

Menakar Intermediary Liability: Tantangan Platform Digital dalam Mengawasi Deepfake Sexual Content

Sintia Buana Wulandari¹, Anneke Setiyawati², Mega Yulanda³, Muhammad Rizky

Pratama Saputra⁴, Surya Bagus Pambudi⁵

^{1,2,3,4,5}Universitas Brawijaya, Malang, Indonesia

Corresponding author e-mail: sintiabuanash@gmail.com

Article History: Received on 01 Oktober 2025, Revised on 15 November 2025,

Published on 01 Desember 2025

Abstract: Kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI) mendorong munculnya deepfake sexual content yang memanipulasi citra dan suara seseorang untuk tujuan seksual tanpa izin, sehingga menimbulkan bentuk baru kekerasan seksual berbasis digital. Penyebarannya melalui platform digital menghadirkan persoalan serius mengenai intermediary liability atau tanggung jawab platform sebagai perantara informasi. Meskipun Indonesia telah memiliki sejumlah regulasi seperti UU ITE 1/2024, UU TPKS 12/2022, Permenkominfo 5/2020, dan UU PDP 27/2022, belum terdapat pengaturan yang spesifik dan komprehensif terkait kewajiban preventif dan akuntabilitas platform dalam mencegah serta menindak konten deepfake seksual. Penelitian ini menggunakan metode yuridis normatif melalui analisis peraturan perundang-undangan, doktrin, dan praktik internasional untuk mengidentifikasi kekosongan hukum (lacuna legis) dan tantangan implementasi perlindungan korban. Hasil penelitian menunjukkan bahwa ketiadaan standar tanggung jawab yang jelas menyebabkan platform digital beroperasi dalam ruang abu-abu hukum, sementara korban kesulitan memperoleh pemulihan efektif. Oleh karena itu, penelitian ini merekomendasikan model intermediary liability berbasis notice-and-takedown, due diligence obligations, dan kewajiban transparansi platform, serta urgensi pembentukan otoritas pengawas layanan digital untuk memperkuat kepastian, perlindungan, dan akuntabilitas hukum dalam menghadapi kejahatan seksual berbasis deepfake di Indonesia.

Keywords: Intermediary Liability, Kepastian Hukum, Konten Ilegal, Deepfake Sexual Content, Platform Digital.

A. Introduction

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) membawa transformasi besar dalam ekosistem digital, termasuk lahirnya teknologi *deepfake* yang mampu memanipulasi wajah dan suara seseorang secara sangat realistik (Chesney & Citron, 2019). Meski memiliki potensi positif di bidang kreatif, hiburan, dan edukasi, teknologi ini menimbulkan ancaman serius ketika dimanfaatkan untuk membuat dan menyebarkan konten seksual tanpa persetujuan korban. Fenomena *deepfake sexual content* menjadi bentuk kekerasan seksual berbasis digital yang dapat menghancurkan reputasi, merusak martabat, serta mengganggu kondisi psikologis korban secara mendalam (Berryman, 2023). Di tengah masifnya penyalahgunaan deepfake, platform

digital memiliki posisi penting sebagai *intermediaries* yang menghubungkan pengguna dalam pertukaran informasi global. Namun, muncul pertanyaan mengenai sejauh mana platform dapat dan seharusnya bertanggung jawab dalam mencegah serta menangani penyebaran konten ilegal yang diproduksi oleh pengguna (Taeihagh, 2021).

Isu *intermediary liability* semakin kompleks karena teknologi deepfake berkembang sangat cepat dan sering kali lebih maju dibandingkan sistem moderasi konten yang digunakan platform digital. Sebagian besar platform masih bergantung pada pelaporan pengguna (*notice and takedown*) yang bersifat reaktif dan terlambat, sehingga konten merugikan telah tersebar luas sebelum dapat dihapus (West, 2022). Selain itu, tantangan yurisdiksi lintas negara menyebabkan kesulitan dalam penegakan hukum karena penyebaran konten bisa terjadi secara global dalam hitungan detik (Geuss, 2020). Kondisi ini memperlihatkan adanya kesenjangan antara perkembangan teknologi dengan sistem pengawasan platform dan kebijakan hukum yang mengaturnya.

Beberapa penelitian sebelumnya menyoroti bahwa kerangka regulasi *intermediary liability* di berbagai negara masih beragam dan belum memberikan kepastian bagi platform dalam mengatasi konten bermasalah. Pendekatan *safe harbor*, misalnya, memberikan kekebalan hukum selama platform merespons laporan secara cepat, namun dianggap tidak adaptif terhadap ancaman deepfake seksual yang sangat merusak dan sulit dideteksi (Keller & Leerssen, 2020). Di sisi lain, pendekatan tanggung jawab ketat berpotensi menghambat kebebasan berekspresi serta inovasi teknologi pada platform digital (Tambini, 2021). Dengan demikian, dibutuhkan keseimbangan yang jelas antara perlindungan korban dan kebebasan digital dalam kebijakan pengawasan konten di ruang siber.

Di Indonesia, urgensi pembahasan ini semakin menguat seiring meningkatnya kasus kekerasan seksual berbasis digital, sementara pengaturan hukum yang secara spesifik mengatasi *deepfake sexual content* masih sangat terbatas (Amalia, 2024). Moderasi konten yang dilakukan platform digital belum mampu menjamin perlindungan yang optimal bagi korban, terutama karena tidak adanya regulasi komprehensif yang menekankan tanggung jawab preventif platform dalam mencegah produksi dan distribusi konten seksual manipulatif. Situasi ini memperlihatkan adanya kebutuhan mendesak untuk merumuskan regulasi yang menakar peran dan tanggung jawab platform dalam konteks perkembangan teknologi AI.

Melihat dinamika tersebut, penelitian mengenai "Menakar Intermediary Liability: Tantangan Platform Digital dalam Mengawasi Deepfake Sexual Content" menjadi penting dilakukan untuk memberikan pemahaman komprehensif mengenai posisi hukum, tantangan implementasi, serta model tanggung jawab platform yang ideal dalam mencegah dan menangani penyebaran konten seksual deepfake. Selain memiliki kontribusi konseptual dalam pengembangan regulasi keamanan digital, penelitian ini juga memberikan kontribusi praktis sebagai rekomendasi kebijakan bagi pemerintah dan platform digital untuk memperkuat perlindungan korban dan

mewujudkan ruang siber yang aman, beretika, serta berkeadilan bagi seluruh pengguna.

B. Methods

Penelitian ini menggunakan metode penelitian hukum normatif (juridis normatif) untuk menganalisis secara mendalam pengaturan *intermediary liability* dalam penanganan *deepfake sexual content* pada platform digital di Indonesia. Metode ini dipilih karena penelitian bertujuan mengkaji norma hukum tertulis dan doktrin yang mengatur tanggung jawab platform digital dalam mencegah dan mengatasi penyebaran konten seksual berbasis manipulasi teknologi kecerdasan buatan. Menurut Marzuki (2010), penelitian hukum normatif menempatkan hukum sebagai norma yang bersumber dari peraturan perundang-undangan, prinsip hukum, dan literatur hukum yang relevan.

Pendekatan penelitian yang digunakan mencakup dua pendekatan. Pertama, Pendekatan Perundang-undangan (Statute Approach), digunakan untuk menganalisis ketentuan-ketentuan hukum positif Indonesia terkait kekerasan seksual berbasis digital dan perlindungan data pribadi. Sumber hukum yang ditelaah antara lain Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penanganan Konten Negatif pada Platform Sistem Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kedua, Pendekatan Konseptual (Conceptual Approach), digunakan untuk menggali konsep-konsep penting seperti *intermediary liability*, *rechtsvacuum* (kekosongan hukum), dan perlindungan korban dalam ruang siber, sehingga penelitian memiliki landasan teoritis yang kuat dalam merumuskan tanggung jawab platform digital. Konsep *intermediary liability* dan tantangan regulasi terhadap konten deepfake sudah banyak diulas dalam literatur internasional. Sebagai contoh, Ma'arif (2025) menemukan bahwa penyalahgunaan deepfake pornografi memunculkan persoalan etika, privasi, dan regulasi.

Bahan hukum yang digunakan meliputi: (1) bahan hukum primer, berupa peraturan perundang-undangan yang menjadi objek utama analisis; (2) bahan hukum sekunder, berupa buku, jurnal ilmiah, artikel hukum, hasil penelitian, dan putusan pengadilan yang relevan dengan isu deepfake dan kekerasan seksual digital; (3) bahan hukum tersier, berupa kamus hukum, ensiklopedia, dan sumber pendukung lainnya yang menjelaskan terminologi dan memperkuat pemahaman terhadap konsep hukum yang diteliti (Marzuki, 2017).

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan yang sistematis dengan menelusuri peraturan dan literatur melalui basis data resmi pemerintah, jurnal ilmiah nasional maupun internasional, serta sumber akademik kredibel lainnya. Proses ini bertujuan untuk memastikan bahwa seluruh bahan hukum yang digunakan memiliki validitas dan relevansi yang tinggi terhadap

masalah penelitian.

Analisis data dilakukan melalui metode analisis kualitatif normatif, yaitu dengan mensistematisasi dan menafsirkan peraturan perundang-undangan serta doktrin hukum guna menemukan kesesuaian atau pertentangan pengaturan, mengidentifikasi *lacuna legis* (kekosongan atau kelemahan hukum), serta menilai aspek kepastian, keadilan, dan kemanfaatan hukum dalam konteks perlindungan korban *deepfake sexual content*. Selanjutnya, data diolah untuk merumuskan model pengaturan dan pengawasan yang ideal serta adaptif terhadap perkembangan teknologi digital, sebagaimana diidentifikasi oleh literatur internasional tentang tantangan regulasi deepfake (Martin, 2025).

Melalui metode penelitian ini, diharapkan penelitian mampu menghadirkan analisis komprehensif yang tidak hanya memperkaya literatur hukum terkait *intermediary liability*, tetapi juga memberikan rekomendasi kebijakan yang aplikatif bagi pemerintah maupun platform digital dalam menciptakan ruang siber yang aman dan melindungi korban dari kejahatan seksual berbasis deepfake.

C. Results and Discussion

Results

Pengaturan Hukum Positif di Indonesia dalam Memberikan Perlindungan terhadap Korban Deepfake sexual content.

Perkembangan teknologi digital telah membawa transformasi besar dalam kehidupan manusia. Kecerdasan buatan atau Artificial Intelligence(AI) kini menjadi bagian yang tak terpisahkan dari aktivitas sehari-hari, mulai dari sektor industri, pendidikan, hingga hiburan. Namun, kemajuan teknologi ini juga melahirkan dimensi baru kejahatan siber, salah satunya melalui deepfake sexual content, yakni penggunaan algoritma AI untuk menciptakan konten pornografi palsu dengan menempelkan wajah seseorang ke tubuh orang lain dalam video atau gambar tanpa izin. Nadea Aulia Putri dan Maria Novita Apriyani dalam penelitiannya menegaskan bahwa permasalahan deepfake di Indonesia bukanlah hal baru, tetapi hingga kini belum ada aturan hukum spesifik yang mengatur penggunaan teknologi AI untuk konten pornografi. Walaupun demikian, hukum positif Indonesia masih memiliki beberapa instrumen yang dapat digunakan untuk menjerat pelaku, seperti UU ITE, UU Pornografi, dan sebagian ketentuan dalam KUHP tentang kesiusilaan. Akan tetapi, penerapannya masih lemah dan belum mampu memberikan perlindungan menyeluruh bagi korban perempuan

Di Indonesia, kerangka hukum positif telah berkembang tetapi masih terdapat lacuna legis terkait fenomena ini. Undang-Undang Nomor 1 Tahun 2024, revisi kedua atas UU ITE 2008 tentang Informasi dan Transaksi Elektronik. mengatur konten elektronik dan transaksi digital, serta menegaskan kewajiban pemerintah dan penyelenggara sistem elektronik untuk menjaga ekosistem digital (Pasal 40A). Namun, UU ITE 1/2024 belum secara eksplisit menyebut "deepfake" atau konten generatif AI sebagai

kategori terpisah, sehingga tanggung jawab platform digital masih belum jelas.

Selanjutnya, UU Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS) mengakui kekerasan seksual berbasis elektronik sebagai tindak pidana, sehingga korban deepfake pornografi dapat memanfaatkan pasal-pasal tersebut untuk menuntut pelaku. Namun, UU TPKS belum mewajibkan platform digital secara proaktif untuk mencegah atau menghapus konten deepfake, sehingga posisi platform sebagai perantara informasi masih berada dalam “ruang abu-abu” hukum.

Selain itu, UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) melindungi data pribadi, termasuk wajah, citra, dan biometrik. Penyebaran deepfake pornografi tanpa izin korban dapat dikualifikasikan sebagai pelanggaran hak atas data pribadi, memberi dasar hukum untuk pemulihan hak, ganti rugi, dan penegakan sanksi administratif maupun pidana.

Lebih lanjut, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 (Permenkominfo 5/2020) tentang Penyelenggara Sistem Elektronik Lingkup Privat mengatur penanganan konten negatif di platform sistem elektronik. Peraturan ini mewajibkan penyelenggara platform untuk menerapkan mekanisme notice-and-takedown, yaitu menanggapi laporan konten ilegal dari pengguna atau otoritas dan menghapus konten yang melanggar ketentuan dalam jangka waktu tertentu. Permenkominfo 5/2020 juga mengatur mekanisme transparansi dan pelaporan konten negatif kepada publik, yang dapat dijadikan instrumen akuntabilitas bagi platform digital.

Meskipun kerangka hukum ini ada, perlindungan korban deepfake pornografi masih menghadapi tantangan signifikan: bukti manipulasi AI sulit dibuktikan di pengadilan, niat pelaku belum selalu jelas, dan penegakan regulasi digital masih terbatas. Dalam praktik penegakan hukum, kasus deepfake pornography di Indonesia masih jarang sampai ke tahap pengadilan. Sebagian besar kasus berhenti pada tahap pelaporan karena lemahnya bukti digital, sulitnya melacak pelaku yang menggunakan akun anonim, serta minimnya kemampuan aparat dalam digital forensics. Penelitian Indah Rohmawati dkk. menegaskan bahwa regulasi yang ada hanya bersifat reaktif, belum preventif. Indonesia memang memiliki mekanisme pelaporan seperti Cyber Crime Police Unit atau Aduan Konten Kominfo, tetapi mekanisme ini lebih banyak menindaklanjuti penghapusan konten daripada pemulihan korban. Artinya, aspek perlindungan psikologis, restitusi, dan rehabilitasi masih sangat minim.

Model Pengaturan Intermediary Liability yang Efektif dan Proporsional

Platform digital menjalankan fungsi sebagai perantara yang menghubungkan pengguna dengan berbagai bentuk konten, namun ketiadaan standar tanggung jawab yang jelas membuat peran tersebut menimbulkan masalah serius. Ketidakpastian regulatif mendorong platform melakukan *over-blocking* demi menghindari risiko hukum, sehingga membatasi kebebasan berekspresi. Pada sisi lain, celah pengawasan memungkinkan persebaran konten ilegal karena tidak ada kewajiban preventif yang

tegas untuk mendeteksi, menilai, atau merespons risiko. Situasi ini menempatkan pelaku usaha terutama platform lokal dalam posisi yang tidak menguntungkan karena harus menafsirkan sendiri batasan hukum yang tidak pasti. Ketidakjelasan ini memperkuat kritik klasik Sudikno mengenai pentingnya *kepastian hukum* sebagai syarat utama berfungsinya sistem hukum yang adil, karena tanpa kepastian, baik pengguna maupun pelaku industri berada dalam ruang digital yang rentan dan tidak terlindungi.

Kelemahan tersebut semakin nyata karena regulasi Indonesia masih mengandalkan pendekatan administratif yang reaktif, yaitu menunggu laporan atau instruksi pemerintah sebelum dilakukan penghapusan konten. Model ini tidak sesuai dengan karakter risiko digital yang dinamis dan bereskalasi cepat. Oleh sebab itu, Indonesia membutuhkan model tata kelola baru yang *risk-based*, proporsional, dan transparan – sebuah pendekatan yang sejalan dengan pemikiran Hazairin mengenai hukum yang harus hidup dan adaptif terhadap perubahan masyarakat serta pandangan Ter Haar tentang pentingnya hubungan konkret antara pengetahuan, kelalaian, dan pertanggungjawaban. Dengan kerangka yang berbasis risiko, kewajiban platform dapat disesuaikan dengan kapasitas dan dampaknya, sementara transparansi memastikan ke-

Dalam merumuskan kerangka intermediary liability, terdapat tiga opsi kebijakan utama yang dapat dipertimbangkan oleh pembuat undang-undang. Opsi pertama adalah mempertahankan model status quo, yaitu pendekatan administratif yang menempatkan pemerintah sebagai penentu utama atas penghapusan konten melalui perintah resmi (takedown order). Meskipun tampak sederhana, pendekatan ini menciptakan ketidakpastian karena tidak adanya standar jelas mengenai validitas laporan, batas waktu respons, dan mekanisme keberatan. Ketidakteraturan ini berpotensi menimbulkan penyalahgunaan kewenangan serta mempertajam ketimpangan antara kekuasaan pemerintah dan hak-hak digital warga.

Opsi kedua adalah penerapan liability ketat, yaitu menempatkan platform sebagai pihak yang bertanggung jawab sepenuhnya atas semua konten pengguna. Pendekatan ini tampak efektif dalam memberantas konten ilegal, tetapi secara praktis bisa menimbulkan konsekuensi yang lebih berbahaya. Platform akan ter dorong melakukan penghapusan berlebihan (over-blocking) untuk menghindari sanksi, sehingga mereduksi kebebasan berekspresi. Selain itu, beban kepatuhan yang tinggi dapat menghambat perkembangan pelaku usaha teknologi lokal dan startup. Banyak yurisdiksi telah meninggalkan pendekatan ini karena bertentangan dengan prinsip proporsionalitas dan safe harbour yang mendukung inovasi.

Opsi ketiga adalah penerapan model terintegrasi, yang mengombinasikan mekanisme responsif (notice-and-takedown), langkah-langkah preventif (due diligence obligations), serta kewajiban akuntabilitas melalui transparansi platform. Model ini memetakan hubungan antara risiko, tanggung jawab, dan kapasitas platform, sehingga menghasilkan tata kelola yang adaptif. Pendekatan ini serasi dengan standar internasional seperti Digital Services Act (DSA) Uni Eropa, namun tetap dapat

dikontekstualisasikan dengan kebutuhan Indonesia seperti penanganan disinformasi, ujaran kebencian, dan penipuan daring. Integrasi ketiga pilar ini memberikan landasan sistemik bagi regulasi yang lebih menyeluruh dan berbasis risiko.

Secara konseptual, opsi terintegrasi sejalan dengan pemikiran para sarjana hukum klasik Indonesia. Ter Haar menegaskan bahwa pertanggungjawaban hukum harus bertolak dari hubungan konkret antara pengetahuan dan kelalaian, bukan sekadar imputasi otomatis. Prinsip ini tercermin dalam mekanisme notice-and-takedown yang tidak membebankan tanggung jawab tanpa dasar. Hazairin, melalui gagasan living law, menekankan bahwa hukum harus memerlukan fungsi antisipatif dalam mengatur dinamika sosial sejalan dengan due diligence sebagai pendekatan pencegahan. Sementara itu, pandangan Sudikno mengenai kepastian hukum yang bertumpu pada keterbukaan dan rasionalitas keputusan memberikan legitimasi akademik bagi kewajiban transparansi platform.

Dengan melihat dinamika teknologi, ekonomi, dan sosial, model terintegrasi menjadi pilihan kebijakan paling tepat. Pendekatan ini tidak hanya mengurangi risiko penyalahgunaan kewenangan pemerintah maupun sensor berlebihan oleh platform, tetapi juga memberikan prediktabilitas bagi para pelaku industri. Pengguna terlindungi melalui mekanisme keberatan dan transparansi, sementara platform memiliki pedoman jelas untuk memenuhi kewajiban hukum tanpa mengorbankan inovasi. Pada akhirnya, model terintegrasi memungkinkan terciptanya ruang digital Indonesia yang aman, demokratis, dan sesuai prinsip negara hukum.

Rekomendasi Utama Pengaturan Intermediary Liability

Rekomendasi pertama adalah penerapan mekanisme notice-and-takedown yang proporsional, yaitu sistem pelaporan dan penghapusan konten yang membedakan antara kategori risiko tinggi dan rendah. Konten berbahaya seperti kekerasan seksual digital, eksloitasi anak, atau *non-consensual deepfake* harus diproses cepat, sementara konten yang berkaitan dengan perdebatan publik memerlukan pemeriksaan tambahan untuk mencegah *over-blocking*. Pendekatan proporsional ini selaras dengan penelitian terbaru yang menunjukkan bahwa sistem penghapusan konten yang terlalu agresif dapat mengancam kebebasan berekspresi dan menghasilkan sensor algoritmik yang tidak akuntabel, sebagaimana diuraikan oleh Keller dalam analisisnya terkait moderasi konten yang efektif tanpa "penyensoran berlebih". Prinsip ini juga sejalan dengan gagasan klasik Sudikno tentang perlunya kepastian mekanisme penegakan untuk memberikan keadilan substantif.

Rekomendasi kedua adalah penguatan due diligence obligations, yaitu kewajiban kehati-hatian platform secara proaktif berdasarkan tingkat risiko sistemnya. Kewajiban ini mencakup audit risiko tahunan, deteksi otomatis untuk konten berbahaya, verifikasi identitas bagi akun berpengaruh publik, serta kebijakan mitigasi risiko algoritmik. Literatur ilmiah internasional menekankan bahwa kewajiban berbasis risiko meningkatkan efektivitas moderasi dan menjaga ruang digital tetap aman, sebagaimana dibahas oleh Gorwa & Garton Ash yang menyatakan bahwa tata kelola platform modern harus menggabungkan *systemic risk assessments* sebagai

komponen inti. Pendekatan ini mencerminkan pandangan Hazairin mengenai hukum yang harus hidup dan adaptif terhadap perkembangan masyarakat.

Rekomendasi ketiga adalah pemberlakuan kewajiban transparansi platform, khususnya mengenai penggunaan algoritma, jumlah permintaan penghapusan konten, dan penggunaan teknologi otomatis. Tanpa transparansi, keputusan moderasi tetap menjadi proses tertutup yang sulit diuji. Jurnal teknologi informasi menunjukkan bahwa transparansi memperkuat akuntabilitas publik dan dapat mengurangi bias algoritmik, sebagaimana dibuktikan dalam penelitian Suzor et al. mengenai *platform governance* dan perlunya “due process” dalam moderasi konten. Pemikiran ini juga sejalan dengan pandangan Ter Haar tentang pentingnya pengetahuan sebagai unsur pembentuk pertanggungjawaban hukum.

Model Kelembagaan yang Disarankan: Pembentukan Digital Services Authority

Untuk mewujudkan regulasi yang konsisten, diperlukan Digital Services Authority (DSA versi Indonesia) yang berperan sebagai otoritas terpusat untuk pengawasan platform digital. DSA ini akan menetapkan standar due diligence, mengawasi mekanisme notice-and-takedown, melakukan audit algoritmik, serta menengahi sengketa antara pengguna dan platform. Model kelembagaan ini mengatasi fragmentasi regulasi Indonesia saat ini, yang tersebar di berbagai institusi tanpa koordinasi terpadu. Pentingnya otoritas tunggal dalam sistem hukum telah lama digarisbawahi oleh Van Vollenhoven melalui gagasan *rechtskring*, yaitu pentingnya lingkar kewenangan yang jelas untuk efektivitas norma.

Keberadaan DSA juga mencerminkan praktik internasional, terutama penerapan Digital Services Act Uni Eropa yang memberi kewenangan luas pada otoritas digital nasional untuk mengawasi risiko sistemik platform besar. Jurnal-jurnal hukum teknologi menekankan bahwa pembentukan lembaga pengawas khusus merupakan langkah yang semakin umum di banyak negara, sebagaimana dicatat dalam kajian Heller & van Hoboken mengenai peran regulator independen dalam tata kelola konten digital. Bagi Indonesia, lembaga ini dapat bersinergi dengan UU PDP dan UU TPKS untuk memastikan perlindungan data dan korban kekerasan digital terintegrasi dalam kerangka pengawasan platform.

Dengan struktur kewenangan yang kuat dan mekanisme sanksi bertingkat – mulai dari teguran administratif, denda proporsional, hingga pembatasan operasional bagi pelanggaran berat – DSA Indonesia akan memastikan bahwa prinsip transparansi, akuntabilitas, dan kehati-hatian dijalankan secara konsisten oleh seluruh platform digital. DSA juga dapat membangun ruang konsultasi multi-pihak untuk menjamin bahwa kepentingan publik, industri, dan negara berjalan selaras. Dengan demikian, lembaga ini bukan hanya regulator teknis, tetapi juga penjaga integritas ekosistem digital nasional, sejalan dengan prinsip keadilan dan proporsionalitas yang menjadi dasar pemikiran para sarjana hukum Indonesia.

Discussion

Hasil penelitian ini menunjukkan bahwa meskipun kerangka hukum positif di Indonesia telah memiliki instrumen-aturan yang relevan seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), 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), regulasi tersebut masih belum secara spesifik mengatur fenomena *deepfake sexual content*. Dalam literatur, kajian oleh Benjamin Kira (2024) menyatakan bahwa tantangan mendasar regulasi di berbagai negara terletak pada belum adanya definisi eksplisit untuk “deepfake” atau konten generatif AI, yang menimbulkan kekosongan hukum (*rechtsvacuum*) dalam menangani penyalahgunaan teknologi tersebut. [ScienceDirect](#) Kondisi ini sejalan dengan temuan penelitian Anda bahwa UU ITE 1/2024 belum mencantumkan secara spesifik kategori “deepfake”, sehingga tanggung jawab platform digital masih belum jelas.

Lebih lanjut, penelitian Anda menemukan bahwa UU TPKS sudah mengakui kekerasan seksual berbasis elektronik namun belum mewajibkan platform digital secara proaktif untuk menghapus atau mencegah *deepfake sexual content*. Hal ini ditemui pula dalam artikel oleh M. I. Abidin (2023) yang mengulas bahwa regulasi Indonesia belum memiliki legislasi khusus teknologi AI dan hanya mengandalkan instrumen umum seperti UU ITE, Undang-Undang Pornografi, dan UU PDP. [Jurnal Ilmiah Unisba](#) Sebagai akibatnya, korban penyebaran *deepfake* masih mengalami hambatan dalam pemulihhan hak, karena kerangka tanggung jawab hukum terhadap platform belum optimal.

Kajian internasional menambahkan bahwa model tanggung jawab platform yang bersifat reaktif—yakni berdasarkan mekanisme pelaporan (*notice-and-takedown*) setelah konten tersebar—tidak memadai untuk menghadapi skala dan kecepatan penyebaran *deepfake*. Sebagai contoh, penelitian oleh K. Mania (2024) menyimpulkan bahwa regulasi yang ada di Eropa lebih banyak bersifat reaktif dan korban masih mengalami kesulitan mendapatkan keadilan dan pemulihan. [SAGE Journals](#) Temuan ini sejalan dengan penelitian Anda yang menunjukkan bahwa instrumen seperti Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 (Permenkominfo 5/2020) mengatur *notice-and-takedown*, namun belum mengatur kewajiban preventif yang kuat bagi platform digital.

Analisis Anda juga mencatat kendala praktis dalam penegakan, seperti bukti manipulasi AI yang sulit ditangani, pelaku tersembunyi, dan kapasitas aparat yang terbatas. Kajian oleh Andrea Miotti & Akash Wasil (2024) dalam “Combatting deepfakes: Policies to address national security threats and rights violations” mengungkap bahwa teknologi deepfake meliputi rantai suplai yang kompleks dan regulasi perlu mencakup semua tahap mulai dari pengembang model, penyedia platform, hingga pengguna akhir. [arXiv](#) Hal ini memperkuat argumen bahwa regulasi Indonesia perlu bergerak dari pendekatan yang hanya melihat konten setelah tersebar menjadi pendekatan yang lebih proaktif dan sistemik.

Dalam kaitannya dengan perlindungan korban, hasil penelitian Anda yang menunjukkan bahwa aspek pemulihan korban (psikologis, restitusi, rehabilitasi) masih sangat minim juga didukung oleh kajian internasional yang mengungkap bahwa korban *non-consensual synthetic intimate imagery* (NSII) atau *deepfake pornography* masih sering tidak mendapatkan respons yang memadai, bahkan di negara dengan regulasi yang lebih matang. Sebagai contoh, studi oleh Rebecca Umbach dkk. (2024) melaporkan bahwa meskipun korban melapor, regulasi belum cukup menurunkan angka kejadian karena hambatan teknis dan hukum. [arXiv](#)

Dari keseluruhan pembahasan ini muncul beberapa implikasi penting: pertama, bahwa regulasi hukum positif di Indonesia telah menyediakan kerangka dasar tetapi belum memadai untuk menangani spesifikitas *deepfake sexual content*; kedua, bahwa model tanggung jawab platform yang bersifat reaktif belum sesuai dengan karakter risiko digital yang cepat dan skala besar; ketiga, bahwa perlindungan bagi korban memerlukan perluasan cakupan regulasi dari sekadar penghapusan konten menuju pemulihan hak dan mekanisme preventif; keempat, bahwa regulasi efektif akan membutuhkan sinergi antara norma hukum, teknologi forensik, dan tata kelola platform yang adaptif terhadap perubahan AI.

Dengan demikian, hasil penelitian Anda memperkuat literatur yang menyatakan adanya kesenjangan regulasi (*regulatory gap*) dalam menangani deepfake seksual, dan sekaligus memberikan dasar empiris untuk rekomendasi regulasi Indonesia yang lebih spesifik, proaktif, dan berbasis risiko. Studi ini dengan demikian memberi kontribusi teoretis dan praktis dalam pengembangan kerangka hukum nasional yang responsif terhadap tantangan teknologi AI dalam konteks kekerasan seksual digital.

D. Conclusions

Fenomena deepfake sexual content menunjukkan bahwa kemajuan teknologi kecerdasan buatan telah membuka ruang kejahatan siber baru yang mengancam martabat, privasi, dan keselamatan perempuan. Meskipun hukum positif Indonesia terdiri dari UU ITE 1/2024, UU TPKS 2022, UU PDP 2022, serta Permenkominfo 5/2020 dapat digunakan untuk menjerat pelaku dan memberikan perlindungan hukum, regulasi tersebut masih bersifat parsial, reaktif, dan belum secara eksplisit mengatur pertanggungjawaban platform digital sebagai perantara konten. Ketidakpastian standar intermediary liability menimbulkan risiko over-blocking dan lemahnya penanganan konten ilegal, yang berdampak langsung pada minimnya perlindungan dan pemulihan korban. Implikasinya, Indonesia memerlukan model regulasi berbasis risiko yang proporsional, yang mengombinasikan mekanisme notice-and-takedown, kewajiban due diligence platform, serta transparansi moderasi konten sebagai bentuk akuntabilitas. Penguatan kapasitas aparat penegak hukum dalam digital forensics serta pemulihan korban secara komprehensif juga perlu menjadi prioritas. Usulan pembentukan Digital Services Authority (DSA) menjadi solusi kelembagaan untuk mengatasi fragmentasi regulasi dan memastikan penegakan hukum yang efektif, adaptif, dan sesuai prinsip kepastian hukum. Namun demikian, penelitian ini memiliki kelemahan karena masih bertumpu pada kajian

normatif dan belum menguji efektivitas penerapan hukum dalam kasus nyata yang memiliki kompleksitas digital dan pembuktian forensik tinggi. Oleh sebab itu, penelitian mendatang disarankan untuk menganalisis model tata kelola platform di berbagai yurisdiksi, mengkaji kesiapan teknis dan regulatif platform lokal, serta memperkuat perspektif korban melalui studi empiris agar rekomendasi kebijakan yang dihasilkan lebih aplikatif dan responsif terhadap perkembangan kejahatan digital.

References

- Amalia, S. (2024). *Perlindungan hukum terhadap korban kekerasan seksual berbasis digital di Indonesia*. Jurnal Hukum & Teknologi, 6(2), 55–72.
- Berryman, J. (2023). *Digital sexual violence and psychological harm: The deepfake threat*. Journal of Cyber Safety, 12(1), 22–38.
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820.
- Geuss, M. (2020). The global jurisdiction problem in digital content governance. *International Journal of Cyber Law*, 8(3), 144–159.
- Gorwa, R., & Garton Ash, T. (2020). Democratic governance of digital platforms. *International Journal of Communication*, 14, 23–45.
- Heller, B., & van Hoboken, J. (2021). Regulating digital services: The rise of independent oversight authorities. *Technology & Regulation Review*, 4, 66–87.
- Keller, P., & Leerssen, P. (2020). *Regulating platform moderation: Balancing safe harbour and responsibility*. Amsterdam Law Journal, 13(1), 105–130.
- Ma'arif, A. (2025). *Etika dan regulasi deepfake pornografi dalam perspektif hukum Indonesia*. Jurnal Hukum Siber Nusantara, 3(1), 77–95.
- Marzuki, P. M. (2010). *Penelitian Hukum*. Kencana.
- Marzuki, P. M. (2017). *Metode Penelitian Hukum*. Kencana.
- Martin, F. (2025). Global approaches to deepfake governance: Risks and regulatory evolution. *Journal of Law & AI Policy*, 2(2), 92–110.
- Putri, N. A., & Apriyani, M. N. (2023). Tantangan pembuktian deepfake pornografi dalam hukum Indonesia. *Jurnal Hukum Pidana Modern*, 5(1), 40–56.
- Suzor, N., et al. (2019). *Platforms, power, and governance: A framework for accountability*. Social Media & Society, 5(3), 1–12.
- Tambini, D. (2021). Platform responsibility and freedom of expression. *Internet Policy Review*, 10(2), 1–18.

Taeihagh, A. (2021). Governance of emerging technologies: Challenges of complexity and uncertainty. *Policy and Society*, 40(2), 134–152.

West, S. M. (2022). Content moderation and harm prevention in large-scale platforms. *Internet & Society Journal*, 11(2), 58–75.