

STUDI PERBANDINGAN: PERLINDUNGAN HUKUM TERHADAP DEEPFAKE BERBASIS KECERDASAN BUATAN (AI)

Ivana Trixie¹, Moody Risky Syailendra Putra²

Universitas Tarumanagara Jakarta^{1,2}

Ivana.205220032@stu.untar.ac.id¹

ABSTRAK

Penelitian ini bertujuan untuk membandingkan perlindungan hukum terhadap penyalahgunaan teknologi *deepfake* berbasis Kecerdasan Buatan (AI) di Indonesia dan Tiongkok. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan perbandingan, serta menelaah bahan hukum primer, sekunder, dan non-hukum untuk mengkaji pengaturan *deepfake* di Indonesia dan Tiongkok. Hasil penelitian menunjukkan bahwa Indonesia masih mengalami kekosongan norma karena tidak memiliki regulasi khusus yang mengatur rekayasa data visual berbasis AI, sehingga penegakan hukum bergantung pada pasal generik yang tidak sesuai dengan sifat manipulasi algoritmik. Sementara itu, Tiongkok telah mengadopsi *Deep Synthesis Regulation* (2023) yang bersifat preventif melalui kewajiban pelabelan, *watermarking*, verifikasi identitas, dan tanggung jawab penyedia layanan AI, sehingga memberikan perlindungan yang lebih komprehensif. Berdasarkan perbandingan tersebut, penelitian ini menyimpulkan bahwa Indonesia membutuhkan regulasi khusus mengenai *deepfake* agar mampu memberikan kepastian hukum, perlindungan korban, serta respons yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan.

Kata Kunci: *Deepfake*, Kecerdasan Buatan (AI), Perlindungan Hak Privasi, Studi Perbandingan Indonesia-Tiongkok.

ABSTRACT

This study aims to compare legal protections against the misuse of AI-based deepfake technology in Indonesia and China. This study uses a normative juridical method with a statutory and comparative approach, and examines primary, secondary, and non-legal legal materials to examine deepfake regulations in Indonesia and China. The results show that Indonesia still experiences a legal vacuum due to the lack of specific regulations governing AI-based visual data manipulation, resulting in law enforcement relying on generic articles that do not align with the nature of algorithmic manipulation. Meanwhile, China has adopted the Deep Synthesis Regulation (2023), which is preventative in nature through mandatory labelling, watermarking, identity verification, and liability for AI service providers, thus providing more comprehensive protection. Based on this comparison, this study concludes that Indonesia needs specific regulations regarding deepfakes to provide legal certainty, victim protection, and a more adaptive response to developments in artificial intelligence technology.

Keywords: Artificial Intelligence (AI), Deepfake, Digital Regulation, Indonesia-China Comparative Study, Privacy Protection.

PENDAHULUAN

Era digital berkembang dengan sangat pesat dan telah mengubah cara manusia berinteraksi, bekerja dan menjalani kehidupan sehari-hari. Pada awal tahun 2000-an, teknologi digital hanya berfungsi untuk komunikasi dasar seperti panggilan suara dan pesan singkat. Namun kini, teknologi tersebut telah berevolusi menjadi sarana multifungsi yang mencakup aktivitas ekonomi, edukasi, hiburan, hingga penyebaran informasi secara masif melalui berbagai platform. Berdasarkan survei Asosiasi Penyelenggara Jasa Internet Indonesia APJII tahun 2024, tercatat 79,5% penduduk Indonesia atau lebih dari 221 juta jiwa menggunakan internet, meningkat signifikan dibandingkan tahun 2018 yang hanya 64,8% atau sekitar 171 juta jiwa. Lonjakan ini tidak hanya membawa manfaat, tetapi juga menghadirkan risiko baru, termasuk penyebaran informasi palsu (hoaks) dan manipulasi konten digital yang kian sulit dibedakan dari kenyataan.

Salah satu teknologi yang memicu persoalan tersebut adalah *deepfake*, yaitu bentuk manipulasi media berbasis kecerdasan buatan (Artificial Intelligence/AI) yang dapat mengubah wajah atau suara seseorang secara hiper-realistik tanpa keterlibatan langsung pihak terkait. (Adriani, 2024). Menurut laporan *The State of Deepfakes* oleh Deeptrace Labs (2019), 96% konten *deepfake* yang beredar di internet berbentuk pornografi non-konsensual, sementara hanya 4% bersifat non-pornografi. Fakta ini menunjukkan bahwa *deepfake* banyak dimanfaatkan untuk tindakan yang melanggar hak moral, privasi, serta martabat korban, khususnya perempuan. Dampaknya bukan hanya pada individu, tetapi

juga pada tatanan sosial, karena mengikis kepercayaan publik terhadap informasi digital dan memperburuk krisis epistemik yang dapat melemahkan demokrasi. (Vaccari, 2020).

Di Indonesia sendiri, pemanfaatan teknologi *deepfake* semakin menunjukkan peningkatan. Pada Januari 2025, Direktorat Tindak Pidana Siber Bareskrim Polri menangkap seorang pelaku yang membuat video *deepfake* Presiden Prabowo Subianto untuk menipu masyarakat dengan modus bantuan dana, yang mengakibatkan kerugian hingga Rp65 juta. (CNN Indonesia, 2025). Kasus lain terjadi di Universitas Udayana, di mana seorang mahasiswa memanipulasi wajah lebih dari 30 mahasiswi ke dalam video pornografi berbasis. (Kompas, 2025). Kedua kasus ini memperlihatkan bahwa *deepfake* tidak hanya digunakan sebagai instrumen penipuan finansial, tetapi juga sebagai sarana pelanggaran hak moral, privasi, dan kepribadian seseorang.

Dalam aspek hukum, Indonesia masih bergantung pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kedua regulasi ini memang menjadi kerangka hukum utama saat ini, tetapi secara substansial belum mengakomodasi perkembangan teknologi AI, termasuk *deepfake*, sehingga menimbulkan berbagai kesenjangan. Meskipun kehadiran UU PDP dapat dipandang sebagai langkah perbaikan regulasi di bidang privasi, instrumen ini masih bersifat

generik dan belum menjawab tantangan spesifik yang ditimbulkan oleh konten berbasis AI seperti *deepfake*. (Arifin, 2024).

Pertama, terdapat gap normatif, karena tidak ada aturan eksplisit mengenai penggunaan identitas digital seseorang, mekanisme persetujuan (consent), atau instrumen teknis seperti pelabelan dan *watermarking* konten sintetis. (Putri, 2024). Aparat penegak hukum masih mengandalkan pasal penipuan atau pencemaran nama baik sebagai substitusi dalam menjerat pelaku, alih-alih menggunakan kerangka hukum yang secara spesifik mengatur teknologi berbasis AI. (Prakoso, 2025). Hal ini menimbulkan sejumlah konsekuensi penting. Pertama, aparat penegak hukum menghadapi kebingungan dalam menentukan ranah hukum yang tepat untuk menangani kasus *deepfake*, mengingat belum adanya aturan khusus yang mengatur secara jelas. (Prakoso, 2025). Kedua, terdapat kesulitan dalam membedakan apakah suatu konten bersifat asli atau hasil manipulasi, sehingga kebenaran faktual sering kali tidak dapat dibuktikan secara meyakinkan. Ketiga, perlindungan terhadap hak privasi masyarakat masih sangat minim, karena regulasi yang ada belum memberikan mekanisme komprehensif untuk melindungi individu dari penyalahgunaan identitas digitalnya. Dengan demikian, penegakan hukum terhadap kasus *deepfake* di Indonesia tidak hanya menunjukkan kelemahan dari sisi efektivitas, tetapi juga berpotensi menimbulkan inkonsistensi dalam penerapan, menciptakan ketidakadilan bagi para pihak, serta mengabaikan pemenuhan hak privasi. Ketiga, masih terdapat kesenjangan

dalam kajian akademik, di mana literatur hukum di Indonesia umumnya hanya membahas isu privasi dan perlindungan data pribadi secara umum, namun belum memberikan telaah yang mendalam mengenai implikasi teknologi *deepfake* terhadap hak moral serta hak kepribadian individu. (Cyberspace Administration of China, 2023).

Sementara itu, negara lain telah mengambil langkah yang lebih progresif. Tiongkok, misalnya, melalui *Provisions on the Administration of Deep Synthesis Internet Information Services* yang berlaku sejak Januari 2023, mewajibkan pelabelan konten *deepfake*, penerapan watermark, serta pengawasan ketat terhadap penyedia layanan berbasis kecerdasan buatan. (Cyberspace Administration of China, 2023). Berdasarkan kondisi tersebut, penelitian ini menegaskan adanya kesenjangan yang kompleks meliputi aspek normatif, penegakan hukum, akademik, dan perbandingan hukum. Oleh karena itu, artikel ini berkontribusi dengan memberikan analisis yuridis normatif mengenai posisi *deepfake* dalam sistem hukum Indonesia serta melakukan studi perbandingan dengan kerangka regulasi di negara lain, khususnya Tiongkok yang telah lebih maju dalam mengatur teknologi sintetis berbasis AI. (Zhou, 2025). Melalui pendekatan perbandingan hukum ini, penelitian tidak hanya bertujuan mengidentifikasi kelemahan sistem hukum Indonesia, tetapi juga menarik pelajaran (lesson learned) dari praktik internasional yang dapat menjadi dasar rekomendasi bagi pembaruan regulasi di Indonesia. Untuk menjawab permasalahan tersebut, penelitian ini menggunakan pendekatan yuridis normatif dengan

mengkaji regulasi, doktrin, putusan pengadilan, serta instrumen hukum internasional. (Marzuki, 2021) Bagian selanjutnya akan menguraikan metode penelitian, hasil analisis, serta implikasi normatif yang dapat menjadi rujukan bagi pengembangan regulasi AI di Indonesia. Regulasi tersebut menegaskan bahwa Tiongkok telah mengadopsi pendekatan preventif dan teknis dalam menghadapi risiko *deepfake*. Kondisi ini sangat kontras dengan Indonesia yang hingga kini belum memiliki instrumen hukum khusus, sehingga respons yang ada masih bersifat tidak komprehensif dan kurang efektif dalam menjawab tantangan yang ditimbulkan oleh konten sintetis berbasis AI seperti *deepfake*.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang menelaah hukum sebagai norma, asas, dan sistem yang berlaku dalam masyarakat serta tercermin dalam peraturan perundang-undangan dan putusan pengadilan. Jenis penelitian ini bersifat deskriptif-analitis dengan pendekatan perundang-undangan (statute approach) dan perbandingan (comparative approach), yang ditujukan untuk menelaah pengaturan hukum mengenai rekayasa data visual (*deepfake*) berbasis kecerdasan buatan serta implikasinya terhadap hak privasi dan hak moral individu di Indonesia dan Tiongkok. Data yang digunakan merupakan data sekunder hasil studi pustaka, yang mencakup bahan hukum primer seperti UUD 1945, UU ITE, UU PDP, dan *Provisions on the Administration of Deep Synthesis Internet Information Services* (Tiongkok, 2023); bahan

hukum sekunder berupa buku, jurnal ilmiah, dan publikasi akademik; serta bahan hukum non-hukum seperti kamus hukum, ensiklopedia, dan dokumen penunjang lainnya untuk memperjelas makna norma. Analisis data dilakukan secara deduktif, dengan menarik kesimpulan dari norma hukum yang bersifat umum menuju permasalahan khusus untuk menilai kesesuaian antara prinsip hukum dan realitas sosial dalam menghadapi fenomena *deepfake*. Melalui metode ini, penelitian diharapkan dapat menghasilkan pemahaman komprehensif yang tidak hanya menggambarkan kondisi pengaturan hukum yang ada, tetapi juga memberikan rekomendasi konkret bagi penguatan perlindungan hak privasi di Indonesia dalam era perkembangan kecerdasan buatan.

HASIL DAN PEMBAHASAN

Bentuk pengaturan hukum di Indonesia terhadap keberadaan konten *deepfake* yang dihasilkan melalui teknologi kecerdasan buatan (AI)

Perkembangan teknologi kecerdasan buatan di Indonesia telah menghadirkan dinamika hukum baru yang menuntut penyesuaian norma untuk perlindungan hak privasi dan identitas digital. (Marzuki, 2021) Salah satu perkembangan paling signifikan dalam bidang kecerdasan buatan ialah munculnya teknologi *deepfake*, yang secara teknis merupakan hasil penerapan algoritma *deep learning* untuk memanipulasi data visual dan audio. (Hanny, 2021). Teknologi ini memungkinkan seseorang mengubah wajah, suara, bahkan gerak tubuh individu lain sehingga tampak autentik, meskipun sepenuhnya merupakan hasil sintesis digital.

(Hao, 2023). Kondisi ini menimbulkan persoalan serius bagi dunia hukum, khususnya dalam konteks perlindungan data pribadi dan hak privasi. (Sekaring, 2025). Fenomena *deepfake* ialah rekayasa citra wajah dan suara menggunakan algoritma AI menjadi ancaman nyata terhadap perlindungan data pribadi. Hingga saat ini, sistem hukum Indonesia belum memiliki regulasi khusus yang mengatur penggunaan maupun penyalahgunaan teknologi *deepfake* secara langsung. Perlindungan hukum terkait dengan perlindungan data pribadi masih mengandalkan aturan umum dalam undang undang nomor 11 tahun 2008 tentang informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kedua instrumen hukum tersebut sudah melindungi hak individu atas data pribadi dan mencegah penyebaran konten hoaks tetapi belum menjangkau terkait dengan fenomena *deepfake* yang melibatkan manipulasi visual dan suara.

Secara regulasi, hak privasi di Indonesia memiliki landasan yang kuat dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menjamin perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, serta harta benda seseorang. Pasal tersebut menjadi landasan utama bagi perlindungan identitas atau data pribadi setiap individu di ruang digital, sekaligus dasar pembentukan peraturan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik (UU ITE). UU PDP secara jelas mengakui wajah dan data biometrik sebagai bagian dari *data pribadi sensitif* yang wajib memperoleh persetujuan langsung sebelum diproses atau disebarluaskan. Namun dalam praktiknya, penegakan hukum terhadap pelanggaran privasi digital yang disebabkan oleh teknologi *deepfake* masih menghadapi kendala serius, khususnya dalam hal pembuktian serta penetapan tanggung jawab terhadap pelaku yang beroperasi melalui akun anonim atau menggunakan server di berbagai negara. Penelitian yang dilakukan oleh Rachman (2022) menegaskan bahwa UU ITE lebih banyak digunakan untuk menjerat pelaku penyebaran konten asusila, meskipun substansinya berbeda dengan kasus manipulasi wajah yang menimbulkan pelanggaran hak privasi. Akibatnya, aparat penegak hukum cenderung melakukan penegakan hukum yang bersifat reaktif dan spesifik tanpa pedoman khusus. (Widodo, 2023). Hal ini menimbulkan ketidakpastian hukum dalam praktik hukum siber karena ketiadaan norma spesifik yang mengatur konten digital hasil sintesis buatan kecerdasan buatan. (Arifin, 2024). Dengan demikian, meskipun secara normatif Indonesia telah memiliki instrumen hukum yang cukup memadai, namun secara substantif masih terdapat kekosongan hukum (legal vacuum) terhadap fenomena *deepfake* yang menuntut regulasi baru yang lebih adaptif terhadap perkembangan teknologi digital. (Rahmawati, 2023).

Jika ditinjau dari perspektif teori hukum, perlindungan terhadap individu dalam

konteks *deepfake* dapat dianalisis melalui teori hak privasi yang pertama kali dikemukakan oleh Samuel D. Warren dan Louis D. Brandeis dalam tulisannya berjudul *The Right to Privacy* (1890). Teori ini menekankan bahwa setiap orang memiliki hak mendasar untuk memperoleh privasi atau “hak untuk dibiarkan sendiri” (*the right to be let alone*) serta berhak mengatur segala bentuk informasi pribadinya yang tersebar di ruang publik. (Samuel, 1890). Dalam konteks hukum Indonesia, prinsip tersebut tercermin dalam konsep perlindungan data pribadi sebagaimana diatur dalam UU PDP, yang memberi hak kepada subjek data untuk memberikan atau mencabut persetujuan atas penggunaan data pribadinya. Akan tetapi, realita hukum menunjukkan bahwa prinsip tersebut belum sepenuhnya terimplementasi pada kasus-kasus *deepfake*, di mana citra wajah dan suara seseorang dapat digunakan tanpa izin untuk tujuan komersial maupun merendahkan martabat. (Adriani, 2024).

Selanjutnya, Alan Westin kemudian mengembangkan teori informational privacy, yang memandang privasi sebagai kemampuan individu untuk mengontrol kapan, bagaimana dan sejauh mana informasi pribadinya dikomunikasikan kepada orang lain. (Alan, 1967). Berdasarkan teori tersebut, penyalahgunaan *deepfake* secara langsung melanggar hak otonomi individu terhadap pengelolaan citra digitalnya. (Prabowo, 2023).

Dalam hukum Indonesia, pelanggaran semacam ini belum sepenuhnya dilindungi karena regulasi yang ada masih terbatas pada perlindungan data yang bersifat statis,

bukan dinamis seperti konten hasil sintesis AI. (Handayani, 2023). Hal ini menunjukkan bahwa negara perlu memperluas definisi hak privasi agar mencakup perlindungan terhadap bentuk-bentuk identitas digital yang dihasilkan melalui teknologi kecerdasan buatan. (Sihombing, 2024).

Keberadaan teknologi *deepfake* juga menimbulkan persoalan serius dari perspektif teori kepastian hukum, sebagaimana dikemukakan oleh Gustav Radbruch (1946) yang menegaskan bahwa hukum harus mencerminkan keadilan, kemanfaatan, dan kepastian. Dalam konteks Indonesia, prinsip kepastian hukum sebagaimana diatur dalam Pasal 28D ayat (1) UUD 1945 menuntut adanya regulasi yang jelas dan dapat ditegakkan terhadap pelanggaran berbasis teknologi digital. (Arifin, 2024). Namun hingga kini, belum terdapat pengaturan eksplisit yang mengatur rekayasa data visual atau *deepfake* dalam sistem hukum nasional, sehingga menimbulkan kekosongan hukum dalam penegakan hukum terhadap pelanggaran yang berkaitan dengan hak privasi dan reputasi individu. (Arifin, 2024).

Kondisi ini berimplikasi pada lemahnya perlindungan hukum terhadap korban, karena aparat penegak hukum masih berpedoman pada ketentuan umum dalam UU ITE dan KUHP yang tidak dirancang untuk fenomena sintesis digital berbasis AI. (Lestari, 2023). Beberapa ahli berpendapat bahwa kekosongan norma ini dapat mengakibatkan ketidakpastian dalam pembuktian unsur *mens rea* dan *actus reus* dari pelaku karena objek tindakannya bukanlah data fisik melainkan hasil pemrosesan algoritmik. (Rachman,

2023). Oleh sebab itu, perlu adanya pembaruan regulasi yang adaptif terhadap perubahan teknologi, dengan merujuk pada praktik negara lain yang telah lebih dahulu mengatur *deepfake* secara spesifik, seperti Tiongkok. (Rahmawati, 2025).

Dalam konteks harmonisasi hukum, pembentukan norma baru tidak hanya penting untuk memberikan kepastian hukum, tetapi juga untuk menjamin keadilan bagi korban serta menegaskan tanggung jawab hukum bagi pembuat dan penyebar konten *deepfake*. (Santoso, 2025). Sehingga, disimpulkan bahwa pengaturan hukum Indonesia terhadap fenomena *deepfake* masih bersifat parsial dan belum memiliki kekuatan normatif yang komprehensif. Ketentuan yang ada dalam UU ITE dan UU PDP baru mencakup aspek umum perlindungan data pribadi, tanpa mengatur mekanisme tanggung jawab hukum maupun prosedur pemulihan bagi korban penyalahgunaan konten hasil sintesis AI. (Prakoso, 2023).

Penelitian oleh Prakoso (2023) menegaskan perlunya mekanisme *notice-and-takedown* serta kerjasama antar-platform digital agar pemulihan hak korban dapat terlaksana secara efektif. (Sihombing, 2024). Di sisi lain, penegakan hukum yang reaktif tanpa regulasi preventif berpotensi menimbulkan ketidakpastian hukum dan mereduksi prinsip keadilan substantif sebagaimana ditekankan dalam teori Radbruch. (Gustav, 1946). Oleh sebab itu, Indonesia perlu membentuk regulasi khusus mengenai teknologi *deepfake* yang tidak hanya berorientasi pada sanksi, tetapi juga pada aspek etik, transparansi algoritma, dan tanggung jawab pengembang AI. (Santoso, 2025). Regulasi semacam ini

diharapkan mampu memperkuat sistem hukum nasional dalam menjamin perlindungan hak privasi dan martabat manusia di era digital. Pembentukan aturan tersebut juga penting sebagai langkah harmonisasi hukum internasional, terutama dengan melihat praktik negara-negara yang telah lebih dahulu menerapkan regulasi deep-synthesis seperti Tiongkok. (Rahmawati, 2023).

Kebijakan dan Regulasi yang Diterapkan oleh Pemerintah Tiongkok dalam Menghadapi Permasalahan Hukum yang Timbul Akibat Penyalahgunaan Teknologi Deepfake Berbasis AI

Negara Tiongkok telah menunjukkan langkah regulatif yang relatif cepat dalam menanggapi fenomena *deepfake*, misalnya dengan mengesahkan Provisions on the Administration of Deep Synthesis Internet Information Services yang mulai berlaku pada Januari 2023. (Cyberspace Administration of China, 2023). Regulasi tersebut memuat kewajiban bagi penyedia layanan sintesis digital untuk memberi label konten yang dihasilkan atau diedit oleh teknologi *deep synthesis*, serta melakukan verifikasi identitas pengguna sebelum memperbolehkan proses manipulasi biometric seperti wajah dan suara. (Law, 2023). Ketentuan ini menandai pendekatan “labeling + traceability” yang secara spesifik merespons risiko dari rekayasa konten berbasis algoritma pembelajaran mesin. (Hao, 2023). Studi perbandingan menunjukkan bahwa dengan regulasi semacam ini, Tiongkok mengubah kerangka kerja perlindungan data pribadi dan keamanan informasi dalam satu paket kebijakan digital yang relatif terkoordinasi. (Zhang, 2024).

Meskipun demikian, para pengamat hukum mencatat bahwa regulasi Tiongkok cenderung menekankan pengendalian sosial dan stabilitas kolektif daripada hak individu atas privasi atau kehormatan personal. (Creemers, 2024). Dalam praktiknya, platform digital di Tiongkok diwajibkan melakukan identifikasi real-name, menyimpan rekam jejak aktivitas, dan melakukan penilaian risiko konten secara mandiri atau melalui lembaga yang ditunjuk pemerintah. (Cyberspace

Administration of China, 2023). Hal ini menunjukkan bahwa regulasi Tiongkok menggabungkan unsur administratif dan pengawasan yang intensif, berbeda dari pendekatan negara lain yang lebih desentralisasi. (Qiu, 2024). Dengan demikian, regulasi Tiongkok bisa dianggap sebagai model untuk pemahaman regulatif dalam kasus *deepfake*, walaupun fokusnya bukan semata hak individu tetapi juga kepentingan publik dan kontrol negara. Farid, 2021).

Analisis hukum Tiongkok menunjukkan bahwa pengaturan “*deep synthesis*” tidak hanya diatur melalui undang-undang biasa, tetapi melalui peraturan administratif yang dikeluarkan oleh badan regulasi seperti *Cyberspace Administration of China* (CAC) dan kementerian terkait, yang memungkinkan pengetatan aturan dengan proses legislasi yang lebih cepat. Misalnya, regulasi mewajibkan agar setiap layanan yang menyediakan teknologi rekayasa citra manusia atau audio mendapatkan persetujuan, melakukan penilaian keamanan, dan menandai konten sehingga pengguna memahami bahwa konten tersebut bukanlah rekaman real. (Wu, 2023). Pendekatan ini mencerminkan konsep

regulasi responsif terhadap teknologi yang berkembang cepat, namun juga menimbulkan pertanyaan mengenai keterbatasan akses bagi inovasi teknologi. (Shen, 2024). Beberapa penelitian menunjukkan bahwa beban regulasi pada startup teknologi di Tiongkok meningkat, dan hal ini dapat memperkuat dominasi perusahaan besar yang memiliki sumber daya untuk mematuhi regulasi tersebut. (Liu, 2024).

Namun dari sisi penegakan, tindakan cepat terhadap aplikasi manipulasi wajah tanpa izin telah dilaporkan sebagai upaya konkret dalam menangani penyalahgunaan *deepfake*. Sebagai contoh, kasus manipulasi wajah selebritas dan orang biasa yang tersebar melalui aplikasi Tiongkok menjadi salah satu pemicu utama regulasi tersebut. (Quan, 2024). Temuan ini menunjukkan bahwa regulasi Tiongkok tidak hanya teoritis, tetapi juga berdasarkan pengalaman empiris terhadap kerugian yang ditimbulkan. (Zhou, 2025).

Dari perspektif teori hak privasi dan hak data pribadi, regulasi Tiongkok dapat ditinjau sebagai upaya negara untuk memasukkan teknologi *deep synthesis* ke dalam kerangka perlindungan data pribadi yang lebih luas. (Wang, 2024). Meskipun demikian, karena orientasi regulasinya lebih ke arah kepentingan sosial dan keamanan nasional, maka implikasi terhadap hak individu seperti otonomi atas citra dan suara masih mendapatkan kritikan. (Zhang, 2024). Teori “*right to informational self-determination*” menyebut bahwa setiap individu berhak mengontrol bagaimana data pribadinya digunakan dan dikomunikasikan namun regulasi Tiongkok dalam praktik menunjukkan bahwa kontrol ini

sering kali bergeser ke pengawasan negara dan platform. (Cheng, 2023).

Dalam konteks rekayasa wajah tanpa izin, regulasi Tiongkok menerapkan verifikasi identitas dan penandaan konten, tetapi persoalan ganti rugi bagi korban atau mekanisme restitusi belum banyak dibahas secara publik. (Li, 2024). Hal ini berbeda dengan teori tanggung jawab perdata di mana korban berhak mendapatkan pemulihan atas kerugian yang dialami. (Chen, 2023). Dengan demikian, regulasi Tiongkok bisa dilihat sebagai model “pengaturan cepat” yang efektif dari sisi pengawasan, namun belum sepenuhnya memenuhi standar hak individu yang lebih luwes seperti yang dikembangkan di negara-barat. (Guo, 2024).

Melihat kelebihan dan kekurangan sistem regulasi Tiongkok, terdapat beberapa pelajaran yang relevan untuk negara lain, termasuk Indonesia. (Santoso, 2025). Kelebihannya meliputi adanya peraturan eksplisit yang menyebut rekayasa konten digital (deep synthesis), kewajiban pelabelan, dan mekanisme identifikasi yang terstruktur unsur yang masih belum ditemukan dalam regulasi Indonesia hingga kini. (Rahmawati, 2025). Di sisi lain, orientasi yang sangat kuat pada stabilitas sosial dan kontrol negara dapat menimbulkan risiko pembatasan kebebasan inovasi maupun kebebasan berekspresi, sebagaimana beberapa pengamat catat dalam studi tentang implementasi aturan di Tiongkok. (Creemers, 2024).

Untuk itu, jika Indonesia ingin mengadopsi elemen regulasi Tiongkok, penyesuaian harus dilakukan agar tetap menjaga keseimbangan antara inovasi

teknologi, hak privasi individu, dan tanggung jawab sosial. (Putri, 2021). Strategi yang disarankan meliputi pengembangan regulasi khusus *deepfake*, penguatan mekanisme ganti rugi dan pemulihan korban, serta kolaborasi multi-stakeholder antara pemerintah, industri teknologi, dan masyarakat sipil. (Prakoso, 2025). Dengan demikian, Indonesia dapat memperkuat kerangka hukum nasional yang adaptif dan responsif terhadap tantangan teknologi AI tanpa mengabaikan prinsip hak asasi manusia dan keadilan. (Marzuki, 2021).

Urgensi Pembentukan Regulasi Khusus Mengenai Penggunaan dan Penyalahgunaan Teknologi *Deepfake* Berbasis Kecerdasan Buatan di Indonesia?

Urgensi pembentukan regulasi khusus mengenai teknologi *deepfake* di Indonesia berangkat dari kenyataan bahwa perkembangan kecerdasan buatan telah melampaui kemampuan adaptasi sistem hukum nasional. (widodo, 2025). Hukum positif yang berlaku masih berfokus pada perlindungan data pribadi dan penyebaran konten bermuatan kesusilaan, belum menyentuh dimensi sintesis digital yang memanipulasi wajah atau suara manusia. (Rachmawati, 2025).

Fenomena *deepfake* telah menimbulkan berbagai risiko sosial, mulai dari penyebaran disinformasi, eksplorasi seksual, hingga pencemaran nama baik yang sulit dipulihkan karena bukti digital bersifat cair dan mudah dihapus. (Sekaring, 2025). Penelitian yang dilakukan oleh Kusnadi (2024) menyebutkan bahwa tanpa regulasi spesifik, aparat penegak hukum hanya

dapat menggunakan pasal-pasal umum dalam UU ITE yang bersifat represif, bukan preventif. (Sekaring, 2025). Kondisi tersebut memperlemah fungsi hukum sebagai sarana perlindungan masyarakat dan menimbulkan *legal uncertainty* di ranah siber. Oleh karena itu, pembentukan regulasi khusus menjadi kebutuhan mendesak untuk menjembatani kesenjangan antara kemajuan teknologi dan mekanisme hukum yang tersedia. (Prakoso, 2024).

Pembentukan regulasi deepfake di Indonesia perlu didasarkan pada pendekatan multidimensional, mencakup aspek etika, privasi, dan tanggung jawab hukum. (Marzuki, 2021). Dari sisi etika, penggunaan kecerdasan buatan harus sejalan dengan prinsip-prinsip AI ethics yang menjamin keadilan, transparansi, dan non-diskriminasi. (UNESCO, 2023). Sedangkan dari sisi hukum, regulasi perlu menetapkan batasan yang jelas antara penggunaan sah teknologi sintesis untuk tujuan kreatif atau edukatif dengan penggunaan ilegal yang melanggar hak privasi dan kehormatan individu. (Handayani, 2024).

Selain itu, pembentukan regulasi harus mengatur kewajiban platform digital untuk melakukan labeling dan traceability terhadap konten hasil AI, seperti yang diterapkan dalam sistem hukum Tiongkok. (Handayani, 2024). Menurut Widodo (2025), integrasi prinsip etika dalam norma hukum tidak hanya mencegah penyalahgunaan teknologi, tetapi juga memperkuat legitimasi hukum di mata masyarakat digital. (Widodo, 2025). Dengan demikian, pembentukan regulasi deepfake bukan hanya soal pembatasan, tetapi

juga penguatan nilai-nilai hukum yang humanis dan adaptif terhadap perubahan zaman. (Sutanto, 2024).

Secara komparatif, keberhasilan Tiongkok dalam membentuk regulasi deep synthesis dapat menjadi referensi bagi Indonesia dalam merumuskan kebijakan yang tepat. (Zhang, 2024). Pendekatan Tiongkok yang menekankan labeling, identifikasi pengguna, dan verifikasi algoritma dapat diadaptasi untuk memperkuat mekanisme penegakan hukum di Indonesia. (Santoso, 2025).

Namun, regulasi Indonesia harus tetap menjunjung prinsip-prinsip hak asasi manusia sebagaimana diatur dalam Pasal 28G UUD 1945 dan Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Perbandingan ini menunjukkan bahwa sistem hukum Tiongkok lebih menekankan keamanan kolektif, sedangkan Indonesia perlu mengedepankan perlindungan terhadap hak individu. (Cheng, 2024). Dengan belajar dari model Tiongkok tanpa mengabaikan konteks sosial-politik domestik, Indonesia dapat membentuk regulasi yang tidak hanya menindak pelanggaran, tetapi juga mendorong inovasi AI yang bertanggung jawab. (Zhang, 2024).

Oleh sebab itu, harmonisasi antara aspek keamanan digital dan perlindungan hak individu menjadi kunci utama dalam merumuskan kebijakan hukum deepfake di Indonesia. Dari perspektif teori hukum pembangunan yang dikemukakan oleh Mochtar Kusumaatmadja, hukum harus berperan sebagai sarana pembaharuan masyarakat (law as a tool of social engineering). (Mochtar, 2020). Dalam konteks ini, pembentukan regulasi

deepfake bukan hanya bertujuan represif, tetapi juga preventif dan edukatif. Regulasi diharapkan dapat mendorong kesadaran masyarakat terhadap etika digital serta memberikan panduan yang jelas bagi pelaku industri kreatif yang menggunakan teknologi sintesis secara sah.

Kajian oleh Prabowo (2024) menegaskan bahwa pendekatan preventif melalui edukasi digital dan *media literacy* akan lebih efektif dalam menekan penyalahgunaan teknologi dibanding penegakan hukum yang semata-mata berbasis sanksi. (Sihombing, 2024). Dengan demikian, rancangan regulasi deepfake harus mencakup program literasi digital, mekanisme notice-and-takedown, serta kewajiban pelaporan bagi platform daring. (Prakoso, 2024). Upaya ini dapat memperkuat posisi hukum sebagai instrumen pembinaan masyarakat, bukan sekadar alat pemidanaan.

Dengan mempertimbangkan kompleksitas sosial dan teknologi, urgensi pembentukan regulasi deepfake di Indonesia tidak dapat ditunda lagi. Regulasi tersebut harus disusun melalui kolaborasi multi-pihak yang melibatkan pemerintah, akademisi, pelaku industri teknologi, serta masyarakat sipil agar menghasilkan norma yang implementatif dan berkeadilan. (Santoso, 2025). Selain mengatur tanggung jawab hukum pelaku, regulasi juga perlu memuat mekanisme pemulihan bagi korban, termasuk hak atas penghapusan data dan kompensasi atas kerugian immateriil. Penguatan lembaga perlindungan data pribadi menjadi faktor penting untuk memastikan efektivitas implementasi regulasi tersebut. (Prabowo, 2025).

Apabila hal ini dapat direalisasikan, Indonesia akan memiliki kerangka hukum yang tidak hanya reaktif terhadap pelanggaran, tetapi juga proaktif dalam mencegah penyalahgunaan teknologi kecerdasan buatan. (Rachman, 2025). Oleh karena itu, pembentukan regulasi deepfake merupakan langkah strategis dalam membangun sistem hukum digital yang adaptif, berkeadilan, dan berorientasi pada perlindungan martabat manusia di era AI.

SIMPULAN

Perkembangan teknologi deepfake berbasis kecerdasan buatan telah menciptakan tantangan serius bagi perlindungan hak privasi, hak moral, dan integritas identitas digital masyarakat Indonesia. Hasil penelitian menunjukkan bahwa kerangka hukum nasional, termasuk UU ITE (UU 1/2024) dan UU PDP (2022), belum memberikan pengaturan spesifik terhadap manipulasi data visual, sehingga menyebabkan terjadinya kekosongan norma dan ketidakpastian dalam penegakan hukum. Aparat penegak hukum terpaksa menggunakan pas-pasal generik yang tidak dirancang untuk mengatasi rekayasa digital berbasis algoritma, sehingga menimbulkan kesulitan pembuktian, ketiadaan mekanisme pemulihan korban, serta potensi ketidakadilan dalam proses hukum. Ketidaksiapan regulasi ini semakin terlihat dari meningkatnya kasus penyalahgunaan deepfake untuk penipuan, pornografi non-konsensual, dan serangan reputasi, yang seluruhnya belum dapat dijawab secara efektif oleh instrumen hukum yang ada.

Studi perbandingan dengan Tiongkok menunjukkan bahwa

negara tersebut telah mengambil langkah lebih progresif melalui Deep Synthesis Regulation (2023) yang mengatur pelabelan konten sintetis, watermarking, verifikasi identitas, kewajiban penyedia layanan AI, serta mekanisme perlindungan korban yang lebih kuat. Pendekatan ini bersifat preventif dan teknis, berbeda dengan pendekatan Indonesia yang masih reaktif.

Berdasarkan temuan tersebut, penelitian ini menegaskan urgensi pembentukan regulasi khusus mengenai deepfake di Indonesia, yang tidak hanya menutup kekosongan hukum, tetapi juga memastikan perlindungan komprehensif terhadap hak privasi, hak moral, dan keamanan digital masyarakat. Regulasi baru perlu mengadopsi standar etik, transparansi algoritma, tanggung jawab platform, serta mekanisme pemulihan korban yang selaras dengan praktik internasional, sekaligus disesuaikan dengan prinsip-prinsip hukum nasional. Dengan demikian, Indonesia dapat membangun sistem hukum yang lebih adaptif, responsif, dan relevan terhadap risiko teknologi kecerdasan buatan di masa mendatang.

DAFTAR PUSTAKA

- Adriani, S. R. (2024). Hak Privasi di Era Artificial Intelligence: Tantangan Implementasi UU PDP. *Jurnal Hukum dan Teknologi Digital Indonesia*. 2(1). 30–33.
- Alan F. W. (1967). *Privacy and Freedom*. Atheneum Press. New York.
- APJII. (2024). Asosiasi Penyelenggara Jasa Internet Indonesia. *Laporan Survei Internet APJII 2024*. Jakarta.
- Arifin, F., & Nugraha, M. (2024). Kekosongan Norma terhadap Teknologi Kecerdasan Buatan dalam UU ITE. *Jurnal Legislasi Indonesia*. 21(1). 20–23.
- Arifin, F., & Nugraha, M. (2024). Urgensi Pembentukan Regulasi Khusus Deepfake di Indonesia. *Jurnal Legislasi Indonesia*. 21(1). 18–20.
- CAC. (10 Januari 2023). Cyberspace Administration of China. *Provisions on the Administration of Deep Synthesis Internet Information Services*,
- Chen, P. (2023). *AI and Law in China: A Comparative Perspective*. Springer. Singapore.
- Cheng, B. (2023). The Right to Informational Self-Determination in the Chinese Context. *Data Protection Law Review Asia*. 2(3). 45–59.
- China, L. (2023). Deep Synthesis Provisions (Effective 10 Jan 2023). *China Law Translate*.
- CNN Indonesia. (2025, Januari 25). *Bareskrim tangkap pelaku deepfake video Presiden Prabowo untuk penipuan bantuan dana*.
- Creemers, T. (2024). Cyber Governance with Chinese Characteristics. *Journal of Cyber Policy*. 9(2). 119–135.
- Deeptrace Labs. (2019). *The State of Deepfakes: Landscape, Threats, and Impact*. Deeptrace Labs. Amsterdam
- Farid, H. (2021). *Digital Forensics and Deepfakes: Understanding Synthetic Media and Its Societal Impact*. MIT Press. Cambridge.

- Guo, Z. (2024). Evaluating Human Rights in AI Regulation: The Chinese Approach. *Human Rights and Technology Journal*. 3(2). 128–142.
- Gustav, R. (1946). *Rechtsphilosophie*, C.F. Müller. Heidelberg.
- Handayani, F., & Maulana, R. (2023). Urgensi Perlindungan Identitas Digital dalam UU PDP. *Jurnal Legislasi Indonesia*. 20(3). 279–282.
- Hao, L. (2023). Emerging Threat of Deepfakes: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 45(2). 789–803.
- Kompas.com. (2025, Februari 2). *Kasus deepfake di kampus: Mahasiswa Udayana manipulasi wajah mahasiswi ke video*.
- Lestari, M. (2023). Kendala Penegakan Hukum Digital di Indonesia. *Jurnal Hukum dan Teknologi Informasi*. 3(2). 45–48.
- Li, Y., & Hu, J. (2024). Civil Liability for Unauthorized AI Generated Content. *Chinese Journal of Private Law*. 22(4). 200–214.
- Liu, Y. (2024). Compliance Costs and Innovation Risks Under Deep Synthesis Regulations. *Tsinghua Law Review*. 27(3). 101–115.
- Marzuki, P. M. (2021). *Pengantar Ilmu Hukum*. Kencana. Jakarta
- Mochtar, K. (2020). *Hukum, Masyarakat dan Pembinaan Hukum Nasional*. Bina Cipta, Bandung.
- Prabowo, N. (2025). Penguatan Lembaga Perlindungan Data dalam Implementasi UU PDP.” *Jurnal Hukum dan Pembangunan Nasional*. 55(2). 312–315.
- Prakoso, R. (2025). Implementasi *Notice-and-Takedown* untuk Perlindungan Data Digital. *Jurnal Hukum dan Pembangunan Nasional*. 55(1). 76–78.
- Prakoso, R. (2025). Legal Gaps in Artificial Intelligence Regulation: A Case Study of Deepfake in Indonesia,” *Lex Et Societatis Journal*. 12(1). 41–44.
- Qiu, J. (2024). Algorithmic Regulation and State Control in China’s Digital Ecosystem. *China Information Journal*. 38(1). 77–92.
- Quan, Z. (26 March 2024). Hangzhou Man Sentenced for Deep-Fake Pornography. *China Daily*,
- Rachman, A. (2025). Reformasi Hukum Siber untuk Mencegah Penyalahgunaan Teknologi AI. *Rechtsvinding Journal of Law and Policy*. 14(2). 252–255.
- Rachman, A., & Sutanto, R. (2023). Analisis Yuridis Terhadap Pembuktian Kejahatan Berbasis AI. *Jurnal Hukum dan Pembangunan Nasional*, 54(3). 321–324.
- Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, *Harvard Law Review*, Vol. 4 No. 5 (1890): 193–220.
- Santoso, H. (2025). Kolaborasi Multi-Stakeholder dalam Pembentukan Hukum AI. *Jurnal Teknologi dan Kebijakan Publik*. 4(1). 88–90.
- Santoso, H., & Prabowo, R. (2025). Pembentukan Hukum Adaptif terhadap Perkembangan AI di Indonesia. *Jurnal Hukum dan Pembangunan*, 55(1). 65–68.
- Shen, A. (2024). Responsive Legislation for Emerging Technologies in China. *Peking*

- University Law Review.* 36(1). 19–33.
- Sihombing, P. K. (2024). Implementasi *Notice-and-Takedown* untuk Perlindungan Hak Digital. *Rechtsvinding Journal of Law and Policy.* 14(2). 248–251.
- Sutanto, R. (2024). Prinsip Humanisme dalam Hukum Digital Indonesia. *Jurnal Lex Renaissance.* 9(1). 19–22.
- 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).
- Wang, M. (2024). Personal Information Protection and Deep Synthesis Rules in China. *Journal of East Asian Law.* 18(2). 99–112.
- Widodo, I. P. N. (2023). Kendala Penegakan Hukum Siber terhadap Pelanggaran Hak Privasi di Indonesia. *Jurnal Rechtsvinding.* 13(2). 211–213.
- Wu, M., & Chen, L. (2023). Regulating Deep Synthesis Technology Under China's Cybersecurity Law. *Chinese Journal of Communication Law.* 12(2). 142–158.
- Zhang, L., & Feng, P. (2024). Balancing AI Innovation and Privacy in Chinese Law. *Frontiers of Law in China.* 19(1). 1–18.
- Zhang, Y., & Li, H. (2023). Digital Governance in China's AI Era: The Deep Synthesis Rules. *Asia Pacific Law Review.* 31(1). 45–62.
- Zhou, H., & Wei, J. (2025). Empirical Study on AI Generated Content and Legal Responsibility in China. *Asia Law Review.* 15(1). 55–60.