Krisnadwipayana University, Jakarta, Indonesia | 2715-243X (Print), 2962-6226 (Online)

JUSTICE Voice

Vol. 5 | No. 1 | 2026 | pp. 47-59
https://doi.org/10.37893/jv.v5i1.1367

Konstruksi Hukum Pidana Terhadap Kejahatan *Deepfake* Dalam Perspektif Manipulasi Bukti Digital

Suntarajaya Kwangtama Tekayadi [a,*], Saparudin Efendi [a], Muhammad Rosikhu [a]

[a] *Fakultas Hukum, Universitas Bumigora, Mataram, Indonesia*

Kata Kunci:

Bukti Digital; Deepfake; Hukum Pidana; Manipulasi Elektronik; UU ITE.

Riwayat artikel:

Naskah dikirim : 05-05-2026
Naskah disetujui : 01-06-2026
Terbit online : 06-06-2026

Abstrak: Perkembangan teknologi kecerdasan buatan telah melahirkan ancaman baru dalam ekosistem hukum digital, salah satunya berupa kejahatan *deepfake*. Teknologi *deepfake* yang memanfaatkan *Generative Adversarial Networks* (GAN) mampu menghasilkan konten audio-visual palsu yang secara visual hampir tidak dapat dibedakan dari konten asli. Kondisi ini menimbulkan potensi penyalahgunaan *deepfake* sebagai sarana manipulasi bukti digital dalam proses peradilan pidana. Artikel ini mengkaji konstruksi hukum pidana terhadap kejahatan *deepfake* melalui pendekatan normatif dengan menelaah peraturan perundang-undangan yang berlaku di Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya serta Kitab Undang-Undang Hukum Pidana (KUHP) baru. Hasil penelitian menunjukkan adanya kesenjangan regulasi yang signifikan dalam mengakomodasi karakteristik teknis *deepfake* sebagai bentuk kejahatan baru. Manipulasi bukti digital berbasis *deepfake* menimbulkan persoalan krusial dalam hukum pembuktian, yaitu melemahnya nilai autentisitas dan integritas alat bukti elektronik. Oleh karena itu, penelitian ini merekomendasikan pembangunan konstruksi normatif baru melalui perluasan penafsiran Pasal 35 UU ITE, kriminalisasi *deepfake* secara eksplisit dalam KUHP baru, serta penetapan standar forensik digital yang baku untuk menguji otentisitas bukti elektronik berbasis kecerdasan buatan.

Keywords:

Digital Evidence; Deepfakes; Criminal Law; Electronic Manipulation; The ITE Law.

Abstract: *The development of artificial intelligence technology has given rise to new threats within the digital legal ecosystem, one of which is deepfake-related crime. Deepfake technology, which utilizes Generative Adversarial Networks (GANs), is capable of generating fabricated audio-visual content that is visually almost indistinguishable from authentic material. This condition creates significant potential for the misuse of deepfakes as a means of manipulating digital evidence in criminal proceedings. This article examines the criminal law framework governing deepfake-related crimes through a normative legal approach by analyzing the applicable laws and regulations in Indonesia, particularly the Law on Electronic Information and Transactions (EIT Law) and its*

* corresponding author: suntarajaya@universitasbumigora.ac.id

amendments, as well as the new Criminal Code (KUHP). The findings indicate a significant regulatory gap in accommodating the technical characteristics of deepfakes as an emerging form of crime. Deepfake-based manipulation of digital evidence poses a critical challenge to the law of evidence, particularly by undermining the authenticity and integrity of electronic evidence. Therefore, this study recommends the development of a new normative legal framework through an expanded interpretation of Article 35 of the EIT Law, the explicit criminalization of deepfake-related conduct in the new Criminal Code, and the establishment of standardized digital forensic procedures for verifying the authenticity of AI-generated electronic evidence.

Article history:
Submitted : 2026-05-05
Accepted : 2026-06-01
Available online : 2026-06-06

Sitasi: Kwangtama Tekayadi, S., Efendi, S., & Rosikhu, M. Konstruksi Hukum Pidana Terhadap Kejahatan Deepfake Dalam Perspektif Manipulasi Bukti Digital. *Justice Voice, 5*(1), 47–59. https://doi.org/10.37893/jv.v5i1.1367

1. Pendahuluan

Revolusi Industri 4.0 dan perkembangan pesat kecerdasan buatan (*Artificial Intelligence*/AI) tidak hanya membawa kemajuan dalam bidang ekonomi dan sosial, tetapi juga melahirkan ancaman baru yang sebelumnya sulit dibayangkan dalam ranah hukum. Salah satu produk AI yang paling mengkhawatirkan dari perspektif hukum adalah teknologi *deepfake*, yaitu teknik manipulasi media digital yang memanfaatkan algoritma *deep learning* untuk menciptakan konten video, audio, atau gambar yang tampak autentik, padahal sesungguhnya merupakan hasil rekayasa digital (Farid, 2008). Fenomena ini menghadirkan tantangan fundamental bagi sistem hukum pembuktian yang selama ini bertumpu pada prinsip autentisitas dan integritas alat bukti.

Kemajuan teknologi *deepfake* ditenagai oleh arsitektur *Generative Adversarial Networks* (GAN) yang memungkinkan komputer mempelajari pola wajah, suara, dan gerak tubuh seseorang, kemudian mereproduksinya dalam konteks yang sepenuhnya berbeda. Penelitian Citron dan Chesney menunjukkan bahwa teknologi ini berpotensi digunakan untuk merusak reputasi, memanipulasi opini publik, hingga memalsukan bukti dalam proses hukum (Chesney & Citron, 2019). Lebih lanjut, Schick memperingatkan bahwa era *infocalypse*, yaitu banjir informasi palsu berbasis AI, sedang melanda peradaban manusia dengan implikasi hukum yang belum sepenuhnya dipahami (Schick, 2020).

Di Indonesia, kerangka hukum yang mengatur kejahatan siber termuat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya. Makarim menegaskan bahwa instrumen hukum telematika di Indonesia masih menghadapi tantangan besar dalam merespons dinamika perkembangan teknologi yang berlangsung jauh lebih cepat dibandingkan kemampuan legislasi untuk mengaturnya (Makarim, 2003). Ketiadaan norma hukum yang secara eksplisit mengatur *deepfake* sebagai tindak

pidana tersendiri menciptakan *vacuum legis* yang berpotensi menimbulkan berbagai permasalahan hukum, terutama ketika teknologi tersebut dimanfaatkan untuk memanipulasi bukti digital dalam proses peradilan.

Sejumlah penelitian terdahulu telah membahas fenomena *deepfake* dan AI-generated content dari berbagai perspektif, baik hukum maupun multidisipliner. Dalam konteks internasional, kajian yang dilakukan oleh Citron berfokus pada implikasi *deepfake* terhadap demokrasi dan keamanan nasional (Chesney & Citron, 2019), sementara penelitian lainnya lebih banyak menyoroti aspek regulasi konten digital, perlindungan privasi, serta kebebasan berekspresi. Di sisi lain, beberapa yurisdiksi, seperti Amerika Serikat dan Uni Eropa, mulai mengembangkan kerangka regulasi yang secara khusus mengatur *synthetic media*. Namun, pendekatan yang diterapkan masih beragam dan belum sepenuhnya menjangkau dimensi hukum pembuktian pidana.

Di Indonesia, penelitian mengenai *deepfake* umumnya masih terbatas pada isu pencemaran nama baik, pelanggaran privasi, dan etika penggunaan teknologi digital. Kajian yang mengaitkan *deepfake* dengan manipulasi alat bukti elektronik dalam sistem peradilan pidana masih sangat terbatas. Selain itu, belum banyak penelitian yang secara komprehensif memetakan kemungkinan penerapan hukum positif Indonesia, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) Baru Tahun 2026, dalam mengkualifikasikan *deepfake* sebagai bentuk tindak pidana yang berkaitan dengan pemalsuan atau manipulasi bukti digital.

Kebaruan penelitian ini terletak pada upaya membangun konstruksi hukum pidana yang secara spesifik menempatkan *deepfake* sebagai instrumen manipulasi bukti digital dalam perspektif sistem pembuktian pidana di Indonesia. Penelitian ini tidak hanya mengkaji *deepfake* sebagai fenomena pelanggaran yang terjadi di ruang siber, tetapi juga menghubungkannya secara langsung dengan prinsip-prinsip hukum pembuktian, seperti autentisitas, integritas, dan validitas alat bukti elektronik. Selain itu, penelitian ini mengintegrasikan pendekatan komparatif secara selektif untuk mengidentifikasi *best practices* dari berbagai negara yang relevan, kemudian mengontekstualisasikannya dengan karakteristik sistem hukum Indonesia, khususnya setelah berlakunya KUHP Baru.

Manipulasi bukti digital berbasis *deepfake* merupakan persoalan yang melampaui sekadar pelanggaran privasi. Ketika *deepfake* digunakan untuk memalsukan rekaman video sebagai alat bukti, memalsukan pernyataan seseorang, atau merekayasa keterangan saksi elektronik, teknologi tersebut secara langsung mengancam sendi-sendi sistem peradilan yang adil dan bermartabat. Citron dan Chesney menegaskan bahwa dampak *deepfake* terhadap integritas sistem pembuktian hukum dapat bersifat *irreversible* apabila tidak

segera diantisipasi melalui instrumen hukum yang memadai (Prayoga & Tuasikal, 2025).

Sejalan dengan pandangan tersebut, Arief mengingatkan bahwa kebijakan hukum pidana harus senantiasa berorientasi pada tujuan perlindungan masyarakat dan pencegahan kejahatan (Arief, 2001). Dalam konteks ini, konstruksi hukum pidana terhadap kejahatan *deepfake* menjadi urgensi akademik dan yuridis yang tidak dapat ditunda. Oleh karena itu, diperlukan telaah yang komprehensif mengenai bagaimana hukum positif Indonesia dapat diinterpretasikan dan dikonstruksikan untuk menjangkau perbuatan *deepfake*, khususnya yang berkaitan dengan manipulasi bukti digital.

Kajian mengenai kejahatan siber di Indonesia telah banyak dilakukan. Namun, penelitian yang secara khusus membahas konstruksi hukum pidana terhadap *deepfake* dalam perspektif manipulasi bukti digital masih sangat terbatas. Sebagian besar literatur hukum di Indonesia membahas *deepfake* dari perspektif pelanggaran privasi atau pencemaran nama baik, tanpa mengkaji secara mendalam implikasinya terhadap sistem pembuktian dalam hukum pidana. Di sisi lain, kajian hukum komparatif yang menganalisis pengaturan *deepfake* di berbagai negara belum banyak dikontekstualisasikan dengan sistem hukum Indonesia yang memiliki karakteristik tersendiri, terutama setelah berlakunya KUHP baru pada Tahun 2026. Penelitian ini berupaya mengisi kesenjangan tersebut dengan menawarkan konstruksi normatif yang sistematis dan komprehensif.

Penelitian ini bertujuan untuk: *pertama*, mengidentifikasi karakteristik yuridis kejahatan *deepfake* dalam perspektif hukum pidana Indonesia; *kedua*, menganalisis konstruksi hukum positif yang dapat diterapkan terhadap tindak pidana manipulasi bukti digital berbasis *deepfake*; dan *ketiga*, merumuskan rekomendasi normatif bagi pembaruan hukum pidana Indonesia dalam menghadapi ancaman kejahatan berbasis kecerdasan artifisial (*artificial intelligence*).

2. Metode

Penelitian ini menggunakan pendekatan penelitian hukum normatif (*normative legal research*). Menurut Soekanto dan Mamudji, penelitian hukum normatif merupakan penelitian hukum yang dilakukan dengan menelaah bahan pustaka atau data sekunder sebagai sumber utama penelitian (Mamudji & Soekanto, 2001). Dalam studi ini, penelitian hukum normatif difokuskan pada analisis substansi norma hukum positif yang berlaku, bukan pada praktik empiris penegakan hukum.

Marzuki menegaskan bahwa penelitian hukum normatif merupakan suatu

proses untuk menemukan aturan hukum, prinsip-prinsip hukum, dan doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi (Marzuki, 2010). Dalam konteks penelitian ini, peneliti berupaya menemukan konstruksi normatif yang tepat untuk merespons persoalan kejahatan *deepfake* yang belum diatur secara eksplisit dalam hukum positif Indonesia.

Pendekatan yang digunakan dalam penelitian ini meliputi: (1) pendekatan perundang-undangan (*statute approach*), yaitu pendekatan yang dilakukan dengan menelaah seluruh peraturan perundang-undangan yang berkaitan dengan isu hukum yang diteliti (Marzuki, 2010); (2) pendekatan konseptual (*conceptual approach*), yaitu pendekatan yang berangkat dari pandangan dan doktrin yang berkembang dalam ilmu hukum; serta (3) pendekatan perbandingan (*comparative approach*), yang digunakan untuk menelaah pengaturan kejahatan *deepfake* dalam sistem hukum negara lain sebagai bahan perbandingan normatif (Efendi dkk., 2016).

Selain itu, penelitian ini juga mengintegrasikan pendekatan futuristik atau *techno-legal approach* untuk memperkuat karakter interdisipliner dalam mengkaji perkembangan teknologi kecerdasan buatan beserta implikasinya terhadap hukum. Pendekatan ini tidak hanya menelaah norma hukum yang berlaku saat ini, tetapi juga mempertimbangkan perkembangan teknologi pada masa mendatang, khususnya dalam konteks *artificial intelligence*, *deepfake*, dan pembuktian digital (*digital evidence*). Dengan demikian, pendekatan ini memungkinkan peneliti merumuskan rekomendasi hukum yang adaptif, responsif, dan antisipatif terhadap dinamika perkembangan teknologi yang berlangsung secara cepat.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana, serta peraturan perundang-undangan terkait lainnya. Bahan hukum sekunder meliputi buku teks hukum, jurnal ilmiah hukum terakreditasi, dan artikel ilmiah yang berkaitan dengan kejahatan siber, pembuktian digital, serta kecerdasan buatan. Adapun bahan hukum tersier berupa kamus hukum dan ensiklopedia hukum.

Metode analisis yang digunakan adalah analisis preskriptif, yaitu metode yang bertujuan memberikan penilaian mengenai benar atau salah menurut hukum serta merumuskan apa yang seharusnya dilakukan berdasarkan ketentuan hukum yang berlaku.

3. Hasil dan Pembahasan

3.1. Analisis Unsur-Unsur Tindak Pidana dalam Kejahatan *Deepfake*

Untuk mengonstruksikan pertanggungjawaban pidana atas kejahatan *deepfake*, terlebih dahulu perlu dilakukan analisis terhadap unsur-unsur tindak pidana (*strafbaar feit*). Calo mengemukakan bahwa manipulasi digital pada dasarnya memenuhi unsur-unsur tindak pidana karena mengandung perbuatan yang dilarang, kesalahan pelaku, dan akibat yang menimbulkan kerugian (Calo, 2014).

Pertama, unsur perbuatan (*actus reus*). Pembuatan konten *deepfake* untuk tujuan memanipulasi bukti digital merupakan rangkaian tindakan aktif yang meliputi pengumpulan data wajah dan suara korban, pelatihan model kecerdasan buatan (*artificial intelligence*), sintesis konten palsu, serta penyebarannya. Wahid dan Labib menegaskan bahwa dalam kejahatan siber, rangkaian tindakan teknis tersebut secara keseluruhan membentuk satu kesatuan *actus reus* yang dapat dimintai pertanggungjawaban pidana (Wahid, 2005).

Kedua, unsur kesalahan (*mens rea*). Arief menekankan bahwa dalam tindak pidana siber, unsur *mens rea* atau niat jahat dapat berupa kesengajaan (*dolus*) untuk memanipulasi fakta hukum demi kepentingan tertentu (Arief, 2006). Dalam konteks *deepfake* sebagai alat manipulasi bukti, *mens rea* tercermin dalam niat pelaku untuk menggunakan konten sintetis sebagai alat bukti palsu dalam proses hukum guna menyesatkan hakim dan memperoleh kemenangan perkara secara tidak sah.

Ketiga, unsur melawan hukum (*wederrechtelijkheid*). Pemalsuan bukti digital berbasis *deepfake* pada hakikatnya bersifat melawan hukum karena bertentangan dengan kewajiban hukum untuk menyajikan bukti yang autentik dalam proses peradilan. Selain itu, perbuatan tersebut juga bertentangan dengan prinsip *fair trial* yang dijamin oleh hukum internasional maupun Konstitusi Indonesia. Berikut konstruksi normatif hukum pidana terhadap manipulasi bukti digital berbasis *deepfake*, yaitu:

a) Perluasan Tafsir Pasal 35 UU ITE

Pasal 35 UU ITE yang melarang manipulasi informasi dan dokumen elektronik agar dianggap seolah-olah autentik secara substantif pada dasarnya telah mencakup esensi perbuatan *deepfake* yang digunakan untuk tujuan pemalsuan bukti (Syahid dkk., 2022). Melalui penafsiran teleologis, frasa "memanipulasi" dalam Pasal 35 UU ITE dapat diinterpretasikan mencakup proses sintesis konten berbasis kecerdasan buatan (*artificial intelligence*/AI) yang menghasilkan representasi visual atau audio yang tidak autentik, tetapi tampak meyakinkan. Citron dan Chesney menegaskan bahwa pendekatan

penafsiran yang luas terhadap ketentuan yang telah ada merupakan langkah pragmatis yang diperlukan sembari menunggu pembentukan regulasi yang lebih khusus.

Namun demikian, penafsiran semata tidak cukup. Diperlukan perumusan norma yang lebih presisi agar tidak bertentangan dengan asas *lex certa* (kepastian hukum) dan asas legalitas dalam hukum pidana. Prinsip tersebut mensyaratkan bahwa rumusan tindak pidana harus dirumuskan secara jelas, tertulis, dan dapat dipahami oleh warga negara sebelum perbuatan tersebut dilakukan.

b) Kriminalisasi Eksplisit dalam KUHP Baru

KUHP baru yang akan berlaku efektif pada tahun 2026 memuat ketentuan mengenai pemalsuan dokumen dalam Pasal 263 dan Pasal 264 (Padang dkk., 2024). Prodjodikoro menjelaskan bahwa tindak pidana pemalsuan pada dasarnya merupakan perbuatan yang bertujuan menyesatkan orang lain mengenai kebenaran suatu fakta (Prodjodikoro, 2012). Dalam konteks tersebut, konten *deepfake* yang digunakan sebagai alat bukti dalam persidangan pada hakikatnya dapat dipahami sebagai bentuk pemalsuan, meskipun dilakukan melalui medium digital yang berbeda.

Dalam pandangan peneliti, diperlukan penambahan norma khusus dalam KUHP maupun UU ITE yang secara eksplisit mengkriminalisasi perbuatan membuat, mendistribusikan, atau menggunakan konten sintetis berbasis kecerdasan buatan (*artificial intelligence*/AI) untuk tujuan memanipulasi proses hukum. Adapun rumusan norma yang diusulkan adalah sebagai berikut:

> "Setiap orang yang dengan sengaja membuat, mendistribusikan, atau menggunakan konten digital yang dihasilkan melalui kecerdasan buatan atau teknologi sintesis lainnya sebagai alat bukti dalam proses hukum dengan tujuan menyesatkan penegak hukum atau hakim, dipidana dengan pidana penjara paling lama 15 tahun dan/atau denda paling banyak Rp15.000.000.000,00."

c) Standar Forensik Digital untuk Pengujian Autentisitas Bukti Elektronik

Mahkamah Agung RI melalui Peraturan Mahkamah Agung Nomor 1 Tahun 2024 tentang Pedoman Mengadili Perkara Pidana yang Menggunakan Alat Bukti Elektronik telah meletakkan dasar hukum bagi penanganan alat bukti elektronik di pengadilan. Namun, regulasi tersebut belum secara spesifik mengatur mekanisme verifikasi autentisitas terhadap konten yang berpotensi merupakan *deepfake*. Mason menegaskan bahwa *chain of custody* dan *forensic integrity* merupakan dua pilar utama dalam memvalidasi alat bukti elektronik (Mason & Seng, 2017).

Untuk mengatasi kelemahan tersebut, perlu ditetapkan standar forensik digital yang mencakup: (a) kewajiban verifikasi metadata dan tanda tangan digital terhadap setiap alat bukti elektronik yang diajukan dalam persidangan; (b) kewajiban pemeriksaan oleh ahli forensik digital bersertifikat yang diakui oleh lembaga negara; (c) penggunaan perangkat deteksi *deepfake* yang terstandarisasi dan telah tervalidasi secara ilmiah; serta (d) pembentukan lembaga sertifikasi forensik digital di bawah Puslabfor Polri yang berwenang memberikan keterangan ahli dalam perkara yang melibatkan alat bukti digital berbasis kecerdasan artifisial (*Artificial Intelligence*/AI).

Beberapa negara telah mengambil langkah konkret dalam mengatur teknologi *deepfake*. Sitompul mencatat bahwa perkembangan regulasi siber internasional dapat dijadikan acuan dalam pembaruan hukum di Indonesia. Amerika Serikat telah mengesahkan *DEEPFAKES Accountability Act* serta berbagai undang-undang di tingkat negara bagian yang secara khusus mengatur pembuatan dan penyebaran konten *deepfake*. Farid menegaskan bahwa deteksi *deepfake* dalam perspektif hukum memerlukan kombinasi antara regulasi yang kuat dan perkembangan teknologi forensik yang memadai.

Uni Eropa melalui *European Union Artificial Intelligence Act* (EU AI Act) yang disahkan pada tahun 2024 mengklasifikasikan sistem kecerdasan buatan yang digunakan untuk memanipulasi konten sebagai AI berisiko tinggi sehingga tunduk pada pengawasan ketat dan persyaratan transparansi (Dewi, 2011). EU AI Act mewajibkan adanya penandaan yang jelas terhadap konten yang dihasilkan oleh AI, suatu mekanisme yang sangat relevan untuk mencegah penyalahgunaan *deepfake* sebagai alat bukti dalam proses hukum. Sementara itu, China sebagai salah satu negara yang paling progresif dalam mengatur teknologi AI telah menerbitkan regulasi mengenai *deepfake* yang berlaku sejak Januari 2023, yang mewajibkan pemberian label khusus pada setiap konten sintetis.

Dalam perspektif perbandingan hukum tersebut, Indonesia perlu mengadopsi pendekatan regulasi yang komprehensif. Pendekatan tersebut tidak hanya bersifat reaktif melalui kriminalisasi terhadap penyalahgunaan *deepfake*, tetapi juga bersifat preventif melalui penerapan kewajiban pelabelan serta penetapan standar teknis yang jelas untuk penggunaan dan distribusi konten sintetis.

3.2. Implikasi *Deepfake* terhadap Sistem Peradilan Pidana dan Rekomendasi Kebijakan Hukum

Arief mengingatkan bahwa kebijakan hukum pidana (*penal policy*) merupakan bagian dari kebijakan sosial yang bertujuan melindungi sekaligus mewujudkan kesejahteraan masyarakat (Arief, 2006). Ancaman *deepfake* terhadap sistem peradilan bukan semata-mata ancaman terhadap individu,

melainkan juga ancaman terhadap keadilan sebagai institusi sosial yang fundamental.

Hamzah menegaskan bahwa asas legalitas dalam hukum pidana menghendaki setiap perbuatan yang diancam dengan pidana terlebih dahulu dicantumkan dalam undang-undang (Moeljatno, 2015). Dalam konteks ini, konstruksi hukum pidana terhadap *deepfake* seharusnya tidak hanya mengandalkan penafsiran ekstensif terhadap ketentuan yang telah ada, tetapi juga didukung oleh pembentukan norma baru yang secara eksplisit dan terukur mengatur kejahatan *deepfake*. Makarim juga menekankan pentingnya harmonisasi antara hukum nasional dan standar internasional dalam menghadapi kejahatan digital.

Berdasarkan analisis normatif dan komparatif yang telah dilakukan, penelitian ini merekomendasikan kebijakan hukum pidana terhadap kejahatan *deepfake* yang mencakup empat aspek. *Pertama*, aspek substansi hukum, yang meliputi perluasan rumusan Pasal 35 UU ITE agar secara eksplisit mencakup konten sintetis berbasis kecerdasan buatan (*artificial intelligence*), penambahan ketentuan khusus dalam KUHP baru mengenai pemalsuan bukti elektronik berbasis AI, serta pembentukan undang-undang khusus yang mengatur penggunaan AI dalam konteks hukum. *Kedua*, aspek struktur hukum, yang meliputi pembentukan unit khusus forensik digital di lingkungan Kepolisian Republik Indonesia, Kejaksaan Agung, dan Mahkamah Agung. *Ketiga*, aspek budaya hukum, yang meliputi penyelenggaraan program edukasi publik mengenai ancaman *deepfake* serta penguatan etika profesi hukum. *Keempat*, aspek kerja sama internasional, yang meliputi ratifikasi instrumen hukum internasional terkait kejahatan siber dan pengadopsian standar forensik digital internasional. Dalam konteks problematika pembuktian kejahatan *deepfake* dalam proses peradilan, keempat aspek tersebut merupakan satu kesatuan kebijakan yang saling melengkapi dalam upaya menjamin efektivitas penegakan hukum dan kepastian pembuktian.

Pembuktian tindak pidana *deepfake* menghadapi tantangan yang kompleks dalam sistem peradilan pidana Indonesia. Surahmad dalam kajiannya mengenai kedudukan alat bukti digital menegaskan bahwa verifikasi autentisitas alat bukti elektronik memerlukan perangkat teknis yang canggih serta keahlian khusus yang hingga saat ini masih terbatas di Indonesia (Tuahuns, 2025). Tantangan tersebut menjadi semakin krusial mengingat hakim sebagai garda terdepan penegakan keadilan pada umumnya belum memiliki kapasitas teknis yang memadai untuk menilai secara mandiri keaslian konten digital berbasis kecerdasan buatan (*Artificial Intelligence*/AI).

Rustamaji dalam penelitiannya mengenai rekonstruksi hukum pembuktian

digital mengidentifikasi tiga problematika utama, yaitu: *pertama*, kesenjangan teknologi antara pelaku kejahatan dan aparat penegak hukum; *kedua*, belum adanya standar baku dalam pembuktian digital; dan *ketiga*, keterbatasan sumber daya manusia yang memiliki kompetensi di bidang forensik digital (Reksodiputro, 2003). Ketiga problematika tersebut semakin diperparah oleh perkembangan teknologi *deepfake* yang berlangsung sangat cepat dan melampaui kapasitas respons sistem hukum dalam mengantisipasinya.

Selain itu, pada tataran implementatif, penggunaan alat bukti elektronik dalam praktik peradilan di Indonesia juga berpotensi menimbulkan persoalan terkait asas *due process of law* dan prinsip *fair trial*. Ketergantungan yang tinggi terhadap bukti digital tanpa disertai mekanisme verifikasi yang ketat dapat mengancam hak terdakwa untuk memperoleh peradilan yang adil, terutama apabila bukti tersebut tidak dapat diuji secara transparan dan akuntabel dalam persidangan. Dalam konteks ini, muncul pula permasalahan terkait prinsip *equality of arms*, yaitu kondisi ketika terdakwa tidak memiliki akses yang setara terhadap teknologi maupun keahlian yang diperlukan untuk membantah keabsahan alat bukti elektronik yang diajukan oleh penuntut umum.

Lebih lanjut, penggunaan alat bukti elektronik berbasis teknologi canggih, seperti AI dan *deepfake*, juga menimbulkan tantangan terhadap prinsip adversarial dalam hukum acara pidana. Hal ini disebabkan oleh potensi ketergantungan hakim yang berlebihan pada keterangan ahli tanpa memiliki kemampuan independen untuk menilai validitas teknis alat bukti tersebut. Kondisi demikian berisiko menciptakan *black box evidence*, yaitu situasi ketika proses pembentukan alat bukti tidak dapat dipahami secara utuh oleh para pihak di persidangan, sehingga mengurangi transparansi dan akuntabilitas proses pembuktian.

Oleh karena itu, diperlukan penguatan kerangka implementatif melalui pengaturan yang lebih rinci mengenai tata cara pengujian alat bukti elektronik. Pengaturan tersebut mencakup hak terdakwa untuk mengajukan pemeriksaan ahli tandingan (*counter-expert*), kewajiban keterbukaan metode forensik (*forensic disclosure*), serta penerapan standar pembuktian yang lebih ketat terhadap alat bukti digital yang dihasilkan atau dimodifikasi menggunakan teknologi AI. Langkah ini penting untuk memastikan bahwa penggunaan alat bukti elektronik tidak hanya sah secara formal, tetapi juga selaras dengan prinsip *due process of law* serta menjamin terpenuhinya *fair trial* dalam sistem peradilan pidana Indonesia.

Dalam rangka mengatasi problematika pembuktian tersebut, Widodo merekomendasikan pendekatan holistik yang memadukan pembaruan instrumen hukum dengan investasi pada kapasitas teknis lembaga penegak hukum (Widodo, 2009). Pandangan tersebut sejalan dengan pendapat Marzuki yang menyatakan bahwa perkembangan hukum harus senantiasa responsif terhadap perubahan

sosial dan teknologi (Marzuki, 2010). Selain itu, Reksodiputro menegaskan bahwa dalam era globalisasi, penegakan hukum pidana tidak dapat berjalan secara efektif tanpa dukungan kerja sama internasional yang kuat.

4. Simpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat ditarik beberapa kesimpulan. *Pertama*, kejahatan *deepfake* memiliki karakteristik teknis dan yuridis yang khas, yaitu kemampuannya menghasilkan konten audio-visual sintetis yang secara visual sulit dibedakan dari konten autentik. Karakteristik tersebut menjadikan *deepfake* sebagai ancaman serius terhadap integritas sistem pembuktian pidana yang bertumpu pada autentisitas dan reliabilitas alat bukti elektronik. Hukum positif Indonesia saat ini belum memiliki norma yang secara eksplisit dan komprehensif mengatur kejahatan *deepfake* dalam perspektif manipulasi bukti digital. Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan ketentuan yang paling relevan untuk digunakan, namun masih memerlukan perluasan penafsiran atau penegasan normatif yang lebih presisi agar mampu menjangkau seluruh dimensi perbuatan *deepfake*. Selain itu, ketentuan mengenai pemalsuan dokumen dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang baru juga masih perlu diperkuat melalui norma yang secara spesifik mengatur pemalsuan berbasis kecerdasan buatan (*artificial intelligence*).

Kedua, konstruksi hukum pidana yang tepat terhadap kejahatan *deepfake* dalam perspektif manipulasi bukti digital memerlukan pendekatan multidimensi yang mencakup perluasan norma melalui *legislative reform*, penetapan standar forensik digital yang baku, penguatan kapasitas institusional aparat penegak hukum, serta pengembangan kerja sama internasional yang efektif. Pembentukan norma hukum yang presisi dan standar forensik yang andal merupakan dua pilar utama dalam membangun konstruksi hukum pidana yang responsif terhadap ancaman *deepfake*. Dalam konteks tersebut, Indonesia perlu segera melakukan pembaruan legislasi dengan mengadopsi pendekatan regulasi yang komprehensif sebagaimana diterapkan oleh Uni Eropa melalui EU AI Act. Pendekatan tersebut tidak hanya bersifat reaktif dan represif, tetapi juga mengedepankan aspek preventif melalui kewajiban transparansi serta pelabelan konten sintetis berbasis kecerdasan buatan. Oleh karena itu, Pemerintah dan DPR RI perlu segera menyusun Rancangan Undang-Undang tentang Kecerdasan Buatan yang memuat ketentuan khusus mengenai larangan penggunaan konten sintetis dalam proses hukum, standar penandaan konten berbasis AI, serta mekanisme pertanggungjawaban pidana bagi pihak yang melanggarnya.

Daftar Pustaka

Arief, B. N. (2001). *Masalah Pengakan Hukum dan kebijakan Penanggulanganan Kejahatan*. Citra Aditya Bakti.

Arief, B. N. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Raja Grafindo Persada.

Calo, R. (2014). Digital Market Manipulation. *The George Washington Law Review*, *82*, 995.

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*, 1753.

Dewi, S. (2011). Cybercrime Dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional. *Masalah-Masalah Hukum*, *40*(4), 522–530. https://ejournal.undip.ac.id/index.php/mmh/article/view/13100

Efendi, J., Ibrahim, J., & Rijadi, P. (2016). *Metode Penelitian Hukum: Normatif dan Empiris*. Prenada Media.

Farid, H. (2008). Digital image forensics. *Scientific American*, *298*(6), 66–71. https://www.jstor.org/stable/26000642

Makarim, E. (2003). *Kompilasi Hukum Telematika*. Raja Grafindo Persada.

Mamudji, S., & Soekanto, S. (2001). *Penilitian Hukum Normatif (Suatu Tinjauan Singkat)*. Rajawali Pers.

Marzuki, P. M. (2010). *Penelitian Hukum*. Kencana Prenada Media Group.

Mason, S., & Seng, D. (2017). *Electronic Evidence*. University of London.

Moeljatno. (2015). *Asas Asas Hukum Pidana*. Rineka Cipta.

Padang, M. A., Siregar, B. J., & Rosmalinda. (2024). Keberpihakan Pemidanaan Dalam Undang-Undang Nomor 1 Tahun 2023. *Locus: Jurnal Konsep Ilmu Hukum*, *4*(2). https://jurnal.locusmedia.id/index.php/jkih/article/view/348

Prayoga, H., & Tuasikal, H. (2025). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia. *Abdurrauf Law and Sharia*, *2*(1), 22–38. https://doi.org/10.70742/arlash.v2i1.194

Prodjodikoro, R. W. (2012). *Asas-Asas Hukum Pidana*. Refika Aditama.

Reksodiputro, M. (2003). *Hak Asasi Manusia dalam Sistem Peradilan Pidana*. Pusat Pelayanan Keadilan dan Pengabdian Hukum UI.

Schick, N. (2020). *Deep Fakes and the Infocalypse: What You Urgently Need to Know*. Hachette.

Syahid, A., Sudana, D., & Bachari, A. D. (2022). Perundungan Siber (Cyberbullying) Bermuatan Penistaan Agama di Media Sosial yang Berdampak Hukum: Kajian Linguistik Forensik. *Semantik*, *11*(1), 17–32. https://doi.org/10.22460/semantik.v11i1.p17-32

Tuahuns, I. Z. (2025). Urgensi Kedudukan Hukum Pembuktian Alat Bukti dalam Praktik Peradilan Pidana Dihubungkan dalam Sistem Hukum Indonesia. *Bulletin of Law Research*, *2*(1), 21–28. https://doi.org/10.65344/bleach.v2i1.100

Wahid, A. (2005). *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama.

Widodo. (2009). *Sistem Pemidanaan dalam Cyber Crime*. Aswaja Pressindo.