Deepfake sebagai Sarana Pemerasan dalam Perspektif Hukum Pidana Indonesia

Rio Irandha Putra[1], Wahab Aznul Hidaya[2], Sokhib Naim[3]

[1] *Fakultas Hukum, Universitas Muhammadiyah Sorong*
E-mail: riocika2015@gmail.com
[2] *Fakultas Hukum, Universitas Muhammadiyah Sorong*
E-mail: wahabaznulhidaya@um-sorong.ac.id
[3] *Fakultas Hukum, Universitas Muhammadiyah Sorong*
E-mail: sokhib.naim@gmail.com

ABSTRACT

This research analyzes Indonesia's legal construction in addressing the misuse of deepfake technology in the criminal offense of extortion, examining both substantive criminal law and evidentiary aspects. The findings indicate that the extortion provision under Article 482 paragraph (1) of the National Penal Code is inadequate to address deepfake-based threats, as the element of "violence" is still interpreted as physical violence, making the offense of intimidation under Article 483 of the National Penal Code and Article 27B paragraph (2) of the Electronic Information and Transactions Law a more precise legal construction. A single act of deepfake-based extortion may even fall within the scope of four overlapping legal regimes simultaneously, namely the National Penal Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Pornography Law, which in turn generates normative fragmentation and threatens legal certainty as conceptualized by Jan Michiel Otto. With respect to evidentiary matters, Law Number 20 of 2025 concerning the Criminal Procedure Code retains the negative statutory system of proof (negatief wettelijke bewijstheorie) while expanding the categories of admissible evidence to nine types, including electronic evidence and judicial observation, both of which are particularly relevant in assessing the authenticity of AI-generated content. Nevertheless, the practical implementation of this evidentiary framework remains constrained by the limited number of certified digital forensic experts and the uneven distribution of accredited forensic laboratories. This research concludes that the core challenge lies not in the absence of applicable norms, but rather in the urgent need for harmonization across legal regimes and the strengthening of law enforcement's technical capacity.

Keywords**:** *Deepfake; Digital Extortion; Indonesian Criminal Law; Electronic Information and Transactions Law; Electronic Evidence; Artificial Intelligence*

ABSTRAK

Penelitian ini menganalisis konstruksi hukum Indonesia terhadap penyalahgunaan deepfake dalam tindak pidana pemerasan, baik dari aspek hukum pidana materiil maupun pembuktiannya. Hasil penelitian menunjukkan bahwa delik pemerasan dalam Pasal 482 ayat (1) KUHP Nasional tidak memadai menjangkau ancaman deepfake karena unsur "kekerasan" masih dimaknai sebagai kekerasan fisik, sehingga konstruksi yang lebih tepat justru ditemukan pada delik pengancaman dalam Pasal 483 KUHP Nasional dan Pasal 27B ayat (2) UU ITE. Satu perbuatan pemerasan berbasis deepfake bahkan berpotensi disentuh oleh empat rezim hukum sekaligus (KUHP Nasional, UU ITE, UU PDP, dan UU Pornografi), yang justru melahirkan fragmentasi norma dan mengancam kepastian hukum sebagaimana digagas Jan Michiel Otto. Pada aspek pembuktian, Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP tetap mempertahankan sistem pembuktian negatif (negatief wettelijke) namun memperluas alat bukti menjadi sembilan jenis, termasuk bukti elektronik dan pengamatan hakim, sekalipun penerapannya masih terkendala keterbatasan ahli forensik digital dan infrastruktur laboratorium. Penelitian ini menyimpulkan bahwa persoalan utama bukan terletak pada kekosongan norma, melainkan pada urgensi harmonisasi antarrezim hukum dan penguatan kapasitas teknis penegakan hukum..

Kata Kunci: *Deepfake*; Pemerasan Digital; Hukum Pidana Indonesia; Undang-Undang ITE; Pembuktian Elektronik; Kecerdasan Buatan

PENDAHULUAN

Memasuki dekade ketiga pada abad 21 ini teknologi berkembang begitu pesat, hal ini membawa begitu banyak perubahan yang signifikan terhadap pola kehidupan masyarakat.[1] Di Indonesia sendiri, perkembangan teknologi sejatinya merupakan perwujudan dari hak konstitusional warga negara dalam memanfaatkan ilmu pengetahuan sebagaimana dijamin dalam UUD NRI Tahun 1945 Pasal 28C Ayat (1) yang menegaskan bahwa setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, termasuk memperoleh manfaat dari ilmu pengetahuan dan teknologi demi meningkatkan kualitas hidupnya. Oleh karena itu, teknologi kini tidak hanya menjadi sarana pendukung aktivitas kita, tetapi juga telah bertransformasi menjadi bagian yang tidak terpisahkan dari kehidupan masyarakat modern. Kehadiran teknologi digital memberikan berbagai kemudahan dalam berbagai aspek baik dalam berkomunikasi, mengakses informasi, melakukan transaksi ekonomi, hingga menunjang berbagai aktivitas sosial lainnya secara lebih cepat dan efisien.

Artificial Intelligence (selanjutnya disebut AI) saat ini telah menjadi sorotan utama dalam perkembangan teknologi modern saat ini, karena dinilai mampu menghadirkan berbagai kemudahan dalam kehidupan. AI merupakan teknologi komputasi yang dirancang untuk meniru bagaimana manusia berpikir, dengan kemampuan pengolahan dan penyimpanan data yang jauh melampaui kapasitas manusia dalam membantu penyelesaian berbagai permasalahan.[2] Integrasi AI saat ini telah menyentuh hampir seluruh lini sektor strategis dan aktivitas harian masyarakat. Mulai dari penggunaan *generative* AI untuk membantu pekerjaan akademis dan profesional, algoritma rekomendasi di media sosial yang mengurasi informasi personal, implementasi *chatbots* dalam layanan konsumen, otomatisasi analisis data berskala besar di sektor industri dan kesehatan, hingga sekedar sebagai hiburan *editing* instan di kalangan masyarakat ramai. Hal ini menunjukkan bahwa AI bukan lagi sekadar wacana futuristik, melainkan sebuah realitas yang secara aktif mendefinisikan ulang cara manusia bekerja, berinteraksi, dan memproses informasi. Manifestasi paling mutakhir namun sekaligus kontroversial dari teknologi AI ini adalah AI berbasis manipulasi audio visual yang dikenal sebagai deepfake. Deepfake merupakan teknik sintesis citra manusia yang memanfaatkan teknologi deep learning untuk menggabungkan dan menumpangkan gambar, video maupun audio yang sudah ada ke sumber lain menggunakan algoritma seperti

[1] Anggil Syahra Putri Mecca, Wahab Aznul Hidaya, and Hadi Tuasikal, 'Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) Dalam Sistem Peradilan Pidana Di Indonesia', *Jurnal Sosial Teknologi*, 5.6 (2025), pp. 1–17 <http://sostech.greenvest.co.id/index.php/sostech/article/view/32207>.

[2] Ahmad Yani, 'Peran Artificial Intelligence Sebagai Salah Satu Faktor Dalam Menentukan Kualitas Mahasiswa Di Era Society 5.0', *Journal of Education Research*, 5.2 (2024), pp. 1089–96, doi:10.37985/jer.v5i2.963.

Generative Adversarial Networks (GANs).[3] Ini menghasilkan gambar, video dan audio yang tampak relistis dan sulit dibedakan dengan yang aslinya oleh mata manusia. Kendati pada awalnya teknologi ini diciptakan untuk tujuan inovasi dan hiburan, kemampuannya dalam merekayasa realitas kini kerap disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab sebagai instrumen kejahatan baru.[4]

PT Indonesia Digital Identity (VIDA) melalui VIDA *Where's The Fraud - Protecting Indonesia Business from* AI *Generated Fraud*, mencatat adanya lonjakan signifikan kasus penipuan berbasis *deepfake* di wilayah Asia Pasifik (APAC) yang mencapai 1550% selama periode 2023–2024.[5] Angka fantastis ini menegaskan bahwa ancaman manipulasi digital bukan lagi sekadar potensi di atas kertas, melainkan sebuah realitas kriminal yang masif berkembang. Di Indonesia sendiri, eskalasi penyalahgunaan teknologi ini kian mengkhawatirkan dengan menyasar berbagai ranah kehidupan. Mulai dari ruang publik melalui penyebaran disinformasi bermotif komersial dan politik, seperti rekayasa video pidato mantan Presiden Joko Widodo berbahasa Mandarin yang menimbulkan berbagai spekulasi di masyarakat, hingga pemalsuan video jurnalis Najwa Shihab dan berbagai figur publik untuk promosi ilegal. [6] [7] Namun, yang paling destruktif, yakni menyerang wilayah privat masyarakat sipil, seperti kasus meresahkan yang terjadi di Jawa Tengah, di mana seorang mahasiswa diproses hukum oleh pihak kepolisian setelah terbukti memanipulasi foto dan video sejumlah siswi SMA menjadi konten vulgar berbasis AI *deepfake* untuk disebarkan secara ilegal ke media sosial.[8]

Dalam kaitannya dengan hukum di Indonesia sendiri, kemunculan *deepfake* ini menimbulkan kompleksitas baru, teknologi ini tidak hanya menantang keaslian informasi, tetapi juga menciptakan sarana baru dalam berbagai tindak pidana, salah satunya adalah potensinya dalam pemerasan digital, sebuah modus yang sejatinya bukan hal baru di Indonesia, mengingat pemerasan berbasis konten intim non-konsensual (*cyber-extortion*) telah lama menjadi fenomena kriminal yang masif, namun kini berpotensi menyatu dengan teknologi *deepfake*. Sebagai refleksi atas ancaman tersebut, pada September 2025, sepuluh tokoh politik Malaysia, termasuk Menteri Komunikasi Fahmi Fadzil, mantan Menteri Ekonomi Rafizi Ramli, serta sejumlah anggota parlemen lainnya menjadi korban pemerasan menggunakan video seks *deepfake*. Para pelaku mengancam menyebarkan rekaman palsu tersebut ke publik apabila tebusan senilai 100.000 dolar AS tidak dibayarkan. Kasus ini tercatat sebagai pemerasan berbasis deepfake dengan jumlah korban pejabat publik terbesar dalam sejarah hukum pidana

[3] Hendra Prayoga and Hadi Tuasikal, 'Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia', *Abdurrauf Law and Sharia*, 1.2 (2024), pp. 22–38.

[4] Wayan Zenitia Devi, 'Implikasi Hukum Terhadap Penyalahgunaan Teknologi Deepkfake Untuk Pemerasan (Sextortion) Dalam Perspektif Hukum Teknologi Informasi Di Indonesia', *Majelis : Jurnal Hukum Indonesia*, 3.1 (2026), pp. 102–14, doi:10.62383/majelis.v3i1.1504.

[5] VIDA, 'VIDA, "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya', 2024.

[6] Verihubs, 'Kasus Deepfake di Indonesia: Prabowo dan Jokowi jadi Korbannya' (Verihubs, 2025).

[7] CNN In, 'Waspada Hoaks Iklan Judi Online, Najwa Shihab, Raffi, Atta Pakai AI' (CNN Indonesia, 2024).

[8] tvOneNews, 'Kasus Penyebaran Konten Deepfake Vulgar Dengan Korban Siswi SMA Naik Ke Penyidikan | TvOne' (YouTube, 2025).

Malaysia, hingga memaksa pemerintah negara tersebut meminta bantuan Google dalam proses investigasinya.[9]

Konvergensi antara teknologi manipulasi *deepfake* dan motif pemerasan siber ini layaknya bom waktu yang hanya menunggu momentum untuk meledak dalam peradilan pidana di Indonesia. Ketika modus pemerasan konvensional mulai mengadopsi *deepfake*, pelaku tidak lagi membutuhkan foto atau video asli korban untuk mengancam, melainkan cukup merekayasa wajah korban ke dalam konten buatan AI demi memeras sejumlah uang. Oleh karena itu, meskipun hingga saat ini belum tercatat kasus konkret yang secara spesifik melibatkan modus pemerasan berbasis *deepfake* di Indonesia, ketiadaan kasus tersebut justru menegaskan urgensi penelitian ini untuk melakukan analisis preventif-antisipatif sebelum momentum tersebut benar-benar tiba. Penulis akan menganalisis sejauh mana kesiapan instrumen hukum pidana Indonesia saat ini, baik dari segi pemenuhan unsur delik materiil, maupun mekanisme pembuktian formilnya di pengadilan, ketika modus pemerasan dalam konteks ini benar-benar terjadi di lapangan.

METODE

Artikel ini menggunakan penelitian hukum normatif dengan sifat preskriptif-analitis. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) untuk mengkaji pengaturan hukum pidana Indonesia terkait penggunaan teknologi *deepfake* sebagai sarana tindak pidana pemerasan serta problematika pembuktiannya. Pengumpulan data dilakukan melalui studi kepustakaan, dengan menelaah bahan hukum primer berupa peraturan perundang-undangan, serta bahan hukum sekunder berupa literatur hukum dan hasil penelitian terdahulu yang relevan. Data dianalisis secara kualitatif dengan metode deskriptif-analitis dan deduktif, yaitu menelaah norma hukum yang berlaku dan mengaitkannya dengan fenomena pemerasan berbasis *deepfake* untuk mengidentifikasi kesenjangan hukum dan implikasi yuridisnya.

PEMBAHASAN

Konstruksi Hukum Indonesia Terhadap Penyalahgunaan *Deepfake* dalam Tindak Pidana Pemerasan

Tindak pidana pemerasan di Indonesia merupakan fenomena klasik yang kuat berakar dalam dinamika sosial-ekonomi masyarakat, jauh sebelum teknologi mengaburkan batas-batas fisik kita.[10] Pada ranah konvensional, tindakan ini merefleksikan adanya relasi kuasa yang timpang, di mana pelaku mengeksploitasi rasa takut atau kerentanan korban demi keuntungan materiil yang melawan hukum. Di Indonesia sendiri kita dapat melihat fenomena ini hidup dalam realitas sehari-hari, mulai dari pungutan liar di jalanan, hingga kedok “biaya keamanan” disektor informal.

[9] Dinda Buana Putri, ‘Parlemen Malaysia Hadapi Gelombang Pemerasan Deepfake Porn, Desak Aturan AI’ (VOI, 2025).

[10] Gustitia Arleta, ‘Upaya Penindakan Pemberantasan Pungli Oleh Satgas Saber Pungli’, *Litigasi*, 20.1 (2019), pp. 148–71, doi:10.23969/litigasi.v20i1.1224.

Pengaturan hukum pidana Indonesia terhadap penggunaan teknologi *deepfake* sebagai sarana untuk melakukan tindak pidana pemerasan pada dasarnya bertumpu pada dua instrumen hukum utama, yaitu Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kedua instrumen ini menjadi fondasi normatif bagi aparat penegak hukum dalam menilai dapat tidaknya suatu perbuatan pemerasan yang dilakukan melalui media digital, termasuk yang memanfaatkan teknologi *deepfake*, dikualifikasikan sebagai tindak pidana.

Sebagai hukum pidana umum, KUHP memuat prinsip-prinsip dasar dan kaidah-kaidah fundamental yang menjadi rujukan utama dalam penegakan hukum pidana di Indonesia.[11] KUHP berfungsi sebagai payung hukum yang menetapkan kerangka normatif dasar bagi penanggulangan berbagai bentuk tindak pidana, termasuk kejahatan-kejahatan baru yang muncul sebagai konsekuensi dari perkembangan teknologi informasi dan komunikasi. Rumusan norma dalam KUHP pada umumnya bersifat terbuka (*open norm*) dan elastis, sehingga memungkinkan dilakukannya penafsiran secara dinamis seiring dengan perubahan sosial dan perkembangan modus kejahatan.[12] Karakter ini menjadi penting dalam menghadapi fenomena kejahatan berbasis AI seperti *deepfake*.

Tindak pidana pemerasan dalam KUHP diatur dalam Pasal 482 ayat (1) KUHP Nasional (UU Nomor 1 Tahun 2023), yang merupakan reformulasi dari Pasal 368 KUHP lama. Inti dari delik pemerasan terletak pada unsur "memaksa seseorang dengan kekerasan atau ancaman kekerasan" dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Unsur ini menimbulkan persoalan yuridis ketika dihadapkan pada praktik pemerasan digital berbasis *deepfake*. Secara normatif, unsur kekerasan atau ancaman kekerasan yang diartikan dalam Pasal ini adalah dalam artian fisik dan lahiriah, seperti ancaman dengan senjata.[13] R. soesilo juga mendefinisikan kekerasan sebagai tindakan menggunakan tenaga atau kekuatan jasmani tidak kecil dan tidak sah, misalnya memukul dengan tangan atau dengan segala macam senjata, menyepak, menendang, dan sebagainya.[14]

Deepfake dalam hal ini beroperasi sepenuhnya dalam ranah ancaman non-fisik dengan cara memanipulasi konten visual dan/atau audio sehingga tampak autentik dan meyakinkan. Ancaman penyebaran konten *deepfake* tidak menyerang tubuh fisik korban, melainkan menargetkan dimensi psikologis, reputasi, kehormatan, dan privasi korban. Dampak yang ditimbulkan dapat berupa tekanan mental yang ekstrem, ketakutan berkepanjangan, serta kehancuran identitas sosial dan profesional korban.

[11] Nia Ayu Mayang Sari, 'Kasus Pidana Diatur Dalam Kitab Undang Hukum Pidana Yang Dikaitkan Dengan Asas Legalitas Dalam Hukum Pidana', *IBLAM LAW REVIEW*, 6.1 (2026), pp. 10–17, doi:10.52249/ilr.v6i1.658.

[12] Ismaidar and others, 'Perkembangan Teori Penemuan Hukum Dalam Sistem Hukum Indonesia Berdasarkan Kitab Undang Undang Hukum Pidana (KUHP) Baru', *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3.6 (2025).

[13] Penjelasan Pasal 482 KUHP Nasional

[14] R Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya* (Politeia, 1996).

Apabila unsur kekerasan yang secara eksplisit dipahami sebagai kekerasan fisik, baik dalam definisi undang-undang maupun doktrin, maka ancaman penyebaran konten *deepfake* ini jelas tidak memenuhi unsur "kekerasan atau ancaman kekerasan" sebagaimana yang ada dalam Pasal ini. Ancaman tersebut tidak diarahkan pada penggunaan kekuatan fisik, maupun ancaman penggunaan kekuatan jasmani terhadap tubuh korban, melainkan pada konsekuensi sosial, psikologis, dan reputasional yang timbul akibat tersebarnya konten di ruang digital. yang berarti, objek yang diserang bukanlah integritas fisik korban, melainkan kehormatan, martabat, serta rasa aman korban di hadapan publik.

Oleh karena itu, sebagai upaya untuk mengatasi keterbatasan ini, relevansi hukum pemerasan berbasis *deepfake* sebenarnya juga dapat ditemukan secara lebih presisi pada Pasal 483 Ayat (1) KUHP Nasional yang mengatur mengenai tindak pidana pengancaman. Unsur utama dalam Pasal ini sama dengan tindak pidana pemerasan, yaitu:

a. Perbuatan materiilnya berupa tindakan memaksa;
b. Perbuatan memaksa ditujukan pada orang tertentu;
c. Tujuannya agar orang lain memberikan benda, utang, atau menghapus piutang; dan
d. Unsur kesalahannya menguntungkan diri atau orang lain dengan tindakan melawan hukum.

Namun, memberikan ruang lingkup yang lebih spesifik dengan menyertakan unsur "ancaman pencemaran atau pencemaran tertulis atau dengan ancaman akan membuka rahasia". Ancaman pencemaran sebagaimana dimaksud dalam Pasal ini memiliki relevansi yang kuat dengan modus pemerasan dengan *deepfake*. Ancaman untuk menyebarluaskan konten Deepfake yang menampilkan seolah-olah korban melakukan perbuatan tertentu yang bersifat memalukan, melanggar norma kesusilaan, atau merugikan reputasi sosialnya secara nyata merupakan bentuk dari ancaman pencemaran ini. Lebih lanjut, Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menempatkan diri sebagai *lex specialis* yang lebih adaptif dalam menanggapi dinamika kejahatan di ruang siber yang kian kompleks.

Sebagai instrumen hukum khusus, undang-undang ITE tidak hanya berfungsi untuk melengkapi kerangka hukum pidana umum, tetapi juga untuk melakukan spesialisasi norma terhadap perbuatan pidana yang memiliki karakteristik unik akibat penggunaan sarana elektronik. Keberadaannya memungkinkan penjangkauan yang lebih tepat dan presisi terhadap bentuk-bentuk kejahatan modern, termasuk pemerasan yang memanfaatkan teknologi *deepfake*.

Secara yuridis, konten *deepfake* dikualifikasikan sebagai Informasi Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 UU ITE, karena merupakan satu atau sekumpulan data elektronik yang diolah dan dimanipulasi sedemikian rupa sehingga memiliki makna dan dapat dipahami oleh orang yang menerimanya. Dengan demikian, ancaman penyebaran konten *deepfake* tidak hanya relevan untuk dianalisis melalui perspektif delik pemerasan dalam KUHP, tetapi juga tunduk pada rezim hukum UU ITE yang secara khusus mengatur integritas, penggunaan, dan penyalahgunaan informasi

elektronik. Dalam konteks ini, UU ITE menawarkan aturan yang lebih adaptif. Pengaturan yang paling relevan dalam Undang-Undang Nomor 1 Tahun 2024 terdapat dalam Pasal 27B, yang secara eksplisit mengatur tindak pidana pemerasan melalui media elektronik. Pasal ini membedakan pemerasan berbasis elektronik ke dalam dua bentuk ancaman yaitu:

a. Pasal 27B ayat (1): Melarang distribusi atau transmisi informasi/dokumen elektronik yang berisi ancaman kekerasan yang ditujukan untuk tujuan menguntungkan diri sendiri maupun orang lain (dengan memaksa memberikan barang, utang, atau menghapus piutang).
b. Pasal 27B ayat (2): Melarang perbuatan serupa namun dengan sarana ancaman pencemaran atau ancaman akan membuka rahasia.

Dalam kaitannya dengan pemanfaatan teknologi *deepfake*, Pasal 27B ayat (2) memiliki posisi yang sangat signifikan sebagai landasan hukum sebagaimana Pasal 483 KUHP Nasional. Ancaman untuk melakukan "pencemaran" dengan menggunakan konten *deepfake* secara jelas telah memenuhi unsur yang dirumuskan dalam pasal ini, meskipun materi yang dijadikan alat ancaman merupakan hasil rekayasa kecerdasan buatan dan bukan peristiwa yang benar-benar terjadi. Selain menjerat motif pemerasan, UU ITE juga mampu menjerat proses teknis di balik kejahatan *deepfake* melalui Pasal 35, Pasal ini melarang tindakan manipulasi, penciptaan, atau perubahan informasi elektronik dengan tujuan agar informasi elektronik tersebut dianggap seolah-olah data yang otentik. Hal ini sangat sesuai dengan sifat konten *deepfake* yang pada dasarnya adalah media manipulasi.

Secara teknis, *deepfake* pada umumnya dapat dibedakan ke dalam dua bentuk:[15] Pertama, face replacement atau face swap, yaitu teknik yang menggantikan wajah seseorang pada foto maupun video dengan wajah orang lain sehingga menghasilkan visual yang seolah-olah autentik. Kedua, *synthetic generation*, yaitu teknik yang tidak sekadar mengganti elemen tertentu, melainkan membangun gambar, video, maupun suara baru secara keseluruhan menggunakan model kecerdasan buatan berdasarkan data latih yang telah dipelajari sebelumnya.

kedua bentuk *deepfake* tersebut pada dasarnya telah memenuhi unsur memanipulasi maupun penciptaan Informasi Elektronik. *Face replacement* memenuhi unsur memanipulasi karena mengubah informasi elektronik yang telah ada sehingga menampilkan representasi yang berbeda dari keadaan sebenarnya. Sementara itu, *synthetic generation* memenuhi unsur penciptaan karena menghasilkan informasi elektronik baru yang sebelumnya tidak pernah ada.

Tidak berhenti pada KUHP Nasional dan UU ITE, konstruksi hukum terhadap pemerasan berbasis *deepfake* sesungguhnya juga bersinggungan dengan dua instrumen hukum lain yang relevan secara substantif, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi. Kedua instrumen ini, meskipun tidak dirancang secara spesifik untuk

[15] Baoping Liu and others, 'A Review of Deepfake and Its Detection: From Generative Adversarial Networks to Diffusion Models', *International Journal of Intelligent Systems*, 2025.1 (2025), p. 9987535, doi:https://doi.org/10.1155/int/9987535.

menjangkau fenomena *deepfake*, pada praktiknya dapat ikut teraktivasi tatkala unsur-unsur perbuatannya terpenuhi, sehingga menambah lapisan kompleksitas dalam menentukan konstruksi hukum yang tepat.

Dari sisi UU PDP, pembuatan konten *deepfake* pada dasarnya selalu diawali dengan proses pengambilan data wajah maupun suara, tanpa persetujuan yang sah dari pemilik data tersebut. Proses ini pada hakikatnya telah memenuhi unsur perolehan atau penggunaan data pribadi secara melawan hukum sebagaimana dilarang dalam UU PDP, Pasal 65 ayat (1) UU PDP mengancam setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi milik orang lain dengan maksud menguntungkan diri sendiri atau orang lain sehingga menimbulkan kerugian bagi subjek data.

Sementara itu, apabila konten *deepfake* yang dijadikan alat pemerasan bermuatan unsur kesusilaan atau seksual, ancaman penyebarannya dapat pula dikonstruksikan melalui UU Pornografi. Pasal 4 ayat (1) UU Pornografi melarang setiap orang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang memuat persenggamaan, kekerasan seksual, atau ketelanjangan, dengan ancaman pidana sebagaimana dirumuskan dalam Pasal 29. Sekalipun konten yang diancamkan sifatnya rekayasa dan tidak benar-benar terjadi pada peristiwa nyata, ancaman untuk menyebarluaskan visual yang menampilkan korban secara seolah-olah melakukan tindakan asusila tetap berpotensi memenuhi unsur perbuatan yang dilarang dalam UU ini, terutama bila pelaku turut mendistribusikan atau mengancam akan mendistribusikan konten tersebut kepada pihak ketiga.

Apabila ketiga peta regulasi tersebut disandingkan, KUHP Nasional dan UU ITE pada irisan pemerasan dan pengancaman elektronik, UU PDP pada irisan penyalahgunaan data pribadi sebagai bahan baku pembuatan *deepfake*, serta UU Pornografi pada irisan muatan kesusilaan konten yang diancamkan, maka tergambar jelas bahwa satu perbuatan pemerasan berbasis *deepfake* berpotensi disentuh oleh sedikitnya empat rezim hukum berbeda secara bersamaan. Kondisi inilah yang menurut hemat penulis justru menjadi persoalan utama dalam konstruksi hukum terhadap kejahatan ini. Tantangan yang dihadapi bukanlah ketiadaan norma yang dapat menjangkau perbuatan tersebut, melainkan sebaliknya, terlalu banyaknya norma yang berpotensi memunculkan fragmentasi norma, sehingga konstruksi hukum terhadap suatu peristiwa konkret sangat bergantung pada penafsiran dan preferensi aparat penegak hukum yang menanganinya. Satu penyidik atau jaksa dapat memilih untuk mengonstruksikan perbuatan tersebut sebagai pemerasan dalam KUHP Nasional, sementara penegak hukum lain pada kasus yang secara faktual serupa dapat memilih jalur Pasal 27B UU ITE, atau bahkan mengombinasikannya dengan UU PDP maupun UU Pornografi sekaligus. Variasi konstruksi yuridis semacam ini, meskipun masing-masing secara doktriner dapat dipertanggungjawabkan, pada gilirannya melahirkan inkonsistensi penegakan hukum yang mengancam terwujudnya kepastian hukum itu sendiri.

Jan Michiel Otto menekankan bahwa kepastian hukum yang nyata atau *real legal certainty* tidak cukup dipahami sekadar sebagai keberadaan hukum tertulis yang jelas secara normatif, melainkan harus memenuhi sejumlah unsur yang saling berkaitan, yaitu tersedianya aturan hukum yang jelas dan konsisten, diterapkannya aturan tersebut secara konsisten oleh instansi pemerintah yang juga tunduk terhadapnya, penyesuaian perilaku warga negara terhadap aturan tersebut, serta adanya hakim yang mandiri dan tidak memihak yang menerapkan aturan hukum secara konsisten ketika terjadi sengketa.[16]

Ketersediaan norma yang berlapis-lapis, meskipun secara kuantitatif tampak sebagai keunggulan sistem hukum karena memberikan banyak pintu masuk penjeratan pidana, justru tanpa adanya pedoman penerapan yang terpadu dapat melahirkan disparitas penegakan hukum antarwilayah maupun antarinstansi. Otto sendiri mengingatkan bahwa di negara-negara berkembang kerap terjadi jurang pemisah antara hukum di atas kertas atau *law on the books* dengan praktik penegakannya di lapangan atau law in action, sehingga kepastian hukum yang seharusnya hadir justru menjadi semu.[17] Apabila instansi penegak hukum tidak memiliki standar baku dalam menentukan konstruksi yuridis suatu perkara, maka yang terjadi adalah penggunaan diskresi yang tidak terukur, dan hukum kehilangan fungsinya sebagai panduan perilaku yang dapat diprediksi oleh masyarakat.

Pembuktian Terhadap Tindak Pidana Pemerasan Berbasis *Deepfake*

Pembuktian merupakan tahapan paling krusial dalam proses penegakan hukum pidana karena pada tahap inilah ditentukan terbukti atau tidaknya seorang terdakwa atas perbuatan yang didakwakan, sebagai inti dari peradilan pidana yang berfungsi mencari kebenaran materiil guna meyakinkan hakim dalam menjatuhkan putusan yang seadil-adilnya. Selama lebih dari empat dekade, hukum acara pidana Indonesia melalui Pasal 183 KUHAP lama secara tegas menganut sistem pembuktian negatif, yang mensyaratkan dua unsur kumulatif, yaitu sekurang-kurangnya dua alat bukti yang sah (unsur *wettelijk*) dan keyakinan hakim yang lahir dari alat bukti tersebut (unsur *negatief*), sehingga keyakinan hakim tidak boleh muncul secara subjektif murni tanpa disokong oleh alat bukti yang ditentukan undang-undang.[18]

Menariknya, dalam Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP yang berlaku sejak 2 Januari 2026, rumusan eksplisit sebagaimana Pasal 183 KUHAP lama tersebut tidak lagi ditemukan secara verbatim. Namun demikian, esensi keyakinan hakim tetap dipertahankan melalui frasa “terbukti secara sah dan meyakinkan” dalam Pasal 244 ayat (1) KUHAP baru, yang mensyaratkan bahwa keyakinan hakim untuk menjatuhkan sanksi pidana harus tetap lahir dari alat-alat bukti yang ditentukan dalam Pasal 235 KUHAP, sehingga secara substansial Indonesia tetap mempertahankan sistem pembuktian negatif menurut undang-undang (*negatief wettelijke bewijstheorie*).

[16] Shidarta, *Moralitas Profesi Hukum Suatu Tawaran Kerangka Berpikir* (PT Refika Aditama, 2006), p. 85.
[17] Emy Muginastiti and Edi Saputra Hasibuan, ‘Analisa Kepastian Hukum Terkait Pengaturan Surat Keterangan Bukan Pelaku Utama Sebagai Syarat Pengajuan Pembebasan Bersyarat’, *Syntax Literate: Jurnal Ilmiah Indonesia*, 11.5 (2026), pp. 4587–4603, doi:10.36418/syntax-literate.v11i5.64411.
[18] H S Brahmana, ‘Teori dan Hukum Pembuktian’ (Lhoksukon: Pengadilan Negeri Lhoksukon)

Perbedaan paling signifikan justru terletak pada perluasan jenis dan kualitas alat bukti itu sendiri: jika KUHAP lama hanya mengenal lima jenis alat bukti yang bersifat tertutup, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa, maka KUHAP baru memperluasnya menjadi sembilan jenis alat bukti, termasuk barang bukti, bukti elektronik, dan pengamatan hakim yang menggantikan kedudukan alat bukti petunjuk. Penggantian "petunjuk" menjadi "pengamatan hakim" dalam Pasal 235 ayat (1) huruf g ini bukan sekadar perubahan istilah, melainkan koreksi konseptual yang menyelaraskan hukum acara pidana Indonesia dengan standar observasi yudisial internasional, dan secara khusus relevan dalam menilai bukti elektronik yang melibatkan kecerdasan buatan, sebagaimana ditegaskan oleh Eddy O.S. Hiariej yang menyatakan bahwa pengamatan hakim berperan penting dalam menilai bukti hasil rekayasa AI, meskipun pengamatan hakim dan keyakinan hakim tetap merupakan dua hal yang berbeda secara fundamental, yang pertama berkedudukan sebagai alat bukti (*bewijsmiddel*) sedangkan yang kedua berkedudukan sebagai syarat pemidanaan (*voorwaarde voor veroordeling*).

Konteks teoretis ini yang menjadi kerangka analisis penting dalam memahami pembuktian tindak pidana pemerasan berbasis *deepfake*, sebab pembuktian dalam tindak pidana ini memiliki karakteristik yang bersifat ganda, disebut ganda karena dalam pemerasan berbasis *deepfake* hukum harus membuktikan dua aspek utama yaitu interaksi manusia berupa tindakan pemerasan sekaligus validitas teknis berupa rekayasa digital melalui kecerdasan buatan. Karakteristik ini memaksa sistem peradilan untuk tidak hanya melihat aspek niat jahat (*mens rea*) dan perbuatan (*actus reus*) secara konvensional, tetapi juga harus membedah integritas data digital yang menjadi instrumen kejahatan tersebut, sejalan dengan tuntutan unsur *wettelijk* dalam teori pembuktian negatif yang mensyaratkan keabsahan formil setiap alat bukti yang diajukan. Berdasarkan Pasal 235 ayat (1) huruf f KUHAP, bukti elektronik kini diakui sebagai alat bukti yang berdiri sendiri, yang dalam penjelasan pasalnya didefinisikan sebagai informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik, termasuk segala rekaman data berupa tulisan, gambar, suara, maupun tanda yang memiliki makna.[6] Pengakuan ini merupakan lompatan besar dalam hukum acara pidana, karena bukti elektronik tidak lagi sekadar diperlakukan sebagai perluasan dari alat bukti petunjuk sebagaimana dalam KUHAP lama, melainkan memiliki bobot pembuktian yang berdiri sendiri selama dapat dijamin keotentikannya.

Secara materiil, fokus utama pembuktian dalam tindak pidana ini tetap tertuju pada terpenuhinya unsur-unsur delik pemerasan, di mana penuntut umum harus mampu menunjukkan hubungan kausalitas antara pengiriman konten deepfake dengan paksaan yang dialami korban untuk menyerahkan sesuatu atau memberikan keuntungan bagi pelaku. Relevansi "kepalsuan" konten deepfake di sini bersifat sekunder terhadap delik pemerasan itu sendiri, artinya pemerasan dianggap tetap terjadi sekalipun ancaman tersebut didasarkan pada materi visual hasil rekayasa, sepanjang ancaman tersebut secara nyata memengaruhi kehendak bebas korban. Namun demikian, dari sisi formil, karakteristik pembuktian ini mewajibkan adanya proses autentikasi sebagaimana diamanatkan oleh Pasal 235 ayat (3) dan ayat (4) KUHAP, yang menegaskan bahwa alat bukti harus dapat dibuktikan autentikasinya dan diperoleh secara tidak melawan

hukum, sementara kewenangan untuk menilai keabsahan dan autentikasi alat bukti tersebut berada di tangan hakim.

Konsekuensi dari ketentuan ini ditegaskan lebih jauh dalam Pasal 235 ayat (5) KUHAP, yang menyatakan bahwa alat bukti yang dinyatakan tidak autentik dan/atau diperoleh secara melawan hukum tidak dapat digunakan sebagai alat bukti dan tidak memiliki kekuatan pembuktian. Mengingat *deepfake* adalah manifestasi dari manipulasi AI, pembuktian bahwa konten tersebut merupakan hasil rekayasa menjadi krusial bukan untuk membatalkan unsur pidana pemerasannya, melainkan untuk memenuhi prinsip kehati-hatian hakim dalam menilai sah atau tidaknya suatu alat bukti, sebagaimana dituntut oleh unsur *wettelijk* dalam teori pembuktian negatif itu sendiri, sebab tanpa pembuktian teknis yang jelas mengenai sifat *deepfake* dari konten tersebut, risiko terjadinya krisis kepercayaan terhadap bukti video secara umum dapat meningkat dan kredibilitas korban sebagai pihak yang dirugikan dapat ikut terancam.

Karakteristik pembuktian ini selanjutnya sangat bergantung pada penggunaan metode scientific crime investigation, metode penyidikan yang mengedepankan penerapan berbagai disiplin ilmu pengetahuan dalam proses pengungkapan suatu tindak pidana.[19] melalui peran strategis keterangan ahli forensik digital. Merujuk pada Pasal 229 ayat (1) KUHAP, kehadiran ahli forensik digital menjadi syarat mutlak untuk mengidentifikasi artefak manipulasi atau jejak algoritma yang tertinggal dalam konten deepfake, guna menjembatani keterbatasan pemahaman teknis aparat penegak hukum sekaligus memberikan keyakinan pada hakim, baik melalui jalur keterangan ahli sebagai alat bukti formal maupun melalui pengamatan hakim atas fakta-fakta teknis yang terungkap di persidangan, bahwa bukti elektronik yang diajukan benar-benar berasal dari transmisi pelaku.

Fokus utama pembuktian delik pemerasan tetap berpusat pada perbuatan mengancam dan niat jahat (*mens rea*) pelaku untuk menguntungkan diri sendiri secara melawan hukum sebagaimana diatur dalam Pasal 483 KUHP Nasional atau Pasal 27B ayat (2) UU ITE, sekalipun konten yang digunakan sebagai sarana ancaman bersifat palsu. Dalam kerangka teori pembuktian negative, terdapat dua lapis pembuktian yang harus disinkronkan untuk membentuk keyakinan hakim yang sah dan meyakinkan, yaitu pembuktian tindak pemerasan melalui persesuaian antara komunikasi ancaman dan ketakutan nyata atau kerugian yang dialami korban, serta pembuktian sifat konten untuk menunjukkan secara teknis bahwa materi tersebut benar merupakan *deepfake* sebagai indikator derajat itikad buruk pelaku yang lebih tinggi.

Sinkronisasi ini memerlukan persesuaian antara bukti digital komunikasi, keterangan saksi korban, keterangan ahli forensik digital, serta jejak transaksi digital seperti bukti transfer bank yang menguatkan adanya kerugian materiil, sehingga membentuk satu kesatuan alat bukti yang memenuhi unsur *wettelijk* sekaligus melahirkan keyakinan hakim yang memenuhi unsur negatief, sebagaimana dituntut oleh frasa “terbukti secara sah dan meyakinkan” dalam Pasal 244 ayat (1) KUHAP baru. Pada akhirnya, urgensi membuktikan kepalsuan konten *deepfake* dalam praktik persidangan memiliki implikasi

[19] Riza Sativa, ‘Scientific Investigation Dalam Penyidikan Tindak Pidana Pembunuhan’, *Jurnal Ilmu Kepolisian*, 15.1 (2021), pp. 57–67, doi:10.35879/jik.v15i1.295.

hukum yang krusial bagi perlindungan korban, sebab pembuktian tersebut bukan semata memperberat posisi hukum pelaku, melainkan juga berfungsi sebagai proteksi hukum bagi korban agar tidak dipersalahkan secara moral maupun hukum atas konten negatif.

Meskipun secara normatif hukum acara pidana Indonesia telah memberikan ruang pengakuan terhadap alat bukti elektronik dan keterangan ahli, penerapannya dalam praktik peradilan masih menghadapi berbagai kendala yang signifikan, yang pada gilirannya turut mempersulit pemenuhan unsur *wettelijk* itu sendiri. Kompleksitas teknologi AI yang digunakan dalam pembuatan *deepfake* menimbulkan kesulitan tersendiri karena sifatnya yang terus berevolusi, di mana setiap kemajuan dalam sistem deteksi kerap diikuti oleh kemajuan algoritma generatif yang lebih halus dan sulit diidentifikasi. Kesenjangan antara pesatnya kemajuan teknologi dengan ketersediaan kapasitas sumber daya manusia yang kompeten di bidang forensik digital juga menjadi kompleksitas. Izazi Mubarok Ketua sebagai Asosiasi Forensik Digital Indonesia sendiri mengakui bahwa jumlah sumber daya manusia ahli di bidang forensik digital di Indonesia masih sangat minim, sehingga penanganan kasus kerap memerlukan kerja sama lintas lembaga.[20] Kondisi serupa juga pernah diutarakan oleh praktisi forensik digital Soni Wirayudha, yang mencatat bahwa personel di pusat laboratorium forensik Polri yang menangani forensik komputer pada masanya hanya berjumlah sekitar dua puluh orang, padahal harus menganalisis barang bukti yang jumlahnya hingga ratusan.[21]

Persoalan keterbatasan sumber daya manusia ini turut diperparah oleh keterbatasan infrastruktur laboratorium yang terakreditasi, sebagaimana diungkapkan Sekretaris Utama Badan Standardisasi Nasional (BSN) dalam Seminar dan Musyawarah Nasional AFDI tahun 2024, yang menyebutkan bahwa hingga saat itu baru terdapat delapan belas laboratorium forensik di Indonesia yang telah diakreditasi oleh Komite Akreditasi Nasional (KAN) sesuai standar internasional ISO/IEC 17025.[22] Ketimpangan distribusi fasilitas semacam ini berpotensi menciptakan disparitas penegakan hukum antarwilayah, karena kecepatan penanganan kasus turut bergantung pada kedekatan geografis dengan fasilitas pengujian yang umumnya masih terpusat. Kendala pembuktian ini mencapai puncaknya pada masalah anonimitas dan tantangan lintas batas yurisdiksi, di mana pelaku dapat menyembunyikan identitas asli melalui penggunaan jaringan VPN, akun anonim, serta pemanfaatan server yang berlokasi di luar negeri guna mengaburkan jejak digital, sehingga penegak hukum berada dalam posisi terbatas untuk menelusuri identitas pelaku maupun mengumpulkan alat bukti, dan proses pembuktian kerap menghadapi risiko tidak terpenuhinya prinsip kepastian hukum dan efektivitas penegakan hukum.

Kendala-kendala ini menegaskan bahwa penegakan hukum terhadap tindak pidana siber tingkat lanjut tidak dapat dilakukan hanya dengan mengandalkan instrumen hukum yang bersifat reaktif, melainkan membutuhkan sinergi lintas sektoral yang mencakup

[20] 'Membangun Karier di Dunia Digital Forensik: Kebutuhan Talenta dan Jalur Sertifikasi' (Xynexis International, 2025).
[21] Mediana Yuliana, 'Profesi Menggiurkan di Era Digital', *Kontan Peluang Usaha* (Kontan, 2012)
[22] 'BSN Ingatkan Kembali Peran Standar untuk Penguatan Forensik Digital Indonesia' (Badan Standardisasi Nasional (BSN), 2023)

investasi pada pendidikan ahli forensik, perluasan akreditasi laboratorium di berbagai wilayah, serta penguatan perjanjian ekstradisi dan bantuan hukum timbal balik di tingkat internasional, agar sistem pembuktian negatif yang dianut hukum acara pidana Indonesia dapat benar-benar terpenuhi unsur formil maupun materiilnya dalam menangani kejahatan berbasis kecerdasan buatan.

Hukum pidana sebagaimana ditegaskan oleh Sudarto tidak hanya berfungsi sebagai alat penanggulangan kejahatan semata, tetapi juga harus mampu memberikan jaminan kepastian dan perlindungan hukum bagi seluruh lapisan masyarakat.[23] Pandangan ini mempertegas bahwa urgensi pembaharuan hukum terkait deepfake bukan hanya tentang menghukum pelaku, melainkan merupakan upaya sistemik untuk menjamin keamanan digital, menjaga martabat individu, serta melindungi hak privasi warga negara dari segala bentuk penyalahgunaan teknologi AI. Tanpa kebijakan strategis yang komprehensif untuk mengatasi hambatan struktural dan teknis ini, perlindungan terhadap hak digital warga negara akan tetap rentan terhadap eksploitasi teknologi AI di masa depan.

SIMPULAN

Konstruksi hukum Indonesia terhadap penyalahgunaan deepfake dalam tindak pidana pemerasan menunjukkan bahwa delik pemerasan konvensional dalam Pasal 482 ayat (1) KUHP Nasional tidak cukup memadai untuk menjangkau modus ini karena unsur kekerasan masih dimaknai secara fisik, sehingga jeratan yang lebih relevan justru ditemukan pada delik pengancaman dalam Pasal 483 KUHP Nasional dan Pasal 27B ayat (2) UU ITE; namun keterlibatan banyak rezim hukum sekaligus, yaitu KUHP Nasional, UU ITE, UU PDP, dan UU Pornografi, justru menimbulkan fragmentasi norma yang membuat konstruksi hukum terhadap suatu peristiwa konkret sangat bergantung pada penafsiran dan preferensi aparat penegak hukum, sehingga melahirkan disparitas penegakan hukum antarwilayah. Persoalan ini berlanjut pada tahap pembuktian, di mana Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP telah membawa kemajuan melalui pengakuan bukti elektronik dan pengamatan hakim sebagai alat bukti yang berdiri sendiri, sehingga memberikan ruang yang lebih adaptif dalam menilai keotentikan konten hasil rekayasa kecerdasan buatan, namun implementasinya di lapangan masih terhambat oleh keterbatasan jumlah ahli forensik digital tersertifikasi serta ketimpangan distribusi laboratorium forensik yang terakreditasi. Dengan demikian, penanggulangan tindak pidana pemerasan berbasis deepfake di Indonesia tidak cukup hanya mengandalkan ketersediaan norma hukum yang berlapis-lapis, melainkan menuntut harmonisasi konstruksi hukum antarrezim serta penguatan kapasitas kelembagaan dan infrastruktur forensik digital, agar kepastian hukum yang substantif dapat terwujud dan hukum pidana mampu menjalankan fungsinya sebagai instrumen perlindungan bagi korban penyalahgunaan teknologi kecerdasan buatan.

REFERENSI

Arleta, Gustitia, 'Upaya Penindakan Pemberantasan Pungli Oleh Satgas Saber Pungli', *Litigasi*, 20.1 (2019), pp. 148–71, doi:10.23969/litigasi.v20i1.1224

[23] Sudarto, *Hukum dan Hukum Pidana* (Alumni, 1986), p. 15.

Brahmana, H S, 'Teori dan Hukum Pembuktian' (Pengadilan Negeri Lhoksukon)

'BSN Ingatkan Kembali Peran Standar untuk Penguatan Forensik Digital Indonesia' (Badan Standardisasi Nasional (BSN), 2023)

CNN In, 'Waspada Hoaks Iklan Judi Online, Najwa Shihab, Raffi, Atta Pakai AI' (CNN Indonesia, 2024)

Devi, Wayan Zenitia, 'Implikasi Hukum Terhadap Penyalahgunaan Teknologi Deepkfake Untuk Pemerasan (Sextortion) Dalam Perspektif Hukum Teknologi Informasi Di Indonesia', *Majelis : Jurnal Hukum Indonesia*, 3.1 (2026), pp. 102–14, doi:10.62383/majelis.v3i1.1504

Ismaidar, Bambang Fitrianto, Kevin Maisyan Rizaldi Mendrofa, Kospiyandi, Rika Suryana Surbakti, and Tri Sandi, 'Perkembangan Teori Penemuan Hukum Dalam Sistem Hukum Indonesia Berdasarkan Kitap Undang Undang Hukum Pidana (KUHP) Baru', *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3.6 (2025), pp. 8400–8407, doi:https://doi.org/10.61104/alz.v3i5.2532

Liu, Baoping, Bo Liu, Tianqing Zhu, and Ming Ding, 'A Review of Deepfake and Its Detection: From Generative Adversarial Networks to Diffusion Models', *International Journal of Intelligent Systems*, 2025.1 (2025), p. 9987535, doi:https://doi.org/10.1155/int/9987535

Mecca, Anggil Syahra Putri, Wahab Aznul Hidaya, and Hadi Tuasikal, 'Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) Dalam Sistem Peradilan Pidana Di Indonesia', *Jurnal Sosial Teknologi*, 5.6 (2025), pp. 1–17 <http://sostech.greenvest.co.id/index.php/sostech/article/view/32207>

'Membangun Karier di Dunia Digital Forensik: Kebutuhan Talenta dan Jalur Sertifikasi' (Xynexis International, 2025)

Muginastiti, Emy, and Edi Saputra Hasibuan, 'Analisa Kepastian Hukum Terkait Pengaturan Surat Keterangan Bukan Pelaku Utama Sebagai Syarat Pengajuan Pembebasan Bersyarat', *Syntax Literate: Jurnal Ilmiah Indonesia*, 11.5 (2026), pp. 4587–4603, doi:10.36418/syntax-literate.v11i5.64411

Prayoga, Hendra, and Hadi Tuasikal, 'Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia', *Abdurrauf Law and Sharia*, 1.2 (2024), pp. 22–38

Putri, Dinda Buana, 'Parlemen Malaysia Hadapi Gelombang Pemerasan Deepfake Porn, Desak Aturan AI' (VOI, 2025)

Sari, Nia Ayu Mayang, 'Kasus Pidana Diatur Dalam Kitab Undang Hukum Pidana Yang Dikaitkan Dengan Asas Legalitas Dalam Hukum Pidana', *IBLAM LAW REVIEW*, 6.1 (2026), pp. 10–17, doi:10.52249/ilr.v6i1.658

Sativa, Riza, 'Scientific Investigation Dalam Penyidikan Tindak Pidana Pembunuhan', *Jurnal Ilmu Kepolisian*, 15.1 (2021), pp. 57–67, doi:10.35879/jik.v15i1.295

Shidarta, *Moralitas Profesi Hukum Suatu Tawaran Kerangka Berpikir* (PT Refika Aditama, 2006)

Soesilo, R, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya* (Politeia, 1996)

Sudarto, *Hukum dan Hukum Pidana* (Alumni, 1986)

tvOneNews, 'Kasus Penyebaran Konten Deepfake Vulgar Dengan Korban Siswi SMA Naik Ke Penyidikan | TvOne' (YouTube, 2025)

Verihubs, 'Kasus Deepfake di Indonesia: Prabowo dan Jokowi jadi Korbannya' (Verihubs, 2025)

VIDA, 'Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya', 2024

Yani, Ahmad, 'Peran Artificial Intelligence Sebagai Salah Satu Faktor Dalam Menentukan Kualitas Mahasiswa Di Era Society 5.0', *Journal of Education Research*, 5.2 (2024), pp. 1089–96, doi:10.37985/jer.v5i2.963

Yuliana, Mediana, 'Profesi Menggiurkan di Era Digital', *Kontan Peluang Usaha* (Kontan, 2012)