Jurnal Pendidikan Sejarah dan Riset Sosial Humaniora (KAGANGA)
Volume 8, Nomor 6, November-Desember 2025
e-ISSN: 2598-4934
p-ISSN: 2621-119X
DOI: https://doi.org/10.31539/61dkna59

URGENSI MODEL KERANGKA YURIDIS ADAPTIF TERHADAP *DEEPFAKE* AI (ARTIFICIAL INTELLIGENCE) DALAM PERSPEKTIF HUKUM SIBER

Zulfikar[1], Partahan V. A Erick Sihombing[2]
Universitas Esa Unggul[1,2]
zulfikar.judge@esaunggul.ac.id

ABSTRAK

Penelitian ini bertujuan untuk menganalisis karakteristik teknologi *deepfake* berbasis *Artificial Intelligence* (AI) yang menimbulkan tantangan baru bagi hukum siber, mengevaluasi efektivitas regulasi Indonesia dalam memberikan perlindungan hukum terhadap penyalahgunaan *deepfake*, serta merumuskan prinsip-prinsip yuridis dan model kerangka hukum adaptif yang relevan. Penelitian ini menggunakan pendekatan normatif yuridis dengan menelaah peraturan perundang-undangan, doktrin hukum, dan literatur ilmiah terkait hukum siber dan AI, yang diperkaya dengan pendekatan konseptual dan komparatif. Hasil penelitian menunjukkan bahwa *deepfake* AI memiliki karakteristik anonim, replikatif, lintas batas, dan berbasis algoritma yang menyebabkan kesenjangan antara perkembangan teknologi dan kemampuan hukum nasional. Regulasi Indonesia masih bersifat sektoral dan parsial serta belum mengatur *deepfake* secara spesifik, sehingga perlindungan hukum terhadap korban belum optimal dan penegakan hukum menghadapi kendala normatif serta pembuktian. Penelitian ini juga menemukan bahwa prinsip perlindungan hak asasi manusia, kepastian hukum, proporsionalitas, tanggung jawab berbasis risiko, dan adaptivitas regulasi merupakan landasan utama dalam membangun kerangka hukum yang responsif. Simpulan penelitian menegaskan urgensi pembentukan kerangka yuridis adaptif guna menjamin keadilan dan kepastian hukum di ruang siber.

Kata Kunci: *Deepfake* AI, Hak Digital, Hukum Siber, Kecerdasan Buatan, Perlindungan Hukum, Regulasi Adaptif.

ABSTRACT

This study aims to analyze the characteristics of deepfake technology based on Artificial Intelligence (AI) that generate new challenges for cyber law, to evaluate the extent to which existing Indonesian regulations provide effective legal protection against deepfake misuse, and to formulate relevant juridical principles and an adaptive legal framework to address technological developments. The research employs a normative juridical approach by examining statutory regulations, legal doctrines, and scholarly literature on cyber law and AI, complemented by conceptual and comparative analyses of regulatory practices in selected jurisdictions. The findings reveal that deepfake AI is characterized by anonymity, replicability, cross-border dissemination, and algorithmic autonomy, which collectively create a regulatory gap between rapid technological advancement and the capacity of national law to govern it. Existing Indonesian regulations remain sectoral, fragmented, and non-specific, resulting in limited

victim protection and significant normative and evidentiary challenges in law enforcement. The study further identifies key juridical principles, human rights protection, legal certainty, proportionality, risk-based responsibility, and regulatory adaptability as essential foundations for an adaptive legal framework. The study concludes that establishing an adaptive juridical model is an urgent necessity to ensure justice, legal certainty, and effective protection of digital rights in cyberspace.

Keywords: *Adaptive Regulation, Artificial Intelligence, Cyber Law, Deepfake AI, Digital Rights, Legal Protection.*

PENDAHULUAN

Perkembangan teknologi *Artificial Intelligence* (AI) dalam dua dekade terakhir telah membawa perubahan mendasar terhadap struktur sosial, ekonomi, dan hukum masyarakat global. AI tidak lagi sekadar alat bantu komputasi, melainkan telah menjadi aktor teknologi yang mampu menghasilkan konten, mengambil keputusan, dan mereplikasi perilaku manusia secara otonom. Salah satu bentuk paling problematik dari perkembangan tersebut adalah teknologi *deepfake*, yakni teknologi AI generatif yang mampu menciptakan atau memanipulasi konten audio-visual secara hiper-realistis sehingga sulit dibedakan dari realitas (Goodfellow et al., 2014; Chesney, 2019). *Deepfake* umumnya dikembangkan melalui *Generative Adversarial Networks* (GAN) yang bekerja dengan mempertemukan dua algoritma, yaitu *generator* dan *discriminator* dalam proses pembelajaran berulang untuk menghasilkan konten palsu yang tampak autentik. Fenomena *deepfake* menimbulkan tantangan serius dalam perspektif hukum siber karena secara langsung mengaburkan batas antara realitas dan rekayasa digital. Dalam konteks hukum, keautentikan informasi merupakan prasyarat penting bagi pembuktian, perlindungan hak, dan penegakan keadilan. Ketika teknologi mampu memproduksi kebohongan digital yang tampak nyata, maka fondasi epistemologis hukum modern menjadi terganggu (Rini, 2022).

Sejumlah penelitian menunjukkan bahwa *deepfake* telah digunakan untuk berbagai tujuan yang melanggar hukum, seperti pornografi non-konsensual, pencemaran nama baik, penipuan finansial, pemerasan, manipulasi politik, dan disinformasi publik (Citron, 2019; Franks, 2022; Westerlund, 2019). Dalam ranah politik dan demokrasi, *deepfake* bahkan dipandang sebagai ancaman serius terhadap integritas pemilu dan kepercayaan publik terhadap institusi negara. Vaccari dan Chadwick (2020) menegaskan bahwa *deepfake* berpotensi mempercepat krisis kepercayaan (crisis of trust) terhadap media digital karena masyarakat semakin sulit membedakan antara informasi benar dan palsu. Kondisi ini berimplikasi langsung terhadap stabilitas sosial dan keamanan nasional, terutama di negara-negara dengan tingkat literasi digital yang belum merata, termasuk Indonesia.

Hukum siber sebagai cabang hukum yang mengatur perilaku manusia dan entitas digital di ruang siber dihadapkan pada tantangan struktural dalam merespons fenomena

deepfake. Ruang siber memiliki karakter lintas batas (*borderless*), anonim, dan berbasis algoritma, sementara sistem hukum nasional pada umumnya masih terikat pada prinsip teritorialitas dan subjek hukum konvensional (Brenner, 2013; Lessig, 2006). Akibatnya, terjadi ketimpangan antara kecepatan inovasi teknologi dan kemampuan hukum dalam meresponsnya, yang sering disebut sebagai fenomena *regulatory lag* (Marchant et al., 2011).

Di Indonesia, pengaturan hukum terkait deepfake masih bersifat implisit dan tersebar dalam berbagai peraturan perundang-undangan. Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Pornografi, serta ketentuan dalam KUHP baru memang dapat digunakan untuk menjerat pelaku penyalahgunaan *deepfake*, namun regulasi tersebut belum dirancang secara spesifik untuk menghadapi karakteristik teknologi AI generatif (Pratama, 2023; Sari, 2024). Hal ini menimbulkan persoalan dalam penegakan hukum, khususnya terkait unsur kesalahan, pembuktian digital, dan pertanggungjawaban hukum atas tindakan yang dilakukan melalui sistem AI. Lebih lanjut, penggunaan pasal-pasal umum untuk menjerat kejahatan *deepfake* berpotensi menimbulkan ketidakpastian hukum dan pelanggaran asas *nullum crimen sine lege*. Aparat penegak hukum sering menghadapi kesulitan dalam membuktikan unsur kesengajaan (*mens rea*) dan kausalitas, terutama ketika konten *deepfake* dibuat atau disebarkan oleh pihak anonim atau melalui sistem otomatis (Suseno, 2022). Selain itu, korban *deepfake* sering kali berada dalam posisi yang lemah karena keterbatasan mekanisme pemulihan hukum dan kurangnya pemahaman aparat terhadap aspek teknis AI (Franks, 2022). Dari perspektif hak asasi manusia, *deepfake* berpotensi melanggar berbagai hak fundamental, seperti hak atas privasi, hak atas martabat manusia, hak atas reputasi, serta hak atas rasa aman di ruang digital. Dalam kasus pornografi *deepfake*, misalnya, korban mengalami reviktimisasi yang berkepanjangan karena konten dapat direplikasi dan disebarluaskan tanpa batas waktu dan ruang (Citron, 2019). Oleh karena itu, *deepfake* tidak dapat dipandang semata sebagai persoalan kriminal individual, melainkan sebagai persoalan struktural yang memerlukan pendekatan regulasi komprehensif dan berbasis HAM.

Di tingkat internasional, respons terhadap *deepfake* dan AI menunjukkan kecenderungan menuju regulasi yang adaptif dan berbasis risiko. Uni Eropa melalui *EU Artificial Intelligence Act* mengadopsi pendekatan *risk-based regulation* dengan mengklasifikasikan sistem AI berdasarkan tingkat risikonya terhadap hak dan keselamatan publik (European Commission, 2021). Amerika Serikat, meskipun belum memiliki undang-undang AI komprehensif, mulai mengembangkan regulasi sektoral dan undang-undang khusus terkait *deepfake*, terutama dalam konteks pemilu dan pornografi non-konsensual (Chesney, 2023). Perkembangan ini menunjukkan bahwa regulasi AI tidak lagi dapat bersifat statis, melainkan harus adaptif terhadap dinamika teknologi. Dalam konteks tersebut, penelitian ini menempatkan urgensi pembentukan model kerangka yuridis adaptif

terhadap *deepfake* AI sebagai fokus utama. Kerangka yuridis adaptif dipahami sebagai model pengaturan hukum yang bersifat dinamis, responsif, dan fleksibel terhadap perubahan teknologi, dengan tetap berlandaskan pada prinsip negara hukum, kepastian hukum, dan perlindungan hak asasi manusia. Pendekatan ini sejalan dengan gagasan *responsive law* yang dikemukakan oleh Nonet dan Selznick (1978), serta konsep *adaptive governance* dalam regulasi teknologi modern (De Bellis, 2020).

Penelitian ini bertujuan untuk menganalisis secara mendalam fenomena deepfake AI dalam perspektif hukum siber serta mengkaji kelemahan dan keterbatasan kerangka hukum nasional dalam mengatur penyalahgunaannya. Selain itu, penelitian ini bertujuan merumuskan model kerangka yuridis adaptif yang mampu menjembatani kesenjangan antara perkembangan teknologi AI dan sistem hukum nasional. Tujuan lain dari penelitian ini adalah menyusun rekomendasi normatif bagi pembentuk undang-undang dan pembuat kebijakan dalam merancang regulasi *deepfake* yang efektif, proporsional, dan berorientasi pada perlindungan hak digital warga negara.

Kebaruan (novelty) penelitian ini terletak pada pendekatannya yang tidak semata-mata menekankan kriminalisasi *deepfake*, tetapi pada perumusan kerangka hukum adaptif sebagai paradigma baru dalam hukum siber. Berbeda dengan penelitian sebelumnya yang cenderung bersifat sektoral atau deskriptif, penelitian ini mengintegrasikan prinsip hukum, teknologi AI, dan perlindungan HAM dalam satu kerangka normatif yang komprehensif. Pendekatan ini sejalan dengan pemikiran Floridi et al. (2018) yang menekankan pentingnya *ethics-by-design* dan *law-by-design* dalam regulasi teknologi AI.

Rumusan masalah dalam penelitian ini diarahkan untuk menjawab pertanyaan mendasar mengenai bagaimana karakteristik *deepfake* AI menimbulkan tantangan baru bagi hukum siber; sejauh mana regulasi Indonesia saat ini mampu memberikan perlindungan hukum yang efektif terhadap penyalahgunaan deepfake; prinsip-prinsip yuridis apa yang relevan untuk membangun kerangka hukum adaptif terhadap *deepfake* AI; serta bagaimana model kerangka yuridis adaptif tersebut dapat diimplementasikan dalam sistem hukum nasional dengan tetap menjamin kepastian hukum dan keadilan.

Kontribusi penelitian ini diharapkan signifikan secara akademik dan praktis. Secara akademik, penelitian ini memperkaya kajian hukum siber dan hukum AI dengan menawarkan konsep kerangka yuridis adaptif sebagai respons terhadap tantangan teknologi generatif. Secara praktis, penelitian ini diharapkan menjadi rujukan bagi pembentuk kebijakan, aparat penegak hukum, dan praktisi hukum dalam merumuskan dan menerapkan regulasi *deepfake* yang lebih efektif. Dengan demikian, penelitian ini menegaskan bahwa adaptivitas hukum bukanlah pilihan, melainkan keniscayaan dalam menghadapi era AI dan *deepfake* yang terus berkembang.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan normatif yuridis sebagai pendekatan utama dalam mengkaji urgensi pembentukan model kerangka

yuridis adaptif terhadap fenomena *deepfake* berbasis *Artificial Intelligence* dalam perspektif hukum siber. Pendekatan normatif yuridis dipilih karena fokus utama penelitian ini adalah hukum sebagai norma (*law in books*), yakni seperangkat kaidah, asas, prinsip, dan doktrin hukum yang mengatur serta seharusnya mengatur perilaku manusia dan penggunaan teknologi di ruang siber. *Deepfake* AI sebagai fenomena teknologi tidak hanya menimbulkan persoalan faktual, tetapi terutama memunculkan problem normatif berupa kekosongan hukum, ketidakcukupan norma, serta disharmoni pengaturan dalam sistem hukum positif yang berlaku (Soekanto, 2006).

Pendekatan normatif yuridis dalam penelitian ini memandang hukum sebagai sistem normatif yang harus mampu memberikan kepastian, keadilan, dan kemanfaatan dalam menghadapi perkembangan teknologi digital yang disruptif. Dalam konteks *deepfake* AI, hukum dihadapkan pada tantangan untuk mengatur teknologi yang berkembang secara cepat, bersifat lintas batas, serta beroperasi melalui algoritma yang tidak sepenuhnya dapat dipahami oleh subjek hukum konvensional. Oleh karena itu, penelitian ini tidak bertujuan untuk mengukur perilaku empiris masyarakat atau efektivitas penegakan hukum secara statistik, melainkan untuk menganalisis kecukupan norma hukum yang ada serta merumuskan konstruksi hukum yang ideal dan adaptif terhadap perkembangan AI (Marzuki, 2017).

Dalam kerangka pendekatan normatif yuridis, penelitian ini menggunakan beberapa metode pendekatan hukum yang saling melengkapi. Pendekatan peraturan perundang-undangan (statute approach) digunakan untuk mengkaji berbagai peraturan perundang-undangan yang relevan dengan pengaturan *deepfake* dan AI. Analisis dilakukan terhadap Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Pornografi, serta ketentuan pidana dalam Kitab Undang-Undang Hukum Pidana yang baru. Pendekatan ini bertujuan untuk menilai sejauh mana norma-norma positif tersebut mampu mengakomodasi karakteristik teknologi *deepfake*, khususnya dalam aspek perbuatan melawan hukum, pertanggungjawaban pidana, pembuktian digital, dan perlindungan hak korban. Melalui pendekatan ini pula dapat diidentifikasi adanya kekosongan norma (legal vacuum), norma yang bersifat terlalu umum, atau norma yang tidak lagi relevan dengan perkembangan teknologi AI (Asshiddiqie, 2010).

Selain itu, pendekatan konseptual (conceptual approach) digunakan untuk membangun dasar teoretis dan konseptual dalam penelitian ini. Pendekatan ini penting karena istilah dan konsep kunci seperti *deepfake*, *artificial intelligence*, *hukum siber*, *tanggung jawab algoritmik*, dan *kerangka yuridis adaptif* belum sepenuhnya memiliki definisi yang mapan dalam peraturan perundang-undangan. Oleh karena itu, penelitian ini merujuk pada doktrin dan pandangan para ahli hukum, filsuf hukum, serta pakar teknologi untuk merumuskan konsep-konsep tersebut secara sistematis dan operasional. Pendekatan konseptual juga digunakan untuk mengkaji teori-teori hukum yang relevan, seperti teori hukum responsif, teori regulasi adaptif, dan teori perlindungan hak asasi manusia dalam ruang digital

(Nonet, 1978; Lessig, 2006; Floridi et al., 2018).

Pendekatan perbandingan hukum (comparative approach) turut digunakan untuk memperkaya analisis normatif penelitian ini. Pendekatan ini dilakukan dengan membandingkan pengaturan dan kebijakan hukum terkait *deepfake* dan AI di beberapa yurisdiksi, seperti Uni Eropa dan Amerika Serikat, yang telah lebih dahulu mengembangkan regulasi atau kebijakan terkait teknologi AI. Perbandingan ini bertujuan untuk mengidentifikasi prinsip-prinsip umum dan praktik terbaik (best practices) dalam pengaturan *deepfake*, seperti pendekatan berbasis risiko (risk-based regulation), kewajiban transparansi, dan mekanisme pertanggungjawaban hukum terhadap penggunaan AI (European Commission, 2021; Chesney, 2019). Hasil perbandingan tersebut tidak dimaksudkan untuk ditransplantasikan secara langsung, melainkan sebagai bahan refleksi normatif dalam merumuskan kerangka yuridis yang sesuai dengan sistem hukum dan nilai-nilai konstitusional Indonesia.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan nasional dan internasional yang relevan, dokumen kebijakan resmi, serta putusan pengadilan yang berkaitan dengan teknologi informasi, privasi, dan kejahatan siber. Bahan hukum sekunder mencakup buku teks hukum, artikel jurnal ilmiah, hasil penelitian, laporan lembaga internasional, dan pendapat para ahli di bidang hukum siber dan AI. Bahan hukum tersier digunakan untuk mendukung pemahaman konsep dan terminologi, seperti kamus hukum, ensiklopedia, dan indeks hukum. Penggunaan ketiga jenis bahan hukum ini bertujuan untuk memastikan bahwa analisis yang dilakukan memiliki dasar normatif dan akademik yang kuat (Soekanto, 2006).

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) yang sistematis dan terstruktur. Penelusuran literatur dilakukan dengan mengakses basis data jurnal ilmiah nasional dan internasional, perpustakaan universitas, serta publikasi lembaga resmi dan organisasi internasional yang kredibel. Proses ini dilakukan secara selektif dengan mempertimbangkan relevansi, otoritas, dan kebaruan sumber, sehingga bahan hukum yang digunakan benar-benar mendukung tujuan penelitian. Studi kepustakaan dipilih karena sesuai dengan karakter penelitian normatif yuridis yang bertumpu pada analisis teks hukum dan doktrin.

Analisis bahan hukum dalam penelitian ini dilakukan secara kualitatif dengan metode analisis normatif-preskriptif. Analisis normatif digunakan untuk menilai konsistensi, koherensi, dan kecukupan norma hukum dalam mengatur fenomena *deepfake* AI. Sementara itu, analisis preskriptif digunakan untuk merumuskan rekomendasi normatif dan model kerangka yuridis adaptif yang diusulkan sebagai solusi atas permasalahan hukum yang diidentifikasi. Dalam proses analisis, penafsiran hukum dilakukan secara sistematis, teleologis, dan futuristik

untuk memastikan bahwa norma hukum dipahami tidak hanya berdasarkan bunyi teksnya, tetapi juga tujuan dan nilai yang hendak diwujudkan, khususnya perlindungan hak asasi manusia dan kepastian hukum di ruang siber (Marzuki, 2017).

Penalaran hukum dalam penelitian ini menggunakan kombinasi penalaran deduktif dan induktif. Penalaran deduktif digunakan untuk menarik implikasi normatif dari prinsip-prinsip hukum umum dan teori hukum ke dalam konteks pengaturan *deepfake* AI. Penalaran induktif digunakan untuk merumuskan prinsip dan model kerangka yuridis adaptif berdasarkan temuan normatif dan perbandingan hukum yang dilakukan. Kombinasi kedua pola penalaran ini memungkinkan penelitian menghasilkan kesimpulan yang logis, sistematis, dan relevan dengan kebutuhan pembaruan hukum di era digital.

Dengan pendekatan normatif yuridis yang komprehensif ini, penelitian diharapkan mampu memberikan analisis hukum yang mendalam dan argumentatif mengenai urgensi pembentukan kerangka yuridis adaptif terhadap deepfake AI. Metode penelitian ini dirancang untuk menghasilkan rekomendasi normatif yang tidak hanya relevan dengan kondisi hukum positif saat ini, tetapi juga adaptif terhadap perkembangan teknologi AI di masa depan, sehingga hukum tetap mampu menjalankan fungsinya sebagai sarana pengendali sosial dan pelindung hak warga negara di ruang siber.

HASIL PENELITIAN DAN PEMBAHASAN

Bagian ini menyajikan hasil analisis normatif-yuridis terhadap urgensi fenomena *deepfake* AI dalam perspektif hukum siber, sekaligus membahas implikasi yuridisnya berdasarkan pertanyaan penelitian yang telah dirumuskan. Pembahasan dilakukan secara sistematis dengan menelaah karakteristik *deepfake* sebagai teknologi disruptif, mengevaluasi efektivitas regulasi hukum nasional yang berlaku, mengidentifikasi prinsip-prinsip yuridis yang relevan dalam membangun kerangka hukum adaptif, serta merumuskan model implementasi kerangka yuridis adaptif yang tetap menjamin kepastian hukum dan keadilan dalam sistem hukum Indonesia.

Karakteristik *Deepfake* AI dan Tantangan Baru bagi Hukum Siber

Hasil kajian normatif menunjukkan bahwa teknologi *deepfake* AI memiliki karakteristik khas yang secara fundamental membedakannya dari bentuk manipulasi digital konvensional, sehingga menimbulkan tantangan baru bagi hukum siber. *Deepfake* merupakan produk *artificial intelligence generatif* yang bekerja melalui algoritma pembelajaran mesin, khususnya *Generative Adversarial Networks* (GAN), yang mampu mereplikasi wajah, suara, dan ekspresi manusia secara sangat realistis (Goodfellow et al., 2014). Karakteristik utama *deepfake* terletak pada kemampuannya menciptakan ilusi autentisitas, yakni membuat konten palsu yang secara visual dan auditori hampir tidak dapat dibedakan dari konten asli oleh manusia awam maupun sistem verifikasi sederhana.

Dalam perspektif hukum siber, karakteristik ini menimbulkan

problem epistemologis dan yuridis. Hukum modern sangat bergantung pada keaslian bukti dan kebenaran faktual sebagai dasar pertanggungjawaban hukum. *Deepfake* mengaburkan batas antara fakta dan rekayasa, sehingga melemahkan kepercayaan terhadap alat bukti digital (digital evidence) yang selama ini dianggap relatif objektif (Chesney, 2019). Kondisi ini berpotensi menimbulkan apa yang disebut sebagai *liar's dividend*, yaitu situasi di mana pelaku kejahatan dapat dengan mudah menyangkal bukti autentik dengan mengklaim bahwa bukti tersebut adalah hasil *deepfake* (Chesney, 2019).

Selain itu, *deepfake* memiliki karakter lintas batas (borderless), anonim, dan mudah direplikasi, sehingga menyulitkan penentuan yurisdiksi dan subjek hukum yang bertanggung jawab. Konten *deepfake* dapat dibuat di satu negara, disebarkan melalui platform global, dan berdampak pada korban di negara lain. Karakter ini menantang prinsip teritorialitas hukum pidana dan menimbulkan kesulitan dalam kerja sama penegakan hukum lintas negara (Brenner, 2013). Dalam konteks hukum siber, *deepfake* juga memunculkan persoalan pertanggungjawaban hukum atas tindakan yang dilakukan oleh atau melalui sistem AI, terutama ketika keterlibatan manusia menjadi semakin minimal (Abbott, 2020).

Dengan demikian, hasil analisis menunjukkan bahwa *deepfake* AI bukan sekadar bentuk baru kejahatan siber, melainkan fenomena teknologi yang menggeser paradigma hukum siber dari pendekatan berbasis pelaku manusia (human-centric liability) menuju kebutuhan pengaturan yang mempertimbangkan peran algoritma, platform digital, dan ekosistem teknologi secara keseluruhan.

Efektivitas Regulasi Indonesia dalam Memberikan Perlindungan Hukum terhadap Penyalahgunaan *Deepfake*

Hasil kajian terhadap regulasi Indonesia menunjukkan bahwa hingga saat ini belum terdapat pengaturan hukum yang secara eksplisit dan komprehensif mengatur *deepfake* AI. Perlindungan hukum terhadap penyalahgunaan *deepfake* masih bergantung pada instrumen hukum yang bersifat umum dan sektoral, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Pornografi, serta ketentuan pidana dalam KUHP nasional yang baru (Pratama, 2023; Sari, 2024).

UU ITE, misalnya, dapat digunakan untuk menjerat penyebaran konten *deepfake* yang bermuatan pencemaran nama baik, kesusilaan, atau berita bohong. Namun, norma dalam UU ITE tidak dirancang khusus untuk menghadapi karakter manipulatif dan sintetis dari *deepfake*. Akibatnya, penegakan hukum sering kali menghadapi kesulitan dalam membuktikan unsur kesengajaan (mens rea) dan kausalitas antara tindakan pelaku dan kerugian korban (Suseno, 2022). Selain itu, UU ITE lebih berorientasi pada distribusi konten, bukan pada proses penciptaan konten berbasis AI.

UU Perlindungan Data Pribadi memberikan dasar perlindungan terhadap penggunaan data pribadi tanpa persetujuan, termasuk data biometrik seperti wajah dan suara. Namun, UU ini belum secara eksplisit mengatur pemrosesan data pribadi oleh sistem AI generatif dan tidak

secara tegas mengatur mekanisme pertanggungjawaban dalam kasus manipulasi data biometrik melalui *deepfake* (Sari, 2024). Dalam praktiknya, korban *deepfake* sering kali kesulitan memperoleh pemulihan hukum yang cepat dan efektif karena proses penegakan hukum yang panjang dan kompleks.

Hasil analisis ini menunjukkan bahwa regulasi Indonesia saat ini masih bersifat reaktif, fragmentaris, dan belum adaptif terhadap perkembangan teknologi AI. Kondisi tersebut menciptakan kekosongan hukum (legal gap) yang berpotensi melemahkan perlindungan hak asasi manusia di ruang digital dan menimbulkan ketidakpastian hukum bagi korban maupun pelaku.

Prinsip-Prinsip Yuridis yang Relevan untuk Membangun Kerangka Hukum Adaptif terhadap *Deepfake* AI

Berdasarkan analisis konseptual dan normatif, penelitian ini menemukan bahwa pembangunan kerangka hukum adaptif terhadap *deepfake* AI harus berlandaskan pada sejumlah prinsip yuridis utama. Pertama, prinsip perlindungan hak asasi manusia, khususnya hak atas privasi, martabat manusia, dan reputasi. *Deepfake* secara inheren berpotensi melanggar hak-hak tersebut, terutama dalam kasus pornografi non-konsensual dan penipuan identitas (Citron, 2019).

Kedua, prinsip kepastian hukum dan proporsionalitas. Regulasi *deepfake* harus memberikan kejelasan mengenai larangan, sanksi, dan mekanisme penegakan hukum tanpa menghambat inovasi teknologi secara berlebihan. Pendekatan ini sejalan dengan prinsip *risk-based regulation* yang menilai AI berdasarkan tingkat risiko dan dampaknya terhadap masyarakat (European Commission, 2021).

Ketiga, prinsip adaptivitas dan responsivitas hukum. Hukum harus mampu menyesuaikan diri dengan perkembangan teknologi yang cepat, sebagaimana ditegaskan dalam konsep *responsive law* (Nonet, 1978) dan *adaptive governance* (De Bellis, 2020). Prinsip ini menghendaki perumusan norma hukum yang fleksibel, berbasis prinsip, dan terbuka terhadap pembaruan.

Keempat, prinsip akuntabilitas dan tanggung jawab. Kerangka hukum adaptif harus memastikan adanya pertanggungjawaban yang jelas, tidak hanya bagi individu pelaku, tetapi juga bagi pengembang teknologi dan platform digital yang memfasilitasi penyebaran *deepfake* (Floridi et al., 2018). Prinsip ini penting untuk mencegah *responsibility gap* dalam penggunaan AI.

Implementasi Model Kerangka Yuridis Adaptif dalam Sistem Hukum Nasional

Hasil pembahasan menunjukkan bahwa implementasi model kerangka yuridis adaptif terhadap *deepfake* AI dalam sistem hukum nasional dapat dilakukan melalui beberapa strategi normatif dan institusional. Pertama, pembentukan regulasi khusus atau penguatan norma dalam undang-undang yang secara eksplisit mengatur *deepfake* dan AI generatif, baik melalui undang-undang baru maupun revisi peraturan yang ada. Regulasi ini harus memuat definisi hukum *deepfake*, klasifikasi risiko, larangan penggunaan tertentu, serta mekanisme sanksi yang proporsional.

Kedua, integrasi pendekatan berbasis risiko dan dampak (risk and impact-based approach) dalam penegakan hukum. Pendekatan ini memungkinkan hukum merespons *deepfake* yang berisiko tinggi terhadap hak asasi manusia secara lebih tegas, tanpa menghambat penggunaan AI untuk tujuan yang sah dan bermanfaat (European Commission, 2021).

Ketiga, penguatan kapasitas institusional aparat penegak hukum melalui peningkatan literasi teknologi dan kerja sama dengan ahli AI. Tanpa pemahaman teknis yang memadai, penegakan hukum terhadap *deepfake* akan sulit dilakukan secara efektif (Abbott, 2020).

Keempat, harmonisasi regulasi nasional dengan kerangka hukum internasional dan penguatan kerja sama lintas negara dalam penanganan kejahatan *deepfake*. Mengingat sifat lintas batas *deepfake*, pendekatan unilateral tidak akan efektif tanpa dukungan kerja sama internasional (Brenner, 2013).

Dengan mengimplementasikan kerangka yuridis adaptif tersebut, sistem hukum nasional diharapkan mampu menjamin kepastian hukum dan keadilan, sekaligus menjaga relevansi hukum di tengah perkembangan teknologi AI yang terus berlanjut.

SIMPULAN

Penelitian ini secara umum bertujuan untuk menganalisis dan merumuskan urgensi pembentukan model kerangka yuridis adaptif terhadap fenomena *deepfake* berbasis *Artificial Intelligence* dalam perspektif hukum siber, dengan menempatkan perlindungan hak asasi manusia, kepastian hukum, dan keadilan sebagai fondasi utama pengaturan. Tujuan tersebut didasarkan pada realitas bahwa perkembangan teknologi AI generatif, khususnya *deepfake*, telah menciptakan bentuk risiko hukum baru yang belum sepenuhnya terakomodasi dalam sistem hukum nasional Indonesia. Dengan pendekatan normatif yuridis, penelitian ini berupaya menjembatani kesenjangan antara dinamika teknologi digital dan kemampuan hukum untuk merespons secara efektif dan berkelanjutan.

Hasil penelitian menunjukkan bahwa karakteristik *deepfake* AI yang bersifat hiper-realistis, mudah direplikasi, anonim, dan lintas batas yurisdiksi menimbulkan tantangan baru bagi hukum siber, khususnya dalam aspek pembuktian, pertanggungjawaban hukum, dan perlindungan hak digital korban (Chesney, 2019; Vaccari, 2020). Teknologi ini mengaburkan batas antara realitas dan rekayasa digital sehingga melemahkan keandalan sistem hukum yang masih bertumpu pada asumsi keautentikan informasi.

Penelitian ini juga menemukan bahwa regulasi Indonesia saat ini belum mampu memberikan perlindungan hukum yang optimal terhadap penyalahgunaan *deepfake*. Pengaturan yang tersebar dalam UU ITE, UU Perlindungan Data Pribadi, UU Pornografi, dan KUHP baru masih bersifat parsial, reaktif, dan belum dirancang secara spesifik untuk menghadapi karakter AI generatif. Kondisi ini menimbulkan kekosongan dan ketidakpastian hukum serta menyulitkan penegakan hukum secara efektif (Pratama, 2023; Sari, 2024).

Selanjutnya, penelitian ini mengidentifikasi sejumlah prinsip yuridis yang relevan sebagai dasar

pembentukan kerangka hukum adaptif terhadap *deepfake* AI, antara lain prinsip perlindungan hak asasi manusia, kepastian hukum, proporsionalitas, akuntabilitas algoritmik, serta pendekatan berbasis risiko (risk-based regulation) sebagaimana berkembang dalam regulasi AI global (Floridi et al., 2018; European Commission, 2021). Prinsip-prinsip tersebut menjadi fondasi normatif untuk merespons dinamika teknologi tanpa menghambat inovasi.

Implikasi hasil penelitian ini bersifat teoretis dan praktis. Secara teoretis, penelitian ini berkontribusi pada pengembangan kajian hukum siber dan hukum AI melalui penguatan konsep kerangka yuridis adaptif. Secara praktis, hasil penelitian ini dapat menjadi rujukan bagi pembentuk undang-undang dan pembuat kebijakan dalam merumuskan regulasi *deepfake* yang lebih komprehensif, sistematis, dan berorientasi pada perlindungan hak digital warga negara.

Penelitian ini memiliki keterbatasan karena berfokus pada pendekatan normatif yuridis dan belum menggali aspek empiris terkait praktik penegakan hukum atau persepsi aparat penegak hukum terhadap *deepfake* AI. Selain itu, dinamika teknologi AI yang sangat cepat juga berpotensi melampaui cakupan analisis normatif yang ada.

Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan kajian empiris dan interdisipliner, termasuk analisis terhadap praktik peradilan, kesiapan institusi penegak hukum, serta pengaruh *deepfake* terhadap masyarakat dan demokrasi digital. Penelitian lanjutan juga dapat mengeksplorasi harmonisasi regulasi nasional dengan kerangka hukum internasional guna menghadapi tantangan *deepfake* yang bersifat global.

DAFTAR PUSTAKA

Brenner, S. W. (2013). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs, 98*(1), 147–155.

Chesney, R., & Citron, D. K. (2023). Regulating deepfakes. *California Law Review, 111*(3), 731–780. https://doi.org/10.2139/ssrn.3213944

Citron, D. K. (2019). Sexual privacy. *Yale Law Journal, 128*(7), 1870–1960.

Citron, D. K., & Chesney, R. (2024). Deepfakes and the law of evidence. *Harvard Law Review Forum, 137*, 1–28.

Citron, D. K., & Franks, M. A. (2019). Criminalizing revenge porn. *Wake Forest Law Review, 49*(2), 345–391.

De Bellis, M. (2020). Adaptive regulation: A new approach to regulating artificial intelligence. *European Journal of Risk Regulation, 11*(2), 327–341. https://doi.org/10.1017/err.2020.25

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Brussels.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … Vayena, E. (2018). AI4People—An ethical framework for a good AI society:

Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Franks, M. A. (2022). *Fearless speech.* Oxford University Press.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*, 2672–2680.

Lessig, L. (2006). *Code: Version 2.0.* Basic Books.

Marchant, G. E., Allenby, B. R., & Herkert, J. R. (2011). *The growing gap between emerging technologies and legal-ethical oversight*. Springer.

Nonet, P., & Selznick, P. (1978). *Law and society in transition: Toward responsive law.* Harper & Row.

Pratama, R. A. (2023). Tantangan hukum terhadap teknologi deepfake dalam perspektif hukum siber Indonesia. *Jurnal Rechtsvinding, 12*(2), 245–262.

Rini, A. S., & Wibowo, A. (2022). Deepfake dan ancaman terhadap kepastian hukum di era digital. *Jurnal Ilmu Hukum Pandecta, 17*(1), 89–104.

Sari, D. P. (2024). Perlindungan hukum terhadap korban pornografi deepfake di Indonesia. *Jurnal Hukum IUS QUIA IUSTUM, 31*(1), 112–130.

Suseno, A. (2022). Pembuktian tindak pidana siber berbasis kecerdasan buatan. *Jurnal Hukum & Pembangunan, 52*(3), 401–420.

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

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 40–53. http://doi.org/10.22215/timreview/1282