

Konstruksi Pertanggungjawaban Pidana terhadap Konten Deepfake di Media Sosial Berdasarkan UU ITE dan Hukum Pidana Indonesia

Rian Rahadian¹, Rizki Mohamad Eka Marsa Sadjat¹, Raka Indra Pratama¹

¹ Universitas Buana Perjuangan Karawang, Indonesia



rian.rahadian@ubpkarawang.ac.id*

Abstract

The rapid advancement of generative artificial intelligence has given rise to deepfakes, synthetic audio-visual content capable of convincingly imitating a person's face, voice, expressions, and gestures to the point of being indistinguishable from authentic recordings. This characteristic makes deepfakes prone to misuse for fraud, defamation, non-consensual pornography, and public information manipulation on social media. Indonesian criminal law does not yet comprehensively and explicitly regulate the term deepfake, so law enforcement against such acts relies on general provisions in the Electronic Information and Transactions Law, the National Penal Code, and the Personal Data Protection Law, none of which were historically designed to address the technical characteristics of AI-generated synthetic content. This study aims to analyze the adequacy of existing legal regulation of deepfake content and to formulate an appropriate construction of criminal liability for creators, uploaders, distributors, and parties who benefit from such content. The study employs a normative legal method with statute, conceptual, case, and comparative approaches. The findings reveal three fundamental problems: normative vagueness in the false-news offense, a legal vacuum concerning liability for automated generative AI use, and a mismatch between conventional *actus reus* elements and the technical mechanism of deepfake production. Based on these findings, this study formulates a tiered criminal liability model that differentiates perpetrators by role, form of fault, and purpose of deepfake use. The study concludes that a proportionate normative reformulation is needed to reach deepfake offenders without sacrificing legitimate freedom of expression, creative content, and satire.

Keywords: Deepfake; Criminal Liability; Ite Law; Artificial Intelligence; Social Media

ARTICLE INFO

Received
May 19, 2026
Revised
July 02, 2026
Accepted
August 28, 2026

Diterbitkan oleh

ISSN

Website

Ini adalah artikel akses terbuka di bawah lisensi CC BY SA

Fakultas Syariah Sekolah Tinggi Agama Islam (STAI) Al-Furqan Makassar

2622-5212

<https://ojs.staialfurqan.ac.id/jtm/>

<https://creativecommons.org/licenses/by-sa/4.0/>



PENDAHULUAN

Kecerdasan artifisial (Artificial Intelligence/AI) telah mengalami lonjakan kapabilitas luar biasa dalam satu dekade terakhir, terutama sejak berkembangnya arsitektur pembelajaran mendalam (deep learning) berbasis generative adversarial network dan model difusi yang memungkinkan mesin menghasilkan gambar, audio, dan video menyerupai realitas dengan presisi tinggi. Salah satu produk paling kontroversial dari perkembangan ini adalah deepfake, yaitu konten audio-visual sintetis yang dihasilkan atau dimanipulasi menggunakan algoritma pembelajaran mesin sedemikian rupa sehingga menampilkan seseorang mengatakan atau melakukan sesuatu yang sesungguhnya tidak pernah ia katakan atau lakukan (Chesney & Citron, 2019). Demokratisasi alat produksi konten sintetis membuat pembuatan deepfake tidak lagi memerlukan keahlian teknis tinggi, sehingga penggunaannya di media sosial berkembang pesat; Kementerian Komunikasi dan Digital melaporkan lonjakan konten deepfake hingga 550% dalam lima tahun terakhir, sementara pemerintah sendiri mengakui belum memiliki teknologi memadai untuk mengidentifikasinya (Suara Pemerintah, 2025; GovInsider Asia, 2024).

Karakteristik viral dan persuasif media sosial menjadikan deepfake instrumen efektif berbagai modus kejahatan. Di Indonesia, kepolisian menangkap pelaku yang membuat video deepfake menampilkan wajah Presiden Prabowo Subianto dan Wakil Presiden Gibran Rakabuming

Raka untuk menipu korban dengan modus bantuan sosial palsu (Antara News, 2025; Hukumonline, 2026a). Kasus lain menunjukkan penyalahgunaan deepfake untuk pornografi non-konsensual terhadap mahasiswi di Solo (Indonesia Online, 2026), manipulasi pidato pejabat publik seperti Menteri Keuangan Sri Mulyani (Liputan6, 2025), serta video AI mendiang Presiden Soeharto dalam kampanye Pemilu 2024 (BenarNews, 2024; CNN, 2024). Dampaknya berlapis: kerugian reputasi dan psikologis individu, kerugian ekonomi berskala besar sebagaimana kasus penipuan konferensi video yang merugikan perusahaan Arup di Hong Kong senilai 25,6 juta dolar AS (CNN Business, 2024), hingga ancaman terhadap integritas informasi publik dan proses demokrasi.

Menghadapi fenomena tersebut, hukum pidana Indonesia belum memiliki norma yang secara eksplisit dan komprehensif menyebut istilah deepfake. Satu-satunya instrumen yang menyentuh isu ini, Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial, secara tegas dinyatakan tidak mengikat secara hukum (JDIH Komdigi, 2023). Penegakan hukum karenanya bertumpu pada penafsiran ekstensif atas ketentuan umum Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana Nasional (KUHP Nasional), dan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang secara historis tidak dirancang untuk karakteristik teknis konten sintetis berbasis AI.

Penerapan UU ITE terhadap deepfake menghadapi persoalan konstruksi yuridis yang serius. Ketentuan yang secara tekstual paling mendekati karakter deepfake, yaitu Pasal 35 UU ITE tentang manipulasi data seolah otentik, dirumuskan untuk konteks pemalsuan dokumen elektronik konvensional dan belum pernah diuji secara luas untuk konten audio-visual hasil AI generatif (Hukumonline, 2026b). Sementara itu, pasal-pasal tentang berita bohong dan pencemaran nama baik mensyaratkan pembuktian unsur kesengajaan yang secara konsisten menimbulkan disparitas penafsiran (Revian & Kusumah, 2026). Persoalan ini diperparah oleh riwayat panjang pembatalan norma berita bohong oleh Mahkamah Konstitusi karena kekaburannya (Putusan MK Nomor 78/PUU-XXI/2023), sementara pasal penggantinya dalam KUHP Nasional kini tengah diuji ulang dengan argumen serupa (MK RI, 2026a; MK RI, 2026b), menunjukkan bahwa perumusan delik "berita bohong" di Indonesia secara struktural rentan terhadap persoalan asas legalitas apabila dipaksakan menjerat deepfake yang secara teknis jauh lebih kompleks daripada berita tekstual biasa.

Kajian akademik terdahulu telah menyentuh sebagian persoalan ini, namun umumnya berhenti pada tahap identifikasi kekosongan hukum tanpa merumuskan model pertanggungjawaban yang operasional. Basah dkk. (2025) dan Gunawan (2026) menyimpulkan bahwa hukum Indonesia belum memiliki ketentuan eksplisit tentang deepfake, namun rekomendasinya bersifat umum berupa anjuran pembentukan regulasi khusus. Kartadinata (2026) menyoroti tantangan pembuktian namun tidak menyajikan skema konkret unsur delik kesalahan sanksi. Sijabat dan Lukitasari (2024) serta Monatares dkk. (2026) menganalisis deepfake dari sudut delik tunggal (pencemaran nama baik atau kesusilaan semata) tanpa mempertimbangkan diferensiasi peran pelaku maupun tujuan penggunaan. Yulianto dan Makhali (2025) mengulas bentuk pertanggungjawaban pidana cybercrime secara umum tanpa spesifik membahas deepfake atau AI, sementara Alaini (2026) dan Oscar serta Hoesein (2025) menyoroti kesenjangan regulasi hoaks dan AI pasca pembaharuan KUHP namun rekomendasinya masih bersifat kelembagaan konseptual, belum dioperasionalkan menjadi norma pasal yang konkret. Di tataran internasional, Zheng, Shu, dan Li (2025) membandingkan pendekatan regulasi deepfake di Amerika Serikat, Uni Eropa, dan Tiongkok, namun tidak menjangkau konteks hukum Indonesia. Dengan demikian, terdapat celah penelitian yang signifikan: belum ada kajian yang merumuskan konstruksi pertanggungjawaban pidana berjenjang yang membedakan secara eksplisit antara pembuat, pengunggah, penyebar, dan pihak yang memperoleh keuntungan dari konten deepfake berdasarkan kombinasi bentuk kesalahan, tujuan penggunaan, akibat hukum, dan kemampuan pembuktian digital.

Berdasarkan celah tersebut, penelitian ini menawarkan novelty berupa konstruksi pertanggungjawaban pidana berjenjang yang memetakan rantai peran subjek (pembuat, pengunggah, penyebar, penerima manfaat, pihak yang memerintahkan/membantu, penyelenggara platform, dan pengendali sistem AI otomatis), dipadukan dengan tipologi delapan bentuk penggunaan deepfake (hiburan/satire, tanpa niat merugikan, penipuan, pencemaran nama baik, pornografi, manipulasi informasi publik, kepentingan politik/kampanye, dan deepfake yang dihasilkan AI generatif secara otomatis). Berdasarkan uraian di atas, penelitian ini bertujuan menganalisis kecukupan pengaturan hukum yang berlaku terhadap konten deepfake dan

merumuskan konstruksi pertanggungjawaban pidana yang tepat bagi pelakunya, melalui dua rumusan masalah: (1) bagaimana pengaturan hukum terhadap konten deepfake dalam sistem hukum pidana Indonesia berdasarkan UU ITE dan peraturan perundang-undangan terkait; dan (2) bagaimana konstruksi pertanggungjawaban pidana terhadap pelaku pembuatan dan penyebaran konten deepfake di media sosial dalam perspektif hukum pidana Indonesia.

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (normative legal research) yang menempatkan norma hukum sebagai objek kajian utama dan bersifat preskriptif, yakni tidak sekadar mendeskripsikan hukum yang berlaku (law in books) melainkan juga memberikan preskripsi mengenai konstruksi hukum yang seharusnya berlaku (das sollen) terhadap fenomena deepfake yang belum sepenuhnya terjangkau oleh hukum positif (Marzuki, 2005).

Penelitian ini menggunakan empat pendekatan yang saling melengkapi: pendekatan perundang-undangan (statute approach) untuk mengkaji secara sistematis dan hierarkis UUD NRI 1945, UU ITE beserta dua kali perubahannya, KUHP Nasional, dan UU PDP; pendekatan konseptual (conceptual approach) untuk membedah doktrin pertanggungjawaban pidana, kebijakan hukum pidana, dan cybercrime guna mengonstruksi proposisi hukum baru; pendekatan kasus (case approach) untuk menganalisis kasus deepfake nyata di Indonesia dan mancanegara sebagai bahan verifikasi empiris; serta pendekatan perbandingan (comparative approach) untuk mengkaji regulasi deepfake di Uni Eropa, Amerika Serikat, Korea Selatan, dan Singapura guna memperkaya perumusan rekonstruksi.

Bahan hukum primer meliputi UUD NRI 1945; UU Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 jo. UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik; UU Nomor 1 Tahun 2023 tentang KUHP Nasional; UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023; serta putusan Mahkamah Konstitusi yang relevan. Bahan hukum sekunder meliputi buku hukum pidana dan cyberlaw, artikel jurnal ilmiah nasional dan internasional, serta laporan resmi lembaga pemerintah, yang seluruhnya diverifikasi keberadaannya secara daring untuk menghindari fabrikasi sumber.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) pada basis data resmi (peraturan.bpk.go.id, jdih.komdigi.go.id, mkri.id), basis data jurnal ilmiah (SINTA, Google Scholar, DOAJ), serta pemberitaan media kredibel untuk kasus kontemporer yang belum termuat dalam putusan pengadilan terpublikasi. Kasus yang dipilih dibatasi pada peristiwa yang benar-benar terjadi dan diberitakan oleh sumber kredibel, baik media arus utama nasional maupun internasional guna menghindari penggunaan ilustrasi hipotetis yang dapat mengurangi validitas empiris analisis.

Analisis dilakukan secara kualitatif dengan interpretasi gramatikal, sistematis, dan teleologis, serta analisis unsur delik secara struktural, yakni menguraikan setiap unsur normatif suatu pasal kemudian menilai apakah unsur tersebut secara faktual dapat dipenuhi oleh karakteristik teknis deepfake, bukan dengan memaksakan pasal tertentu untuk menjerat perbuatan yang dikaji. Analisis komparatif dilakukan dengan memetakan definisi, larangan, mekanisme pertanggungjawaban, dan perlindungan korban pada setiap yurisdiksi perbandingan, kemudian menilai elemen mana yang secara konseptual dan konstitusional dapat diadaptasi ke dalam sistem hukum Indonesia tanpa mengabaikan karakteristik hukum pidana Indonesia yang bercorak civil law.

HASIL DAN PEMBAHASAN

1. Landasan Teoretis

a. Teori Pertanggungjawaban Pidana

Pertanggungjawaban pidana dalam tradisi hukum pidana Eropa Kontinental yang dianut Indonesia bertumpu pada asas kesalahan (schuldbeginssel) yang tercermin dalam adagium geen straf zonder schuld (tiada pidana tanpa kesalahan) dan actus non facit reum nisi mens sit rea (perbuatan tidak menjadikan seseorang bersalah kecuali disertai niat jahat). Moeljatno (2002) merumuskan pertanggungjawaban pidana sebagai keadaan psikis tertentu pada diri pembuat dan hubungan antara keadaan tersebut dengan perbuatan yang dilakukan, sehingga pembuat dapat dicela atas perbuatannya. Tiga syarat pemidanaan yang lazim diakui adalah kemampuan bertanggung jawab (toerekeningsvatbaarheid), adanya kesalahan dalam arti sempit berupa kesengajaan (dolus) atau kealpaan (culpa), dan tidak adanya alasan penghapus pidana, baik alasan pembenar yang menghapus sifat melawan hukum perbuatan maupun alasan pemaaf yang

menghapus kesalahan pembuat. Ketiga syarat ini menjadi kerangka utama untuk menilai dapat tidaknya pembuat, pengunggah, atau penyebar deepfake dipertanggungjawabkan secara pidana, khususnya dalam menakar hubungan antara perbuatan teknis pembuatan konten sintetis dengan keadaan batin pembuatnya.

b. Teori Kebijakan Hukum Pidana

Kebijakan hukum pidana merupakan bagian dari kebijakan penanggulangan kejahatan yang mencakup upaya rasional menetapkan perbuatan mana yang seyogianya dijadikan tindak pidana dan sanksi apa yang paling tepat, dengan memperhatikan bahwa sarana penal merupakan upaya terakhir (*ultimum remedium*) serta memperhatikan kepastian hukum dan proporsionalitas sanksi (Arief, 2008). Teori ini digunakan untuk menilai apakah kebijakan kriminal Indonesia saat ini, yang menjerat deepfake melalui pasal-pasal umum tanpa norma khusus, telah memadai atau justru menimbulkan inkonsistensi kebijakan penal.

c. Teori Cybercrime / Hukum Pidana Digital

Cybercrime dipahami sebagai kejahatan yang memanfaatkan jaringan komputer sebagai sarana, sasaran, maupun insidental terhadap perbuatan pidana lain, dengan karakteristik anonimitas pelaku, skalabilitas, dan sifat lintas batas yang menyulitkan penegakan hukum berbasis yurisdiksi teritorial (Wall, 2007). Deepfake merupakan bentuk lanjutan cybercrime dengan realisme sintetis tinggi yang mengaburkan batas antara informasi otentik dan palsu, menciptakan apa yang oleh Chesney dan Citron (2019) disebut "liar's dividend" situasi ketika pelaku kejahatan nyata dapat berkelit dengan menuduh bukti otentik sebagai deepfake. Teori ini menjelaskan mengapa kerangka pertanggungjawaban konvensional yang berbasis pembuktian akibat langsung perlu direformulasi agar menjangkau karakteristik unik kejahatan berbasis AI generatif ini.

2. Pengaturan Hukum terhadap Konten Deepfake dalam Sistem Hukum Pidana Indonesia

a. Karakteristik Deepfake dan Kedudukannya dalam Hukum Positif

Deepfake secara teknis dihasilkan melalui autoencoder atau generative adversarial network yang melatih model AI dengan data wajah/suara target, kemudian menghasilkan atau menukar representasi wajah/suara tersebut ke rekaman lain (Chesney & Citron, 2019). Karakteristik ini membedakan deepfake secara fundamental dari manipulasi digital konvensional: deepfake menghasilkan representasi biometrik baru yang tidak pernah benar-benar terjadi (*fabrication*), bukan sekadar mengubah konteks peristiwa yang benar-benar terekam; prosesnya melibatkan model pembelajaran mesin yang menghasilkan tingkat kealamian jauh lebih meyakinkan; dan alat pembuatannya kini demokratis, dapat dioperasikan tanpa keahlian teknis tinggi. Perbedaan ini penting secara yuridis karena unsur "manipulasi" dalam pasal-pasal hukum pidana Indonesia dirumuskan pada masa manipulasi digital konvensional menjadi acuan utama, sehingga penerapannya terhadap deepfake memerlukan penafsiran ekstensif yang harus diuji kecermatannya unsur demi unsur, bukan dipaksakan begitu saja.

b. Analisis UU ITE

Ketentuan yang secara tekstual paling relevan adalah Pasal 35 UU ITE, yang melarang "manipulasi, penciptaan, perubahan... Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar dianggap seolah-olah data yang otentik", dengan ancaman pidana hingga dua belas tahun dan/atau denda Rp12.000.000.000,00 (Pasal 51 ayat (1)) (Hukumonline, 2026b). Frasa "penciptaan" data yang dianggap "seolah-olah otentik" secara akurat menggambarkan mekanisme kerja deepfake, namun penerapannya pada video/audio memerlukan argumentasi tambahan bahwa konten tersebut termasuk kategori "Informasi Elektronik dan/atau Dokumen Elektronik" argumentasi yang secara tekstual dapat dibangun namun belum teruji luas di pengadilan Indonesia, sehingga sifatnya masih penafsiran ekstensif, bukan penerapan eksplisit yang disediakan pembentuk undang-undang.

Pasal 27 ayat (1) UU ITE tentang muatan kesusilaan secara langsung relevan untuk deepfake pornografi non-konsensual (Indonesia Online, 2026), karena berorientasi pada dampak muatan, bukan keotentikan sumber, sehingga relatif siap diterapkan tanpa kesulitan konseptual berarti. Pasal 27A UU ITE (hasil Perubahan Kedua UU Nomor 1 Tahun 2024), pengganti ketentuan pencemaran nama baik, merumuskan "setiap orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal... dalam bentuk informasi elektronik" dengan ancaman diturunkan menjadi dua tahun dan bersifat delik aduan (Hukumonline, 2024b; NU Online, 2024). Ketentuan ini dapat diterapkan pada deepfake berisi tuduhan tercela, dengan catatan keberadaan disclaimer eksplisit bahwa konten adalah rekayasa dapat memengaruhi penilaian unsur delik (Sijabat & Lukitasari, 2024). Adapun Pasal 28 UU ITE tentang berita bohong,

yang pasca 2024 mengatur pula "pemberitahuan bohong yang menimbulkan kerusuhan" (ayat (3)), mensyaratkan unsur "kerusuhan" yang bersifat kumulatif dan berorientasi akibat, sehingga sulit diterapkan pada deepfake yang "hanya" menimbulkan kemarahan publik tanpa gangguan ketertiban fisik nyata, persoalan pembuktian kesengajaan yang juga dikonfirmasi oleh disparitas putusan terkait pasal ini (Revian & Kusumah, 2026). Sebagai pelengkap, Pasal 32 UU ITE tentang perubahan/perusakan/pemindahan data elektronik milik orang lain secara tekstual lebih berorientasi pada perlindungan integritas sistem dan data (data integrity) ketimbang perlindungan identitas personal, sehingga kurang tepat diterapkan langsung pada konten deepfake dibandingkan Pasal 35, meskipun ancaman pidananya juga berat, yakni penjara paling lama delapan tahun dan/atau denda paling banyak Rp2.000.000.000,00 berdasarkan Pasal 48 ayat (1) UU ITE.

c. Analisis UU PDP dan KUHP Nasional

UU PDP memberikan jalur pertanggungjawaban alternatif yang selama ini kurang diperhatikan: wajah dan suara yang digunakan melatih model AI pembuat deepfake merupakan data biometrik yang tergolong data pribadi spesifik (Pasal 4), sehingga pengumpulannya tanpa persetujuan dapat dijerat Pasal 65 jo. Pasal 67 (ancaman hingga lima tahun) dan Pasal 68 tentang pemalsuan data pribadi (ancaman hingga enam tahun), terlepas dari bagaimana hasil akhirnya digunakan (Hukumonline, 2025a). Pasal 70 UU PDP turut membuka kemungkinan menjerat penyelenggara platform yang secara struktural memfasilitasi pengumpulan data biometrik tanpa persetujuan melalui pertanggungjawaban korporasi.

KUHP Nasional yang berlaku efektif sejak 2 Januari 2026 mengkodifikasi ulang delik berita bohong dalam Pasal 263-264 (pengganti UU Nomor 1 Tahun 1946 yang telah dicabut Pasal 622 KUHP Nasional), dengan ancaman hingga enam tahun bagi yang mengetahui kebohongan dan empat tahun bagi yang "patut menduga". Ketentuan ini kini justru sedang diuji materi kembali di Mahkamah Konstitusi (Perkara Nomor 93/PUU-XXIV/2026) dengan dalil kekaburan norma yang serupa dengan pendahulunya (MK RI, 2026a), menunjukkan pola berulang bahwa delik "berita bohong" di Indonesia secara struktural rentan persoalan asas legalitas. Pasal 433 KUHP Nasional (pencemaran nama baik) dan Pasal 492 (penipuan) juga relevan namun beririsan dengan UU ITE yang mengancam lebih berat untuk perbuatan serupa yang dilakukan melalui sarana elektronik, sehingga berdasarkan asas *lex specialis*, UU ITE semestinya diterapkan lebih dahulu untuk deepfake yang disebarkan melalui media sosial, dan KUHP Nasional hanya relevan sebagai pengisi kekosongan bagi perbuatan yang tidak sepenuhnya dilakukan melalui sistem elektronik. Adapun Pasal 391 KUHP Nasional tentang pemalsuan surat, meskipun secara konseptual dapat diperluas ke dokumen elektronik palsu, semestinya dikesampingkan pula terhadap deepfake berbentuk dokumen digital karena Pasal 35 UU ITE telah mengatur secara *lex specialis* pemalsuan data elektronik dengan ancaman yang jauh lebih berat.

d. Keterbatasan Pengaturan dan Lex Specialis-Lex Generalis

Analisis unsur delik di atas menunjukkan tiga persoalan normatif: kekaburan norma (*vague norm*) pada delik berita bohong yang berisiko melanggar asas legalitas material; ketidaksesuaian norma (*normative mismatch*) pada Pasal 35 UU ITE yang secara historis tidak dirancang untuk konten sintesis AI; dan kekosongan hukum (*legal vacuum*) pada pertanggungjawaban penyelenggara platform maupun pengguna AI generatif otomatis yang belum diatur satu pasal pun. Penerapan pasal terhadap deepfake harus mengikuti asas *lex specialis derogat legi generali* secara berjenjang: UU ITE dan UU PDP sebagai *lex specialis* atas perbuatan yang dilakukan melalui sistem elektronik atau menyasar data biometrik, dan KUHP Nasional sebagai *lex generalis* pengisi kekosongan, agar penegakan hukum tidak memaksakan pasal secara serampangan.

3. Konstruksi Pertanggungjawaban Pidana terhadap Pelaku Konten Deepfake

Karakteristik ekosistem digital menuntut agar pertanggungjawaban pidana deepfake dipahami sebagai rantai peran (*chain of roles*), bukan relasi tunggal pelaku korban, yang melibatkan sekurang-kurangnya tujuh kategori subjek: pembuat (*creator*) yang menghasilkan konten deepfake; pihak yang mengunggah (*uploader*) untuk pertama kali; pihak yang menyebarkan (distributor/*resharer*); pihak yang menggunakan deepfake untuk memperoleh keuntungan (*beneficiary*); pihak yang memerintahkan atau membantu (*instigator/accomplice*) sesuai ajaran penyertaan; penyelenggara platform media sosial; dan pengendali sistem AI otomatis dalam hal konten dihasilkan tanpa intervensi manusia pada setiap luarannya.

a. Mens Rea dan Pembuktian Digital

Persoalan sentral pertanggungjawaban pidana deepfake terletak pada pembuktian mens rea, mengingat rantai peran di atas memungkinkan derajat pengetahuan yang sangat bervariasi antarsubjek. Pembuat yang secara sadar merancang konten untuk menipu atau mencemarkan nama baik memenuhi unsur *dolus directus*, sedangkan pengunggah atau penyebar lanjutan yang menerima konten tanpa mengetahui bahwa itu hasil rekayasa berada pada posisi berbeda-baik *dolus eventualis* maupun *culpa*, sebagaimana problem serupa yang diidentifikasi Revian dan Kusumah (2026) pada penyebaran hoaks konvensional. Setiap subjek harus dinilai berdasarkan derajat pengetahuan aktualnya sendiri, bukan disamaratakan hanya karena berada dalam rantai penyebaran yang sama.

Tantangan pembuktian dalam perkara deepfake bersifat berlapis dua: pembuktian keaslian/manipulasi konten secara forensik digital, yang secara teknis semakin sulit seiring perkembangan model AI generatif yang menghilangkan artefak visual/audio penanda deepfake; dan pembuktian identitas pelaku (*attribution*), yang semakin sulit ketika pelaku menggunakan akun anonim atau infrastruktur lintas yurisdiksi. Kombinasi kedua lapis pembuktian ini menjadikan perkara deepfake secara struktural lebih menuntut kapasitas forensik digital dibandingkan delik pidana konvensional.

b. Diferensiasi Berdasarkan Tujuan Penggunaan

Kelayakan pemidanaan deepfake sangat bergantung pada tujuan penggunaannya. Deepfake untuk hiburan/satire yang secara wajar dapat dikenali publik sebagai karya fiksi dilindungi kebebasan berekspresi konstitusional dan tidak memenuhi unsur kesalahan, kecuali konteksnya dihilangkan pihak ketiga (*context collapse*) sehingga tanggung jawab beralih kepada penyebar tersebut; sementara deepfake yang dibuat tanpa niat merugikan namun tersebar di luar kendali pembuatnya berada pada spektrum *culpa* dan sepatutnya mendapat pendekatan restoratif, bukan pemidanaan penuh.

Deepfake untuk penipuan sebagaimana kasus bansos Prabowo-Gibran dan penipuan konferensi video Arup di Hong Kong konsisten memenuhi *dolus directus* dan paling siap dijerat kombinasi Pasal 35 dan Pasal 28 ayat (1) UU ITE serta Pasal 492 KUHP Nasional. Deepfake untuk pencemaran nama baik menuntut pembuktian tuduhan yang merusak kehormatan korban melalui Pasal 27A UU ITE yang bersifat delik aduan. Deepfake untuk pornografi non-konsensual, dengan dampak psikologis korban paling berat, beririsan dengan tiga rezim sekaligus: Pasal 27 ayat (1) UU ITE, UU Pornografi, dan UU PDP terkait penggunaan data biometrik tanpa persetujuan.

Deepfake untuk manipulasi informasi publik menghadapi kesulitan pembuktian unsur "kerusuhan" yang bersifat kumulatif, sementara deepfake untuk kepentingan politik/kampanye sebagaimana kasus video AI mendiang Presiden Soeharto menjelang Pemilu 2024 menghadapi kekosongan hukum paling nyata karena Undang-Undang Pemilihan Umum tidak memiliki satu pasal pun tentang penggunaan AI dalam kampanye. Adapun deepfake yang dihasilkan AI generatif secara otomatis menimbulkan persoalan mens rea paling kompleks karena "pembuat" konvensional sulit diidentifikasi; pertanggungjawaban dalam kategori ini harus dibebankan kepada pihak yang mengendalikan sistem berdasarkan prinsip pertanggungjawaban atas risiko yang diciptakan, dengan pertanggungjawaban korporasi (Pasal 70 UU PDP) sebagai jalur tambahan bagi penyelenggara platform (Sari, Hasibuan, & Suharto, 2026).

4. Rekonstruksi Konstruksi Pertanggungjawaban Pidana

Berdasarkan analisis di atas, Tabel 1 merangkum konstruksi pertanggungjawaban pidana yang diusulkan penelitian ini, yang menautkan tujuan penggunaan deepfake dengan bentuk kesalahan, ketentuan hukum yang relevan, dan tingkat pertanggungjawaban.

Tabel 1. Konstruksi Pertanggungjawaban Pidana Berdasarkan Tujuan Penggunaan Deepfake

Tujuan Penggunaan	Bentuk Kesalahan	Ketentuan Hukum yang Relevan	Pertanggungjawaban
Hiburan/satire	Tidak ada <i>dolus</i> merugikan	Dilindungi Ps. 28E-28F UUD NRI 1945	Tidak dipidana bila proporsional & berkonteks jelas
Tanpa niat merugikan	<i>Culpa</i> (lalai)	Ps. 264 KUHP Nasional	Ringan; pendekatan restoratif diutamakan
Penipuan	<i>Dolus directus</i>	Ps. 35 jo. 51(1) & 28(1) UU ITE; Ps.	Penuh; delik materiil

Tujuan Penggunaan	Bentuk Kesalahan	Ketentuan Hukum yang Relevan	Pertanggungjawaban
		492 KUHP Nasional	
Pencemaran nama baik	Dolus directus	Ps. 27A jo. 45(4) UU ITE (delik aduan)	Penuh, bergantung aduan korban
Pornografi non-konsensual	Dolus directus	Ps. 27(1) UU ITE; UU Pornografi; Ps. 65/67 UU PDP	Penuh; irisan tiga rezim hukum
Manipulasi informasi publik	Dolus/dolus eventualis	Ps. 28(3) UU ITE; Ps. 263 KUHP Nasional	Bergantung unsur 'kerusuhan' (rentan vague norm)
Politik/kampanye	Dolus directus	Kekosongan hukum UU Pemilu; residual Ps. 28(3)/27A	Lemah/vacuum
AI generatif otomatis	Created-risk liability	Ps. 35 UU ITE (pengendali); Ps. 70 UU PDP (korporasi)	Dibebankan ke pengendali manusia & korporasi

Selain diferensiasi berdasarkan tujuan penggunaan, konstruksi pertanggungjawaban juga harus memetakan rantai peran subjek secara berjenjang, sebagaimana dirangkum pada Tabel 2, yang menautkan perbuatan setiap subjek dengan bentuk kesalahan serta pertanggungjawaban dan sanksinya.

Tabel 2. Rantai Pertanggungjawaban Pidana Berdasarkan Subjek Pelaku

Subjek Pelaku	Perbuatan	Bentuk Kesalahan	Pertanggungjawaban & Sanksi
Pembuat (creator)	Menciptakan konten deepfake dari data biometrik target	Dolus directus	Penuh; hingga 12 th/Rp12 M (Ps. 51(1) UU ITE), kumulatif Ps. 68 UU PDP
Pengunggah (uploader)	Mengunggah pertama kali ke media sosial	Dolus directus/eventualis	Penuh; sepadan pembuat bila identik orangnya
Penyebar (distributor)	Membagikan ulang dengan/tanpa amplifikasi	Dolus eventualis atau culpa	Berjenjang sesuai derajat pengetahuan; ringan bila murni culpa
Penerima manfaat (beneficiary)	Memanfaatkan deepfake ciptaan pihak lain untuk keuntungan	Dolus directus (lucri causa)	Penuh; delik materiil, kerugian nyata wajib dibuktikan
Pemberi perintah/pembantu	Memerintahkan, membiayai, atau membantu sarana	Dolus directus atas peran masing-masing	Sepadannya pelaku utama atau dikurangi sesuai ajaran penyertaan
Penyelenggara platform	Gagal melakukan moderasi konten yang layak	Culpa institusional (bila diatur)	Saat ini: sanksi administratif; diusulkan due diligence liability
Pengendali sistem AI otomatis	Mengonfigurasi/memberi prompt pada sistem otomatis	Created-risk liability	Dibebankan ke pengendali manusia & korporasi penyedia (Ps. 70 UU PDP)

Model yang diusulkan bercorak differentiated liability model: menautkan sanksi dengan peran kausal subjek, tujuan penggunaan, dan derajat kesalahan yang benar-benar dapat dibuktikan, alih-alih pendekatan satu pasal untuk semua bentuk deepfake. Model ini dirancang menghindari dua risiko sekaligus pemidanaan berlebihan (overcriminalization) terhadap deepfake satire/kreatif yang dilindungi kebebasan berekspresi, dan pemidanaan yang tidak memadai

(undercriminalization) terhadap deepfake berbahaya yang selama ini luput dari jangkauan norma yang tidak dirancang khusus untuknya. Novelty penelitian ini terletak pada diferensiasi eksplisit antara pembuat, pengunggah, penyebar, dan penerima manfaat berdasarkan kombinasi bentuk kesalahan, tujuan penggunaan, akibat hukum, dan kemampuan pembuktian digital sesuatu yang belum ditemukan secara utuh dalam penelitian terdahulu yang umumnya berhenti pada identifikasi kekosongan hukum semata.

5. Analisis Kasus dan Perbandingan Hukum

Beberapa kasus nyata menguatkan konstruksi di atas. Kasus deepfake bansos Prabowo-Gibran menunjukkan Pasal 35 UU ITE hasil revisi 2024 telah mulai diterapkan aparat, namun tetap memerlukan Pasal 378 KUHP sebagai pelengkap dakwaan (Hukumonline, 2026a). Kasus deepfake pornografi di Solo, yang proses hukumnya memakan waktu sekitar tujuh bulan sejak laporan hingga penetapan tersangka, mengilustrasikan lambannya penegakan hukum dibandingkan kecepatan penyebaran konten (Indonesia Online, 2026) persoalan yang terkait langsung dengan kompleksitas pembuktian forensik digital yang telah diuraikan. Kasus manipulasi audio-visual potongan pidato Menteri Keuangan Sri Mulyani yang beredar seolah menyatakan pernyataan yang tidak pernah diucapkannya turut menunjukkan bahwa deepfake dapat memicu kemarahan publik secara cepat sebelum sempat diklarifikasi (Liputan6, 2025), sekalipun pemberitaan yang dapat ditelusuri tidak menyebutkan proses pidana konkret terhadap pembuatnya menggambarkan kesenjangan antara kecepatan penyebaran dan kecepatan penegakan hukum. Kasus video AI mendiang Presiden Soeharto pada Pemilu 2024 membuktikan legal vacuum pada kategori deepfake politik, karena Komisi Pemilihan Umum tidak memiliki aturan spesifik mengenai AI/deepfake dalam kampanye (BenarNews, 2024).

Sebagai pembanding internasional, kasus penipuan konferensi video Arup di Hong Kong menunjukkan bahwa teknologi deepfake video real-time telah melampaui kapasitas verifikasi manusia biasa (CNN Business, 2024), sementara krisis deepfake pornografi berbasis sekolah di Korea Selatan pada 2024 mendorong amandemen undang-undang yang bahkan mengkriminalisasi kepemilikan/konsumsi sadar konten deepfake porno (Korea Herald, 2024), pendekatan lebih luas dari UU ITE Indonesia yang baru menjerat pembuatan dan distribusi. Kasus deepfake pornografi Taylor Swift di Amerika Serikat pada Januari 2024, yang menyebar hingga puluhan juta tayangan sebelum ditindak (Wikipedia, 2024), mendorong lahirnya TAKE IT DOWN Act yang mewajibkan platform menghapus konten serupa dalam waktu 48 jam sejak laporan korban (Wikipedia, 2025) menunjukkan bahwa momentum publik dapat mempercepat reformasi hukum secara konkret, sesuatu yang belum terjadi secara sistemik di Indonesia meskipun kasus Solo memiliki karakteristik kerugian yang tidak kalah serius.

Perbandingan hukum menunjukkan beberapa model yang dapat memperkaya rekonstruksi Indonesia. Uni Eropa melalui Artificial Intelligence Act mewajibkan transparansi/pelabelan konten AI generatif tanpa melarang pembuatannya secara mutlak, dengan pengecualian bagi karya artistik dan satire (artificialintelligenceact.eu, 2024) pendekatan yang proporsional karena tetap melindungi deepfake kreatif yang sah. Singapura mengatur secara khusus larangan deepfake kandidat dalam masa kampanye melalui Elections (Integrity of Online Advertising) Act yang terpisah dari delik informasi bohong umum (Malay Mail, 2024), model yang secara langsung relevan mengisi kekosongan hukum pemilu Indonesia. Tiongkok, melalui Provisions on the Administration of Deep Synthesis yang berlaku sejak Januari 2023, mewajibkan pelabelan konten hasil deep synthesis serta verifikasi identitas nyata pengguna platform (China Briefing, 2023) elemen yang secara konseptual dapat diintegrasikan ke dalam kewajiban due diligence penyelenggara sistem elektronik di Indonesia. Korea Selatan menunjukkan bahwa perluasan pertanggungjawaban hingga tahap konsumsi/kepemilikan sadar dapat menjadi opsi kebijakan bagi Indonesia untuk kategori deepfake pornografi, mengingat skala korban potensial pada kasus Solo yang serupa dengan krisis di Korea Selatan.

6. Implikasi terhadap Pembaruan Hukum Pidana

Rekonstruksi ini berimplikasi pada tiga hal. Pertama, diperlukan penjelasan resmi atau perubahan redaksional Pasal 35 UU ITE yang secara eksplisit mencakup konten hasil kecerdasan artifisial generatif, guna mengatasi ketidaksesuaian norma yang selama ini bergantung pada penafsiran ekstensif hakim. Kedua, diperlukan ketentuan khusus larangan deepfake kandidat dalam Undang-Undang Pemilihan Umum, mengadaptasi model Singapura. Ketiga, diperlukan kewajiban due diligence dan pelabelan konten AI generatif bagi penyelenggara sistem elektronik,

mengadopsi elemen kewajiban platform dari model Uni Eropa dan Tiongkok yang disesuaikan dengan prinsip proporsionalitas dan kebebasan berekspresi konstitusional Indonesia.

KESIMPULAN

Penelitian ini menyimpulkan dua hal. Pertama, hukum pidana Indonesia hingga saat ini tidak memiliki norma yang secara eksplisit mengatur deepfake, sehingga penegakan hukum bergantung pada penafsiran ekstensif atas UU ITE (khususnya Pasal 27, 27A, 28, dan 35), KUHP Nasional (Pasal 263-264, 433, dan 492), serta UU PDP, yang secara historis tidak dirancang untuk karakteristik teknis konten sintetis berbasis AI dan menyisakan kekaburan norma, ketidaksesuaian norma, serta kekosongan hukum. Kedua, konstruksi pertanggungjawaban pidana yang tepat bagi deepfake adalah model berjenjang (*differentiated liability model*) yang membedakan pertanggungjawaban pembuat, pengunggah, penyebar, penerima manfaat, pihak yang memerintahkan/membantu, penyelenggara platform, dan pengendali sistem AI otomatis berdasarkan bentuk kesalahan, tujuan penggunaan, akibat hukum, dan kemampuan pembuktian digital sebagaimana dipetakan pada Tabel 1. Model ini diharapkan mengisi kekosongan hukum yang selama ini menjadi celah bagi pelaku kejahatan deepfake tanpa mengorbankan kebebasan berekspresi dan konten kreatif/satire yang sah secara konstitusional, sekaligus menjadi rujukan konkret bagi pembentuk undang-undang, aparat penegak hukum, dan penyelenggara platform dalam menyusun kebijakan yang proporsional. Kajian kasus dan perbandingan hukum yang dilakukan menegaskan bahwa kekosongan hukum paling mendesak terletak pada dua titik: pertanggungjawaban penyelenggara platform yang saat ini murni bersifat administratif, dan perlindungan terhadap integritas proses elektoral dari penyalahgunaan deepfake, yang keduanya belum memiliki norma pidana khusus dalam sistem hukum Indonesia hingga saat ini.

REFERENSI

Buku

- Arief, B. N. (2008). Bunga rampai kebijakan hukum pidana. Kencana Prenada Media Group.
Marzuki, P. M. (2005). Penelitian hukum. Kencana Prenada Media Group.
Moeljatno. (2002). Asas-asas hukum pidana. Rineka Cipta.
Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Artikel Jurnal

- Alaini. (2026). Analisis yuridis tindak pidana penyebaran hoaks dalam perspektif hukum pidana Indonesia pasca pembaharuan KUHP. *Indonesia of Journal Business Law*, 5(1), 19–40. <https://doi.org/10.47709/ijbl.v5i1.7535>
- Basah, D. A. Y., Wijaya, A., & Januady, I. (2025). Kriminalisasi pelanggaran protokol digital: Tinjauan hukum pidana terhadap penyebaran deepfake di media sosial. *Innovative: Journal of Social Science Research*, 5(4), 386–398. <https://doi.org/10.31004/innovative.v5i4.20258>
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1819. <https://doi.org/10.2139/ssrn.3213954>
- Gunawan. (2026). Limitasi normatif pertanggungjawaban pidana atas penyalahgunaan deepfake berbasis artificial intelligence di Indonesia. *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)*, 6(5), 3929–3936. <https://doi.org/10.38035/jihhp.v6i5.9050>
- Kartadinata, A. (2026). Rekonstruksi delik pidana dalam kejahatan deepfake: Tantangan pembuktian dan perlindungan korban. *MUARA HUKUM: Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik*, 2(1), 36–48. <https://doi.org/10.64365/muarakum.v2i1.203>
- Monatares, C., Holijah, Andriy, P. R., Ramadhani, N., & Perdana, I. (2026). Kesenjangan regulasi hukum pidana terhadap kejahatan deepfake: Studi kasus manipulasi konten asusila dalam putusan Pengadilan Negeri Semarang. *Journal of Law and Legal System*, 2(1), 154–166. <https://doi.org/10.61994/jlls.v2i1.1925>
- Oscar, K., & Hoesein, Z. A. (2025). Mendorong regulasi adaptif dan progresif untuk menghadapi penyalahgunaan artificial intelligence di Indonesia. *Journal of Innovative and Creativity (Joecy)*, 5(3), 31501–31511. <https://doi.org/10.31004/joecy.v5i3.4647>
- Revian, R. F. M., & Kusumah, H. A. (2026). Batas kesengajaan dalam ruang digital: Kajian yuridis pertanggungjawaban pidana penyebar hoaks yang tidak mengetahui kebohongan informasinya menurut UU ITE. *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)*, 6(5), 3548–3556. <https://doi.org/10.38035/jihhp.v6i5.8645>

- Sari, B. W. N., Hasibuan, A. H. H., & Suharto. (2026). Criminal liability for deepfake dissemination: Under Indonesia's cybercrime framework. *Mulawarman Law Review*, 11(1). <https://ejournal.fh.unmul.ac.id/mulrev/article/view/2128>
- Sijabat, S. A. U., & Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik. *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, 13(2), 179–194. <https://doi.org/10.20961/recidive.v13i2.86771>
- Yulianto, H. P., & Makhali, I. (2025). Bentuk pertanggung jawaban pidana bagi pelaku tindak pidana cyber. *Mizan: Jurnal Ilmu Hukum*, 14(2), 490–503. <https://doi.org/10.32503/mizan.v14i2.8447>
- Zheng, G., Shu, J., & Li, K. (2025). Regulating deepfakes between *lex lata* and *lex ferenda*—A comparative analysis of regulatory approaches in the U.S., the EU and China. *Crime, Law and Social Change*, 83, Article 1. <https://doi.org/10.1007/s10611-024-10197-z>

Peraturan Perundang-undangan dan Regulasi Asing

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024.
- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional).
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.
- Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.
- Mahkamah Konstitusi Republik Indonesia. (2024). Putusan Nomor 78/PUU-XXI/2023 perihal pengujian Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- Elections (Integrity of Online Advertising) (Amendment) Act 2024 (Singapore).
- Act on Special Cases Concerning the Punishment of Sexual Crimes, amendment (Republic of Korea, 2024).

Dokumen dan Sumber Berita

- Antara News. (2025). Polri tangkap pelaku video deepfake atasnamakan pejabat negara. <https://www.antaranews.com/berita/4603782/polri-tangkap-pelaku-video-deepfake-atasnamakan-pejabat-negara>
- artificialintelligenceact.eu. (2024). Practical guide: Article 50 AI Act – Transparency obligations. <https://artificialintelligenceact.eu/transparency-rules-article-50/>
- BenarNews. (2024). Suharto deepfake used in election campaign. <https://www.benarnews.org/english/news/indonesian/suharto-deepfake-used-in-election-campaign-01122024135217.html>
- CNN. (2024). AI deepfake brings back Indonesia's dead dictator Suharto in disturbing scam. <https://www.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl>
- China Briefing. (2023). China to regulate deep synthesis (deepfake) technology starting January 2023. <https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/>
- CNN Business. (2024). Arup revealed as victim of \$25 million deepfake scam involving Hong Kong employee. <https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>
- GovInsider Asia. (2024). Hadang deepfake, pemerintah Indonesia dorong implementasi AI yang beretika. <https://govinsider.asia/indo-en/article/hadang-deepfake-pemerintah-indonesia-dorong-implementasi-ai-yang-beretika>
- Hukumonline. (2024b). Perubahan penting soal pencemaran nama baik di UU ITE baru. <https://www.hukumonline.com/berita/a/perubahan-penting-soal-pencemaran-nama-baik-di-uu-ite-baru-lt65a90c5004886/>
- Hukumonline. (2025a). Jenis tindak pidana Pelindungan Data Pribadi. <https://www.hukumonline.com/klinik/a/jenis-tindak-pidana-pelindungan-data-pribadi-lt694a430534712/>

- Hukumonline. (2026a). Deepfake menyebar cepat, hukum bergerak lambat. <https://www.hukumonline.com/berita/a/deepfake-menyebar-cepat--hukum-bergerak-lambat-lt68f065103ad53/>
- Hukumonline. (2026b). Jerat pidana pemalsuan bukti transfer. <https://www.hukumonline.com/klinik/a/jerat-pidana-pemalsuan-bukti-transfer-lt68980c8659e82/>
- Indonesia Online. (2026). Deepfake porno di Solo: Trauma korban dan lambannya proses hukum. <https://indonesiaonline.co.id/deepfake-porno-di-solo-trauma-korban-dan-lambannya-proses-hukum/>
- JDIH Kementerian Komunikasi dan Digital. (2023). Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. https://jdih.komdigi.go.id/produk_hukum/view/id/883
- Korea Herald. (2024). South Korea passes bill to criminalize watching, possessing deepfake porn. <https://www.koreaherald.com/article/3480484>
- Liputan6. (2025). Bantah sebut 'guru beban negara', Sri Mulyani: Video itu hasil deepfake dan tak utuh. <https://www.liputan6.com/bisnis/read/6138074/bantah-sebut-guru-beban-negara-sri-mulyani-video-itu-hasil-deepfake-dan-tak-utuh>
- Malay Mail. (2024). As clock ticks down to general election, Singapore passes law banning deepfakes of candidates. <https://www.malaymail.com/news/singapore/2024/10/16/as-clock-ticks-down-to-general-election-singapore-passes-law-banning-deepfakes-of-candidates/153804>
- MK RI. (2026a). Aktivis uji Pasal penghasutan dan berita bohong dalam KUHP baru [Perkara Nomor 93/PUU-XXIV/2026]. <https://www.mkri.id/berita/aktivis-uji-pasal-penghasutan-dan-berita-bohong-dalam-kuhp-baru-24765>
- MK RI. (2026b). Aktivis tuding Pasal penyebaran berita bohong dalam KUHP untuk membungkam kebebasan berpendapat. <https://www.mkri.id/berita/aktivis-tuding-pasal-penyebaran-berita-bohong-dalam-kuhp-untuk-membungkam-kebebasan-berpendapat-24803>
- NU Online. (2024). Waspada bermedsos, kenali sanksi UU ITE jilid II termasuk potensi kriminalisasinya. <https://www.nu.or.id/nasional/waspada-bermedsos-kenali-sanksi-uu-ite-jilid-ii-termasuk-potensi-kriminalisasinya-mCvwX>
- Suara Pemerintah. (2025). Deepfake naik 550%, Kemkomdigi minta platform global sediakan fitur cek konten AI. <https://suarapemerintah.id/2025/09/deepfake-naik-550-kemkomdigi-minta-platform-global-sediakan-fitur-cek-konten-ai/>
- Wikipedia. (2024). Taylor Swift deepfake pornography controversy. https://en.wikipedia.org/wiki/Taylor_Swift_deepfake_pornography_controversy
- Wikipedia. (2025). TAKE IT DOWN Act. https://en.wikipedia.org/wiki/TAKE_IT_DOWN_Act