

PERTANGGUNGJAWABAN PIDANA PENYALAHGUNAAN DEEPFAKE BERBASIS ARTIFICIAL INTELLIGENCE DALAM PERSPEKTIF UNDANG-UNDANG ITE BARU

*Criminal Liability for Artificial Intelligence-Based Deepfake Misuse in the Perspective of the Revised
ITE Law*

Albert Andre Saturnus

Fakultas Hukum, Universitas Pendidikan Ganesha, Bali, Indonesia

Korespondensi: albert@undiksha.ac.id

ABSTRAK

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah melahirkan fenomena deepfake—rekayasa digital yang mampu menghasilkan konten visual dan audio sintetis dengan tingkat kemiripan yang sulit dibedakan dari aslinya. Di Indonesia, penyalahgunaan deepfake telah berkembang menjadi ancaman nyata, khususnya dalam kasus penipuan finansial dan penyebaran konten pornografi nonconsensual (revenge porn). Penelitian ini bertujuan mengkaji kecukupan ketentuan pidana dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE (UU ITE Baru) dalam menjerat pelaku penyalahgunaan deepfake. Menggunakan metode yuridis normatif yang didukung pendekatan komparatif dan konseptual, penelitian ini menemukan bahwa meski UU ITE Baru mengalami pembaruan signifikan, terdapat celah hukum yang melemahkan efektivitas penegakan hukumnya. Pasal-pasal yang ada belum mendefinisikan deepfake secara eksplisit sebagai entitas hukum tersendiri, sehingga penerapan Pasal 27, 28, dan 35 masih memerlukan penafsiran ekstensif yang rentan terhadap ketidakpastian hukum. Penelitian ini merekomendasikan kriminalisasi khusus terhadap pembuatan dan penyebaran deepfake ilegal serta penguatan mekanisme pembuktian berbasis forensik digital.

Kata Kunci: deepfake; kecerdasan buatan; pertanggungjawaban pidana; UU ITE; perlindungan hukum

ABSTRACT

The advancement of Artificial Intelligence (AI) technology has given rise to deepfake—a digital manipulation capable of generating synthetic visual and audio content indistinguishable from authentic material. In Indonesia, deepfake misuse has evolved into a tangible threat, particularly in financial fraud and nonconsensual pornographic content (revenge porn). This research critically examines the adequacy of criminal provisions in Law Number 1 of 2024 on the Second Amendment to the ITE Law (New ITE Law) in prosecuting deepfake perpetrators. Employing a normative juridical method supplemented by comparative and conceptual approaches, this study finds that despite significant reforms, several legal loopholes persist that undermine enforcement effectiveness. Existing provisions do not explicitly define deepfake as a distinct legal entity, rendering the application of Articles 27, 28, and 35

Article History

Received: Juni 2026

Reviewed: Juni 2026

Published: Juni 2026

Copyright : Author

Publish by : CAUSA



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

dependent on extensive interpretation susceptible to legal uncertainty. The research recommends specific criminalization of illegal deepfake creation and distribution, alongside strengthened digital forensic evidence mechanisms.

Keywords: *deepfake; artificial intelligence; criminal liability; ITE Law; legal protection*

I. PENDAHULUAN

A. Latar Belakang

Revolusi industri keempat telah membawa transformasi mendalam terhadap berbagai dimensi kehidupan manusia, tidak terkecuali dalam dunia hukum dan kejahatan digital. Salah satu produk paling mengkhawatirkan dari kemajuan kecerdasan buatan adalah teknologi deepfake—sebuah mekanisme rekayasa konten digital berbasis pembelajaran mesin (machine learning) yang mampu menciptakan gambar, video, atau rekaman suara palsu dengan tingkat presisi yang mengagumkan sekaligus mengerikan. Berbeda dengan manipulasi foto atau video konvensional yang masih dapat diidentifikasi secara visual, deepfake menggunakan model jaringan saraf tiruan (deep neural networks) untuk mensintesis wajah, ekspresi, dan suara seseorang sedemikian rupa sehingga hasilnya hampir mustahil dibedakan dari konten otentik (Mirsky & Lee, 2021).

Di Indonesia, penyalahgunaan deepfake telah berkembang menjadi ancaman nyata. Laporan Otoritas Jasa Keuangan (OJK, 2023) mencatat peningkatan 43% kasus penipuan digital yang diduga melibatkan teknologi klonasi identitas berbasis AI. Sementara itu, Komnas Perempuan (2023) melaporkan lonjakan 67% kasus Kekerasan Berbasis Gender Online (KBGO) dibandingkan tahun sebelumnya, dengan sebagian besar korban adalah perempuan yang wajahnya disisipkan ke dalam konten pornografi secara paksa. Merespons eskalasi ancaman ini, pemerintah mengesahkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE (selanjutnya disebut UU ITE Baru) yang diharapkan mampu menutup celah regulasi yang ada.

Namun pertanyaan mendasar yang belum terjawab secara tuntas adalah apakah ketentuan pidana dalam UU ITE Baru tersebut benar-benar cukup kokoh untuk menjerat pelaku penyalahgunaan deepfake, atau justru masih menyisakan ruang-ruang abu-abu yang dapat dimanfaatkan sebagai celah hukum. Pertanyaan inilah yang menjadi inti dari penelitian ini.

B. Research Gap dan Tujuan Penelitian

Kajian akademik domestik yang ada masih terbatas pada analisis UU ITE versi sebelumnya (UU No. 19 Tahun 2016), sehingga relevansinya terhadap UU ITE Baru yang disahkan tahun 2024 perlu dikaji ulang secara komprehensif (Wahyudi & Prabowo, 2022). Kajian yang berfokus pada aspek teknis deepfake juga seringkali mengabaikan dimensi hukumnya, sementara kajian hukum yang ada cenderung deskriptif dan

kurang kritis dalam mengidentifikasi celah regulasi yang nyata. Kesenjangan ini menjadi semakin urgen mengingat para penegak hukum memerlukan panduan yang jelas dalam menghadapi kasus-kasus deepfake yang belum memiliki preseden yurisprudensi di Indonesia.

Bertolak dari latar belakang tersebut, penelitian ini dirumuskan dengan tiga tujuan: pertama, menjelaskan secara komprehensif bahaya sosial dan hukum yang ditimbulkan oleh teknologi deepfake; kedua, menganalisis kritis kecukupan pasal-pasal UU ITE Baru untuk menjerat pelaku deepfake; dan ketiga, merumuskan rekomendasi konkret mengenai penafsiran hukum yang berlaku (*ius constitutum*) dan arah pembaruan hukum pidana yang ideal (*ius constituendum*).

II. TINJAUAN PUSTAKA

A. Deepfake: Definisi, Cara Kerja, dan Tipologi

Istilah "deepfake" merupakan gabungan dari "deep learning" dan "fake", pertama kali muncul sebagai fenomena publik sekitar tahun 2017. Secara teknis, deepfake bekerja dengan memanfaatkan arsitektur Generative Adversarial Networks (GANs), yakni sepasang jaringan saraf tiruan yang saling berkompetisi: satu jaringan (generator) bertugas menciptakan konten palsu, sementara jaringan lainnya (discriminator) bertugas mendeteksi kepalsuan tersebut. Melalui iterasi pembelajaran berulang, generator terus meningkatkan kualitas hasilnya hingga discriminator tidak lagi mampu membedakannya dari yang asli (Chesney & Citron, 2019).

Dalam konteks kejahatan, penyalahgunaan deepfake dapat diklasifikasikan dalam beberapa tipologi utama. Pertama, pornografi nonconsensual (Non-Consensual Intimate Images/NCII). Kedua, penipuan identitas (identity fraud), termasuk pembuatan video seolah-olah seseorang mengucapkan sesuatu yang tidak pernah dilakukannya. Ketiga, manipulasi politik yang digunakan untuk menciptakan video palsu pemimpin negara guna mendestabilisasi kepercayaan publik (Vaccari & Chadwick, 2020). Studi Deeptrace Labs (2019) menemukan bahwa 96% dari seluruh konten deepfake di internet bersifat pornografi, dan hampir seluruhnya merupakan rekayasa wajah perempuan.

B. Teori Pertanggungjawaban Pidana

Dalam doktrin hukum pidana, pertanggungjawaban pidana (criminal liability) didasarkan pada dua elemen fundamental: *actus reus* (perbuatan jahat) dan *mens rea* (niat jahat). Seseorang baru dapat dipidana apabila terbukti telah melakukan perbuatan yang dilarang hukum dan dilakukan dengan kesengajaan atau kelalaian (Moeljatno, 2008). Dalam kaitannya dengan kejahatan deepfake, penerapan teori ini menimbulkan tantangan karena perbuatan yang relevan mencakup spektrum luas—mulai dari pembuatan konten, distribusinya, hingga penggunaannya untuk penipuan.

Selain teori pertanggungjawaban individu, teori pertanggungjawaban korporasi melalui konsep *directing mind and will* juga relevan untuk platform digital yang memfasilitasi distribusi konten deepfake. Di Indonesia, pertanggungjawaban korporasi dalam ranah hukum pidana kini secara eksplisit diakui dalam Pasal 52A UU ITE Baru (Clough, 2010).

C. Kerangka Hukum Siber Indonesia dan Komparasi Global

UU ITE Baru membawa beberapa perubahan substantif: penambahan klausul perlindungan terhadap kekerasan berbasis gender online (KBGO), penegasan kewajiban platform digital untuk moderasi konten secara aktif, serta penguatan ketentuan mengenai bukti elektronik. Meski demikian, kebaruan-kebaruan ini belum sepenuhnya menjawab tantangan spesifik yang ditimbulkan oleh teknologi deepfake (Djafar, 2024).

Perbandingan internasional menunjukkan tren global menuju kriminalisasi eksplisit deepfake. Amerika Serikat menerapkan kombinasi regulasi negara bagian dan federal, di mana beberapa negara bagian seperti California dan Virginia telah mengkriminalisasikan deepfake pornografi secara spesifik (Jeong, 2021). Uni Eropa melalui AI Act 2024 mengklasifikasikan sistem AI yang digunakan untuk manipulasi konten berbahaya sebagai high-risk AI system yang tunduk pada regulasi ketat (European Parliament, 2024). Korea Selatan pada tahun 2020 telah secara tegas mengamendemen undang-undang perlindungan dari kekerasan seksual untuk mengkriminalisasikan deepfake pornografi dengan ancaman pidana hingga 5 tahun (Kim, 2021).

D. Penelitian Terdahulu

Chesney dan Citron (2019) dalam karya mereka *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* menjadi referensi paling komprehensif dalam memetakan dimensi ancaman deepfake dari perspektif hukum dan keamanan nasional. Dari kajian domestik, Wahyudi dan Prabowo (2022) mengidentifikasi bahwa UU ITE Perubahan Pertama belum memiliki ketentuan yang secara eksplisit mengatur deepfake. Setiawan (2023) menemukan bahwa rendahnya literasi hukum digital di kalangan penegak hukum menjadi hambatan signifikan. Cahyadi dan Ramadhan (2024) menyoroti bahwa hakim di Indonesia belum memiliki panduan yurisprudensi yang memadai untuk menghadapi bukti forensik digital yang semakin kompleks.

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif (normative juridical research), yaitu penelitian yang mendasarkan kajiannya pada bahan-bahan hukum untuk menemukan dan menganalisis norma-norma hukum yang relevan (Marzuki, 2011). Metode ini dilengkapi dengan pendekatan komparatif untuk memahami regulasi deepfake di negara-negara lain, dan pendekatan konseptual untuk membangun kerangka teoritis dalam menganalisis permasalahan hukum yang belum memiliki rujukan yurisprudensi yang mapan.

Bahan hukum primer mencakup Undang-Undang Nomor 1 Tahun 2024, Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS), dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Bahan hukum sekunder meliputi jurnal ilmiah hukum dan teknologi, laporan resmi lembaga negara, serta

dokumen kebijakan publik yang berkaitan dengan regulasi AI dan kejahatan siber. Analisis dilakukan melalui interpretasi gramatikal, sistematis, dan teleologis (Rahardjo, 2014).

IV. HASIL DAN PEMBAHASAN

A. Bahaya Nyata Deepfake: Dari Teknologi ke Kejahatan

1. Deepfake sebagai Instrumen Penipuan Finansial

Manifestasi paling merusak dari penyalahgunaan deepfake adalah penggunaannya sebagai alat penipuan finansial. Berbeda dengan penipuan konvensional, deepfake memungkinkan pelaku untuk benar-benar "menjadi" orang lain dengan meminjam wajah dan suara seseorang yang dipercaya oleh calon korban. Kasus paling mencolok terdokumentasi di Hong Kong pada Februari 2024, di mana seorang karyawan keuangan tertipu mentransfer sekitar HK\$200 juta setelah mengikuti panggilan video konferensi yang seluruh pesertanya adalah deepfake dari para petinggi perusahaan (CNN, 2024).

Laporan OJK (2023) mencatat peningkatan 43% kasus penipuan yang melibatkan identitas palsu secara digital, dengan sejumlah kasus diduga menggunakan teknologi klonasi suara (voice cloning) berbasis AI. Yang membuat deepfake finansial begitu berbahaya adalah kemampuannya mengeksploitasi mekanisme kepercayaan kognitif manusia yang paling mendasar: pengenalan wajah. Ketika mekanisme ini dieksploitasi oleh deepfake, korban seringkali tidak memiliki kecurigaan sedikit pun—kondisi yang oleh para ahli forensik psikologi disebut sebagai trust exploitation (Tolosana et al., 2020).

2. Deepfake dan Pornografi Nonconsensual

Dimensi paling mengerikan dari penyalahgunaan deepfake adalah penerapannya dalam pornografi nonconsensual. Jika revenge porn konvensional menggunakan konten nyata yang pernah dibuat bersama korban, deepfake revenge porn tidak memerlukan konten asli sama sekali—cukup dengan foto wajah korban dari media sosial, teknologi ini dapat memproduksi konten pornografi seolah-olah korban menjadi pemainnya (Citron & Chesney, 2019). Cyber Civil Rights Initiative (2022) menemukan bahwa 93% korban deepfake nonconsensual mengalami dampak psikologis serius, termasuk kecemasan, depresi, dan pikiran untuk mengakhiri hidup, sementara 54% melaporkan kehilangan pekerjaan akibat konten tersebut.

Komnas Perempuan (2023) mencatat lonjakan 67% kasus KBGO dibandingkan tahun sebelumnya, dengan mayoritas korban adalah perempuan berusia 18-35 tahun. Yang memperparah situasi ini adalah sifat viral konten digital yang sulit dihapus secara permanen—sekali diunggah, konten deepfake dapat menyebar ke ribuan platform lintas yurisdiksi, sehingga bahkan jika pelaku dipidana sekalipun, konten yang menjadi sumber penderitaan korban mungkin tidak pernah sepenuhnya hilang dari ruang digital.

3. Ancaman terhadap Demokrasi dan Keamanan Nasional

Di luar dampak individual, deepfake menyimpan potensi destruktif terhadap tatanan demokrasi. Kemampuannya menciptakan video palsu tokoh publik yang mengucapkan pernyataan provokatif dapat

memicu kepanikan massal atau krisis diplomatik sebelum konten tersebut sempat difalsifikasi (Vaccari & Chadwick, 2020). Dalam konteks pemilu Indonesia 2024, kekhawatiran mengenai potensi penggunaan deepfake untuk disinformasi politik telah mendapat perhatian dari Bawaslu (2024), meskipun regulasi spesifik untuk menanganinya masih sangat minim.

B. Analisis Yuridis UU ITE Baru dalam Perspektif Deepfake

1. Pasal-Pasal Relevan dan Potensi Penerapannya

Setidaknya terdapat enam klaster pasal dalam kerangka hukum positif Indonesia yang secara potensial dapat diterapkan pada kasus penyalahgunaan deepfake.

Klaster pertama adalah Pasal 27 UU ITE Baru yang mengatur larangan distribusi konten yang memuat pelanggaran kesusilaan (ayat 1), pengancaman (ayat 4), serta pencemaran nama baik (ayat 3). Untuk kasus deepfake pornografi, Pasal 27 ayat 1 menjadi yang paling relevan. Namun rumusan pasal ini tidak secara eksplisit menyebutkan konten sintetis atau hasil rekayasa AI, membuka celah argumentasi defensif bahwa konten tersebut adalah "fiksi" dan tidak menampilkan orang nyata.

Klaster kedua adalah Pasal 35 yang melarang manipulasi, penciptaan, atau perubahan informasi elektronik dengan tujuan agar informasi tersebut seolah-olah autentik—pasal yang secara teoritis paling dekat dengan karakteristik deepfake, namun tidak mencakup deepfake satire atau parodi. Klaster ketiga adalah Pasal 14 UU TPKS yang mengatur pidana bagi yang memproduksi atau menyebarkan konten seksual melalui sistem elektronik tanpa persetujuan—ketentuan yang lebih tepat sasaran untuk deepfake pornografi. Klaster keempat adalah Pasal 65 UU PDP yang mengancam pidana bagi yang memproses data biometrik, termasuk wajah dan suara seseorang, tanpa hak.

2. Lima Celah Hukum yang Teridentifikasi

Celah pertama adalah ketiadaan definisi eksplisit tentang deepfake dalam UU ITE Baru. Hukum pidana Indonesia menganut prinsip legalitas yang ketat—*nullum crimen sine lege*—yang mengharuskan suatu perbuatan didefinisikan secara jelas sebelum dapat dipidana. Ketika undang-undang tidak menyebutkan deepfake secara eksplisit, jaksa penuntut harus melakukan "lompatan analogis" yang rawan dibantah oleh penasihat hukum pelaku (Marzuki, 2011).

Celah kedua adalah kompleksitas pembuktian yang melampaui kapasitas teknis aparat penegak hukum saat ini. Standar autentikasi alat bukti elektronik dalam Pasal 5 dan Pasal 11 UU ITE Baru belum mengakomodasi prosedur pembuktian untuk konten sintetis berbasis AI, sementara jumlah ahli forensik digital bersertifikasi yang mampu menganalisis deepfake di Indonesia masih sangat terbatas (Cahyadi & Ramadhan, 2024).

Celah ketiga berkaitan dengan yurisdiksi lintas batas. Meski Pasal 2 UU ITE Baru menyatakan keberlakuannya di luar wilayah Indonesia apabila akibatnya dirasakan di Indonesia, implementasinya menghadapi tantangan mekanisme kerja sama hukum internasional (MLAT) yang terbatas dan ketidakmauan platform asing untuk tunduk pada hukum Indonesia (Wahyudi & Prabowo, 2022). Celah

keempat adalah absennya standar tanggung jawab platform digital atas konten deepfake. Celah kelima adalah minimnya mekanisme pemulihan korban yang terintegrasi, mulai dari penghapusan konten darurat hingga kompensasi dan pendampingan psikologis (Citron, 2022).

3. Perbandingan: Pelajaran dari Regulasi Asing

Pengalaman Korea Selatan yang secara tegas mengkriminalisasikan deepfake pornografi sejak 2020 dengan ancaman penjara 5 tahun memberikan pelajaran bahwa pendekatan langsung dan spesifik lebih efektif dalam memberikan kepastian hukum dan efek deterren dibandingkan mengandalkan interpretasi pasal-pasal umum (Kim, 2021). Sementara AI Act Uni Eropa 2024 menunjukkan pentingnya mengatur deepfake dalam konteks regulasi AI yang lebih holistik, suatu pendekatan yang juga perlu dipertimbangkan Indonesia dalam rencana regulasi AI nasional yang sedang disusun (European Parliament, 2024).

C. Tafsir Hakim dan Konstruksi Hukum atas Deepfake

Ketika kasus penyalahgunaan deepfake masuk ke pengadilan, hakim dihadapkan pada tantangan penafsiran yang belum pernah ada presedennya. Pandangan bahwa hakim bukan sekadar corong undang-undang (*la bouche de la loi*) tetapi memiliki keleluasaan untuk melakukan penemuan hukum (*rechtsvinding*) menjadi penting (Wahyudi & Prabowo, 2022). Secara konkret, hakim dapat menerapkan interpretasi teleologis untuk menafsirkan Pasal 35 UU ITE Baru secara lebih luas—bahwa pembuatan konten deepfake untuk tujuan menipu atau merugikan orang lain masuk dalam cakupan pasal tersebut, didukung oleh Naskah Akademik UU ITE Baru yang menyatakan kehendak pembentuk undang-undang untuk mengantisipasi perkembangan teknologi yang belum terprediksi.

Hakim juga perlu memberikan perhatian khusus pada standar penerimaan bukti forensik digital: ahli harus memiliki sertifikasi internasional dalam forensik digital; metodologi yang digunakan harus berdasarkan standar ilmiah yang dapat diverifikasi; dan temuan ahli harus disajikan dengan tingkat kepastian yang jelas. Penerbitan PERMA atau SEMA yang mengatur standar pembuktian untuk kasus kejahatan berbasis AI menjadi kebutuhan yang mendesak (Cahyadi & Ramadhan, 2024).

D. Ius Constituendum: Rekomendasi Pembaruan Hukum Pidana

1. Kriminalisasi Khusus Deepfake

Rekomendasi utama penelitian ini adalah memasukkan ketentuan kriminalisasi khusus terhadap penyalahgunaan deepfake dalam pembaruan KUHP atau revisi UU ITE berikutnya. Rumusan yang ideal mencakup: definisi yang jelas tentang deepfake dan konten sintetis berbasis AI dalam konteks hukum pidana; gradasi ancaman pidana berdasarkan tingkat kesengajaan dan dampak yang ditimbulkan; serta kewajiban pelabelan (*disclosure obligation*) bagi konten sintetis yang dibuat untuk keperluan sah seperti hiburan, satire, atau penelitian (Jeong, 2021).

2. Reformasi Pertanggungjawaban Platform Digital

Model pertanggungjawaban berbasis pengetahuan yang dimodifikasi (modified knowledge-based liability) diusulkan: platform tidak secara otomatis bertanggung jawab atas konten deepfake yang diunggah pengguna, namun akan dikenakan sanksi apabila terbukti mengetahui adanya konten deepfake ilegal di platformnya dan gagal mengambil tindakan dalam jangka waktu yang ditentukan, misalnya 24 jam setelah menerima laporan. Model ini menyeimbangkan perlindungan korban dan kebebasan berekspresi digital (Simons, 2020).

3. Perlindungan dan Pemulihan Korban

Pembaruan hukum yang berperspektif korban (victim-centered approach) mencakup: hak atas penghapusan konten darurat yang dapat dikabulkan pengadilan dalam 24-48 jam; hak atas kompensasi finansial dari pelaku dan platform yang lalai; serta akses wajib ke layanan konseling psikologis yang dibiayai negara. Ketentuan ini perlu diintegrasikan secara sistematis dengan mekanisme UU TPKS dan UU PDP yang sudah ada (Citron, 2022; Lembaga Perlindungan Saksi dan Korban [LPSK], 2023).

4. Penguatan Kapasitas Kelembagaan

Dalam jangka pendek, Polri perlu membentuk unit khusus kejahatan berbasis AI dengan personel forensik digital yang tersertifikasi. Kejaksaan Agung perlu mengembangkan panduan penuntutan khusus untuk kasus deepfake. Dalam jangka menengah dan panjang, Indonesia perlu mengintensifkan kerja sama internasional dalam penanganan kejahatan deepfake lintas batas, termasuk melalui partisipasi aktif dalam Budapest Convention on Cybercrime (Interpol, 2021).

V. KESIMPULAN

Penelitian ini menarik tiga kesimpulan utama. Pertama, teknologi deepfake berbasis AI telah berkembang menjadi ancaman hukum dan sosial yang nyata di Indonesia, dengan dua modus utama yang paling merusak: penipuan finansial yang mengeksploitasi kepercayaan interpersonal melalui klonasi identitas visual, dan pornografi nonconsensual yang menghancurkan kehidupan korban melalui rekayasa konten seksual tanpa persetujuan.

Kedua, meskipun UU ITE Baru (UU No. 1 Tahun 2024) telah mengalami pembaruan yang lebih komprehensif, ketentuan pidananya masih belum cukup kuat untuk menjerat pelaku penyalahgunaan deepfake secara efektif. Lima celah hukum yang teridentifikasi—ketiadaan definisi eksplisit deepfake, kompleksitas pembuktian, tantangan yurisdiksi lintas batas, ketidakjelasan tanggung jawab platform, dan minimnya mekanisme pemulihan korban—berpotensi melemahkan efektivitas penegakan hukum secara signifikan.

Ketiga, menghadapi kekosongan regulasi yang ada, hakim dapat menerapkan interpretasi teleologis dan sistematis untuk memperluas cakupan Pasal 35 UU ITE Baru dan mensinkronisasikannya dengan UU TPKS dan UU PDP. Namun solusi jangka panjang yang sesungguhnya hanya dapat dicapai melalui kriminalisasi khusus deepfake, reformasi pertanggungjawaban platform digital, penguatan

mekanisme perlindungan korban, dan peningkatan kapasitas kelembagaan penegak hukum secara menyeluruh.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.
<https://peraturan.bpk.go.id/Details/287837>

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120. <https://peraturan.bpk.go.id/Details/219121>

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. <https://peraturan.bpk.go.id/Details/232104>

Buku

Clough, J. (2010). *Principles of cybercrime*. Cambridge University Press.

Marzuki, P. M. (2011). *Penelitian hukum* (Ed. rev.). Kencana Prenada Media Group.

Moeljatno. (2008). *Asas-asas hukum pidana* (Ed. 8). Rineka Cipta.

Rahardjo, S. (2014). *Ilmu hukum*. Citra Aditya Bakti.

Artikel Jurnal, Laporan, dan Sumber Lain

Badan Pengawas Pemilihan Umum Republik Indonesia. (2024). *Laporan pengawasan pemilu 2024: Ancaman disinformasi digital dan deepfake*. Bawaslu RI. <https://www.bawaslu.go.id/laporan/pengawasan-pemilu-2024>

Cahyadi, A., & Ramadhan, F. (2024). Standar pembuktian kejahatan siber berbasis artificial intelligence di pengadilan Indonesia. *Jurnal Hukum dan Teknologi Indonesia*, 5(1), 45-67.
<https://doi.org/10.21787/jhti.5.1.2024.45-67>

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. <https://doi.org/10.15779/Z38RV0D15J>

Citron, D. K. (2022). The case for a federal deepfake prohibition. *University of Colorado Law Review*, 93(2), 401-463. <https://scholar.law.colorado.edu/lawreview/vol93/iss2/3>

Cyber Civil Rights Initiative. (2022). *2022 CCRI survey results: Non-consensual pornography and deepfakes*. CCRI. https://cybercivilrights.org/wp-content/uploads/2022/01/CCRI_2022_Report.pdf

Cyberspace Administration of China. (2022). *Provisions on the management of deep synthesis internet information services*. CAC. https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

- Djafar, W. (2024). Reformasi UU ITE 2024 dan tantangan perlindungan kebebasan berekspresi di era kecerdasan buatan. *Jurnal Hak Asasi Manusia*, 15(1), 12-34. <https://doi.org/10.33476/jham.15.1.2024.12-34>
- European Parliament. (2024). *Artificial Intelligence Act (Regulation EU 2024/1689)*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- Interpol. (2021). *Cybercrime threats during COVID-19 and beyond: INTERPOL report*. Interpol. <https://www.interpol.int/en/content/download/16108/file/COVID-19%20Cybercrime%20Analysis%20Report.pdf>
- Jeong, A. (2021). Regulating deepfakes: Legal and ethical considerations. *Harvard Journal of Law & Technology*, 34(2), 615-658. <https://jolt.law.harvard.edu/assets/articlePDFs/v34/34HarvJLTech615.pdf>
- Kim, S. (2021). South Korea's response to deepfake pornography: Legal analysis and policy implications. *Asian Journal of Law and Society*, 8(3), 589-612. <https://doi.org/10.1017/als.2021.19>
- Komisi Nasional Anti Kekerasan Terhadap Perempuan. (2023). *Catatan tahunan 2023: Kekerasan berbasis gender online dan tantangan keadilan digital*. Komnas Perempuan. <https://komnasperempuan.go.id/catatan-tahunan-2023>
- Lembaga Perlindungan Saksi dan Korban. (2023). *Laporan tahunan 2023: Perlindungan korban kekerasan berbasis teknologi*. LPSK RI. <https://www.lpsk.go.id/berita/laporantahunan2023>
- Lim, M. (2020). The politics of cyber law: Internet and the ITE Law in Indonesia. *Indonesia and the Malay World*, 48(140), 86-103. <https://doi.org/10.1080/13639811.2020.1717482>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1-41. <https://doi.org/10.1145/3425780>
- Otoritas Jasa Keuangan. (2023). *Statistik penanganan pengaduan konsumen dan masyarakat: Laporan triwulan III 2023*. OJK. <https://ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Statistik-Pengaduan-2023.pdf>
- Setiawan, B. (2023). Literasi hukum digital aparat penegak hukum dalam menghadapi kejahatan berbasis AI di Indonesia. *Jurnal Penelitian Hukum De Jure*, 23(2), 201-218. <https://doi.org/10.30641/dejure.2023.V23.201-218>
- Simons, M. (2020). Platform liability for AI-generated content: Navigating between strict and negligence standards. *Journal of Internet Law*, 24(3), 1-15. <https://www.journalofinternetlaw.com/platform-liability-ai-generated-content>
- Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131-148. <https://doi.org/10.1016/j.inffus.2020.06.014>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, 6(1), 1-13. <https://doi.org/10.1177/2056305120903408>
- Wahyudi, R., & Prabowo, H. (2022). Celah hukum dalam penanganan kejahatan deepfake menurut UU ITE dan KUHP Indonesia. *Padjadjaran Journal of Law*, 9(3), 412-435. <https://doi.org/10.22304/pjih.v9n3.a4>