi lebih besar apabila standar penilaian terhadap barang bukti digital tidak disertai skeptisisme yang proporsional dan pemahaman teknis minimum. Di sisi lain, jika setiap bukti digital selalu dicurigai sebagai *deepfake* tanpa analisis yang memadai, proses peradilan dapat buntu dan merugikan korban yang mengandalkan bukti digital untuk membuktikan tindak pidana yang dialaminya.

Relevansi dan Adopsi Standar Forensik Digital Internasional

Berbagai lembaga internasional dan asosiasi profesional telah mengembangkan pedoman mengenai penanganan *digital evidence*, yang menekankan prinsip integritas, keandalan, dan akuntabilitas dalam setiap tahap proses forensik. Pedoman tersebut mencakup kewajiban dokumentasi yang rinci, penggunaan perangkat lunak yang tervalidasi, penerapan metode yang dapat diuji ulang, dan penyusunan laporan yang dapat dipahami oleh hakim serta pihak lain di pengadilan (Horsman, 2020). Dalam beberapa tahun terakhir, fokus khusus mulai diberikan pada deteksi *deepfake* dengan memanfaatkan teknik analisis pola visual, audio, dan pembelajaran mesin. Pendekatan multimodal berbasis AI ini terus berkembang, namun belum sepenuhnya distandarkan dalam pedoman internasional (Ramadhan et al., 2022).

Indonesia belum secara eksplisit mengadopsi standar forensik digital internasional dalam regulasi tertulis, tetapi beberapa laboratorium forensik dan unit siber di institusi penegak hukum mulai mengacu pada praktik-praktik tersebut dalam prosedur internal dan pelatihan (Putra & Riyanta, 2025). Pengintegrasian standar internasional, seperti ISO/IEC 27037, ke dalam kebijakan nasional berpotensi meningkatkan kualitas penanganan bukti digital dan memberikan kerangka penilaian yang lebih kokoh bagi hakim dalam menilai barang bukti digital, terutama bukti yang melibatkan indikasi rekayasa AI.

SIMPULAN

Berdasarkan analisis normatif dan empiris terhadap perkembangan penggunaan barang bukti digital di Indonesia, kebutuhan utama yang muncul adalah pembaruan menyeluruh terhadap kerangka hukum acara pidana, khususnya KUHAP dan regulasi pelaksananya. Reformasi ini harus memuat definisi yang jelas mengenai barang bukti digital, kategori dan klasifikasi hukumnya, serta standar penilaian yang dapat dijadikan rujukan oleh hakim, jaksa, dan penyidik ketika berhadapan dengan bukti elektronik, termasuk rekaman yang berpotensi merupakan hasil rekayasa kecerdasan buatan. Dalam konteks tersebut, pengaturan tentang alat bukti elektronik yang selama ini tersebar di dalam UU ITE dan perlindungan data pribadi di dalam UU PDP perlu diintegrasikan secara eksplisit ke dalam sistem pembuktian pidana, sehingga tidak lagi terjadi fragmentasi pengaturan antara hukum acara dan hukum materiil, serta memberikan kepastian bahwa informasi elektronik, dokumen elektronik, dan

data pribadi yang diproses secara digital memiliki posisi yang tegas dalam struktur alat bukti

Di samping itu, urgensi untuk merumuskan aturan khusus maupun memperkuat pasal-pasal yang sudah ada terkait *deepfake* menjadi semakin nyata seiring meningkatnya penggunaan teknologi ini untuk kepentingan kriminal seperti pornografi non-konsensual, penipuan identitas, dan manipulasi opini publik. Deepfake tidak cukup hanya dipahami sebagai varian dari pemalsuan biasa, karena karakter teknologinya memungkinkan penyebaran masif dan dampak psikologis serta sosial yang jauh lebih luas. Oleh karena itu, perlu dirumuskan ketentuan yang secara khusus mengkualifikasi perbuatan membuat, menyimpan, dan menyebarkan deepfake tertentu sebagai tindak pidana, sekaligus menyediakan pedoman minimal autentikasi terhadap konten yang diduga hasil rekayasa AI sebelum dapat dijadikan dasar pembuktian. Pedoman ini penting agar hakim tidak semata-mata mengandalkan kesan visual atau audio, tetapi melakukan penilaian berbasis analisis teknis dan keterangan ahli yang memadai.

Penguatan kerangka regulasi tidak akan efektif tanpa peningkatan kapasitas aparat penegak hukum. Penyidik, penuntut umum, dan hakim memerlukan pelatihan teknis yang berkelanjutan mengenai cara kerja kecerdasan buatan, karakteristik deepfake, dan prinsip-prinsip digital forensics. Pelatihan ini bukan hanya terkait penggunaan perangkat lunak forensik, tetapi juga mencakup pemahaman konseptual tentang integritas data, autentikasi, dan risiko bias algoritmik, sehingga mereka mampu berkomunikasi secara efektif dengan para ahli forensik dan mengajukan pertanyaan yang tepat dalam proses pembuktian. Dalam kerangka tersebut, kerja sama dengan lembaga riset, perguruan tinggi, dan komunitas profesional di bidang keamanan siber menjadi penting, karena institusi-institusi tersebut umumnya lebih cepat mengikuti perkembangan teknologi dan dapat menyediakan dukungan ilmiah maupun laboratorium bagi penegak hukum.

Peran lembaga peradilan, terutama Mahkamah Agung, juga krusial untuk mengarahkan praktik pembuktian melalui pedoman atau surat edaran yang memberikan kerangka penilaian terhadap barang bukti digital. Pedoman tersebut dapat mengatur, misalnya, kewajiban untuk menjelaskan secara eksplisit dalam pertimbangan hukum putusan mengenai bagaimana suatu barang bukti digital diautentikasi, sejauh mana potensi manipulasi digital telah dipertimbangkan, dan bagaimana bukti tersebut dikaitkan dengan alat bukti lain. Dengan adanya kerangka yang lebih seragam, disparitas penilaian antar hakim dan pengadilan dapat diminimalkan, dan para pihak yang berperkara memperoleh gambaran yang lebih jelas mengenai standar pembuktian yang digunakan untuk menerima atau menolak bukti digital.

Indonesia perlu mendorong harmonisasi dengan standar forensik digital internasional guna memastikan bahwa praktik penanganan barang bukti digital sejalan dengan prinsip-prinsip global mengenai integritas dan keandalan bukti. Harmonisasi ini dapat ditempuh baik melalui adopsi langsung pedoman internasional ke dalam regulasi nasional, maupun dengan menyusun standar nasional yang mengacu pada prinsip-prinsip terbaik yang telah diakui secara luas di komunitas digital forensics. Integrasi prinsip-prinsip tersebut ke dalam hukum positif akan membantu membangun kepercayaan publik terhadap sistem peradilan pidana, karena menunjukkan

bahwa negara tidak hanya mengandalkan perangkat hukum lama untuk menghadapi tantangan baru, tetapi juga secara aktif menyesuaikan tata kelola pembuktian dengan dinamika teknologi AI dan deepfake. Dengan demikian, kedudukan barang bukti digital dalam perkara pidana di Indonesia diharapkan menjadi lebih jelas, kuat, dan adaptif, sekaligus tetap menjaga perlindungan hak asasi manusia dan keadilan substantif bagi semua pihak yang terlibat dalam proses peradilan.

DAFTAR PUSTAKA

Akmal, L., R, M., & Erdiansyah, E. (2022). Analisis Urgensi Pemeriksaan Digital Forensik pada Persidangan Tindak Pidana Informasi dan Transaksi Elektronik Perkara Melanggar Kesusilaan dan Relevansinya dengan Pertimbangan Hukum Hakim dalam Menjatuhkan Putusan. *Jurnal Online Mahasiswa (JOM) Bidang Ilmu Hukum*, *9*(2).

Brill, A. E., Pollitt, M., & Morgan Whitcomb, C. (2006). The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. *Journal of Digital Forensic Practice*, *1*(1), 3–11. https://doi.org/10.1080/15567280500541488

Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, *98*(1), 147–155.

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*, 100076. https://doi.org/10.1016/j.fsir.2020.100076

Kerr, O. S. (2005). Digital Evidence and the New Criminal Procedure. 105 Columbia Law Review 279 (2005). *Columbia Law Review*, *105*(279). https://doi.org/https://ssrn.com/abstract=594101

Manggala, B. S., Putri, A., Suzeeta, N. S., Zalfa, N., Marpaung, V. C., Natalia, I. H., & Nugroho, A. A. (2024). Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Kasus Penipuan Berkedok Investasi Online (Studi Kasus Doni Salmanan). *Media Hukum Indonesia (MHI)*, *2*(2), 295–301. https://doi.org/https://doi.org/10.5281/zenodo.11378972

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *JUSTISI*, *10*(1), 20–35. https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Putra, S. D., & Riyanta, S. (2025). Digital Forensic Governance Strategy in Indonesia to Realize The Credibility of Accountable and Efficient Public Law Enforcement Agencies. *Journal of Social Research*, *4*(7), 1316–1327. https://doi.org/10.55324/josr.v4i7.2600

Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, 162–168. https://doi.org/10.25299/itjrd.2022.8968