



Hukum dan Etika Deepfake Urgensi Regulasi Khusus atas Konten Manipulatif di Media Sosial dalam Konteks Demokrasi Digital

Althea Serafim Kriswandaru ^{a,1}, Berliant Pertiwi ^{b,2}

^aUniversitas Sains dan Teknologi Komputer (STEKOM), Indonesia

^bUniversitas Sains dan Teknologi Komputer (STEKOM), Indonesia

¹altheaserafim@stekom.ac.id ²berliant@stekom.ac.id

* email korespodensi : altheaserafim@stekom.ac.id

INFORMASI ARTIKEL

Sejarah Artikel

Diserahkan

2025-04-16

Diterima

2025-04-21

Dipublikasikan

2025-04-30

Kata Kunci:

AI-Generated Disinformation;

Deepfake Regulation;

Digital Democracy;

ABSTRAK

The proliferation of deepfake technology, powered by artificial intelligence, presents a growing threat to digital democracy by enabling the spread of highly realistic manipulated content that can distort public perception, undermine trust, and disrupt electoral integrity. This study critically examines the urgency of establishing specific legal regulations for deepfake content in Indonesia, where existing cyber laws remain too general to address the nuances of AI-generated disinformation. Employing a qualitative normative-legal approach and comparative analysis with legal frameworks in the United States, South Korea, and the European Union, the research identifies a significant regulatory gap and offers a multidimensional framework that integrates legal, ethical, and democratic perspectives. The findings reveal that Indonesia lacks a clear definition and legal category for manipulated content, resulting in insufficient legal protections for individuals and institutions vulnerable to digital deception. The study proposes a context-sensitive model of regulation that aligns with international best practices and responds to Indonesia's legal and sociopolitical realities. This research contributes to the discourse on digital law by offering a novel regulatory scheme capable of addressing the ethical and democratic challenges posed by deepfake technology.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.

1. PENDAHULUAN

Perkembangan teknologi digital dalam dua dekade terakhir mengubah cara manusia memproduksi, mengakses, dan menyebarkan informasi ¹. Salah satu teknologi yang memicu perdebatan luas adalah deepfake, yakni hasil rekayasa konten digital berbasis kecerdasan buatan (AI) yang dapat memanipulasi wajah, suara, hingga gerakan tubuh seseorang dengan tingkat realisme tinggi ². Meskipun awalnya dimanfaatkan untuk hiburan dan industri kreatif, deepfake

¹ Rajat Chakraborty and Ruchira Naskar, 'Role of Human Physiology and Facial Biomechanics towards Building Robust Deepfake Detectors: A Comprehensive Survey and Analysis', *Computer Science Review*, 54 (2024), doi:10.1016/j.cosrev.2024.100677.

² Momina Masood and others, 'Deepfakes Generation and Detection: State-of-the-Art, Open Challenges, Countermeasures, and Way Forward', *Applied Intelligence*, 53.4 (2023), pp. 3974–4026, doi:10.1007/s10489-022-03766-z.

telah berkembang menjadi alat manipulasi yang mengancam integritas ruang publik digital³. Di tengah arus informasi yang masif dan kecepatan distribusi konten melalui media sosial, teknologi ini semakin sulit untuk dikendalikan, apalagi diidentifikasi secara awam⁴. Keberadaan konten manipulatif semacam ini menimbulkan kekhawatiran, tidak hanya terhadap aspek privasi individu, tetapi juga terhadap fondasi demokrasi, yakni kepercayaan publik terhadap informasi dan aktor politik⁵.

Di Indonesia, yang merupakan salah satu negara dengan penetrasi media sosial tertinggi di dunia, ancaman yang ditimbulkan oleh teknologi deepfake menjadi semakin relevan⁶. Demokrasi digital yang idealnya menjadi instrumen partisipatif dalam membangun masyarakat sipil justru bisa terancam ketika disinformasi yang disisipkan dalam konten palsu tidak dibatasi oleh regulasi hukum yang memadai⁷. Deepfake tidak sekadar mengaburkan batas antara fakta dan fiksi, tetapi juga berpotensi menjadi senjata politik dalam kontestasi elektoral dan konflik sosial⁸. Di tengah situasi tersebut, muncul kebutuhan mendesak untuk memahami dan mengatur teknologi ini secara sistematis agar demokrasi digital tidak menjadi korban dari kemajuan teknologi yang tidak terkelola⁹.

Sayangnya, sistem hukum di Indonesia belum memiliki mekanisme yang memadai untuk merespons dinamika baru ini¹⁰. Ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan perlindungan data pribadi belum secara eksplisit mencakup kategori konten berbasis AI seperti deepfake¹¹. Ketiadaan regulasi khusus menimbulkan kekosongan hukum yang bisa dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab¹². Di sisi lain, masyarakat juga belum sepenuhnya menyadari ancaman yang ditimbulkan oleh konten palsu berbasis teknologi, apalagi ketika konten tersebut diproduksi dengan kecanggihan teknis yang sulit dibedakan dari kenyataan¹³. Oleh karena itu, diperlukan kajian mendalam yang

³ Anesa Hasani and others, 'Personal Rights and Intellectual Properties in the Upcoming Era: The Rise of Deepfake Technologies', *Lecture Notes in Networks and Systems*, 1036 LNNS (2024), pp. 379–91, doi:10.1007/978-3-031-62881-8_32.

⁴ Evgeny Pashentsev, 'The Malicious Use of Deepfakes Against Psychological Security and Political Stability', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 47–80, doi:10.1007/978-3-031-22552-9_3.

⁵ Arash Heidari and others, 'Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 14.2 (2024), pp. 1–45, doi:10.1002/widm.1520.

⁶ Sergei A. Samoilenko and Inna Suvorova, 'Artificial Intelligence and Deepfakes in Strategic Deception Campaigns: The U.S. and Russian Experiences', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 507–29, doi:10.1007/978-3-031-22552-9_19.

⁷ Mohamed Chawki, 'Navigating Legal Challenges of Deepfakes in the American Context: A Call to Action', *Cogent Engineering*, 11.1 (2024), doi:10.1080/23311916.2024.2320971.

⁸ Jelena Cupać, Hendrik Schopmans, and İrem Tuncer-Ebetürk, 'Democratization in the Age of Artificial Intelligence: Introduction to the Special Issue', *Democratization*, 31.5 (2024), pp. 899–921, doi:10.1080/13510347.2024.2338852.

⁹ Darya Bazarkina and others, 'The Threats and Current Practices of Malicious Use of Artificial Intelligence in Psychological Security in China', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 335–75, doi:10.1007/978-3-031-22552-9_13.

¹⁰ Anton Liagusha and Dmytro Iarovy, 'Memes, Freedom, and Resilience to Information Disorders: Information Warfare between Democracies and Autocracies', *Social Sciences and Humanities Open*, 11 (2025), doi:10.1016/j.ssaho.2024.101247.

¹¹ Dewi Sulistianingsih and others, 'Online Dispute Resolution: Does the System Actually Enhance the Mediation Framework?', *Cogent Social Sciences*, 9.1 (2023), doi:10.1080/23311886.2023.2206348.

¹² Amelia Cahyadani and others, 'Adopting Pillar One: An Ideal Model for the Transformation of Indonesia's Tax Law to Realize SDGs Goal XVII and Its Challenges', *Cogent Social Sciences*, 11.1 (2025), doi:10.1080/23311886.2025.2459321.

¹³ Yulu Jin and Yu Wang, 'Reassessing Smart City Development and Personal Data Protection: A Regulatory Framework', *International Review of Economics and Finance*, 99 (2025), doi:10.1016/j.iref.2025.104022.

tidak hanya melihat aspek teknis, tetapi juga menelusuri dimensi hukum dan etika dari fenomena ini ¹⁴.

Data terbaru menunjukkan bahwa produksi konten deepfake mengalami lonjakan drastis secara global. Laporan ¹⁵ mengungkapkan bahwa jumlah video deepfake yang teridentifikasi meningkat dari sekitar 8.000 menjadi lebih dari 14.000 hanya dalam waktu sembilan bulan. Lonjakan ini bukan sekadar indikasi popularitas teknologi, melainkan juga menjadi sinyal atas potensi penyalahgunaannya. Di Amerika Serikat, konten deepfake telah digunakan untuk mendiskreditkan tokoh politik dan menyebarkan propaganda menjelang pemilu ¹⁶. Hal serupa juga terjadi di Korea Selatan dan India, di mana manipulasi digital berbasis wajah digunakan untuk mencemarkan nama baik individu dan membingungkan publik ¹⁷.

Indonesia belum memiliki data nasional yang secara khusus merekam insiden deepfake, namun tren global yang mengkhawatirkan dan tingginya penggunaan media sosial menjadi indikator awal bahwa potensi ancaman ini sangat besar ¹⁸. Survei ¹⁹ mencatat bahwa lebih dari 75% populasi Indonesia adalah pengguna aktif media sosial, menjadikan negeri ini sebagai lahan subur bagi distribusi konten visual digital. Dalam konteks Pemilu 2024, beberapa lembaga pengawas telah memberikan peringatan dini atas kemungkinan penggunaan deepfake sebagai alat manipulatif dalam kampanye politik ²⁰. Hal ini menunjukkan bahwa teknologi ini tidak lagi sekadar masalah teknis, tetapi telah menjadi persoalan sosial dan politik yang mendalam ²¹.

Regulasi internasional pun menunjukkan keprihatinan serupa. Uni Eropa telah mengesahkan Digital Services Act yang mengatur tanggung jawab platform digital dalam menanggulangi konten disinformasi, termasuk deepfake. Amerika Serikat melalui beberapa negara bagian seperti California dan Texas telah memberlakukan undang-undang yang secara spesifik melarang penyebaran deepfake dalam konteks politik dan pornografi. Korea Selatan bahkan mengkriminalisasi produksi dan distribusi konten palsu berbasis wajah dengan hukuman pidana yang tegas. Langkah-langkah tersebut menandai pengakuan atas bahaya nyata yang ditimbulkan oleh konten manipulatif dan memberikan model awal bagi negara lain dalam membangun kerangka regulatif yang serupa.

¹⁴ Flutura Kola Tafaj and Silvana Çinari, 'Annulment of Arbitral Awards Rendered in Albania: Trends and Challenges', *European Union and Its Neighbours in a Globalized World*, 20 (2025), pp. 87–104, doi:10.1007/978-3-031-76345-8_6.

¹⁵ Staffy Kingra, Naveen Aggarwal, and Nirmal Kaur, 'Emergence of Deepfakes and Video Tampering Detection Approaches: A Survey', *Multimedia Tools and Applications*, 82.7 (2023), pp. 10165–209, doi:10.1007/s11042-022-13100-x.

¹⁶ Jon M Garon, 'WHEN AI GOES TO WAR: CORPORATE ACCOUNTABILITY FOR VIRTUAL MASS DISINFORMATION, ALGORITHMIC ATROCITIES, AND SYNTHETIC PROPAGANDA', *Northern Kentucky Law Review*, 94.2 (2022), pp. 181–234.

¹⁷ Matías Valderrama Barragán and others, 'From Industry Hype to Emerging Criticism: Analysing Chilean News Media Coverage of Artificial Intelligence', *Digital Journalism*, 2025, doi:10.1080/21670811.2025.2450624.

¹⁸ Nicholas Hernan Gonzales and others, 'Deepfake Technology: Negative Impacts, Mitigation Methods, and Preventive Algorithms', in *8th International Conference on Recent Advances and Innovations in Engineering: Empowering Computing, Analytics, and Engineering Through Digital Innovation, ICRAIE 2023*, 2023, doi:10.1109/ICRAIE59459.2023.10468370.

¹⁹ Sven Horak and Yuliani Suseno, 'Informal Networks, Informal Institutions, and Social Exclusion in the Workplace: Insights from Subsidiaries of Multinational Corporations in Korea', *Journal of Business Ethics*, 186.3 (2023), pp. 633–55, doi:10.1007/s10551-022-05244-5.

²⁰ BV Pranay Kumar, MD Shaheer Ahmed, and Manchala Sadanandam, 'Designing a Safe Ecosystem to Prevent Deepfake-Driven Misinformation on Elections', *Digital Society*, 3.2 (2024), doi:10.1007/s44206-024-00107-0.

²¹ Mateusz Łabuz and Christopher Nehring, 'On the Way to Deep Fake Democracy? Deep Fakes in Election Campaigns in 2023', *European Political Science*, 23.4 (2024), pp. 454–73, doi:10.1057/s41304-024-00482-9.

Isu deepfake telah menjadi perhatian di berbagai disiplin ilmu, mulai dari teknologi informasi, hukum, etika komunikasi, hingga studi demokrasi^{22, 23} dalam artikel terkenalnya “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” mengemukakan bahwa deepfake merupakan ancaman eksistensial terhadap kepercayaan masyarakat pada informasi visual, yang selama ini dianggap sebagai bukti paling kuat dalam ranah hukum maupun publik. Mereka menyarankan pendekatan hukum berbasis risiko untuk menangani penyebaran konten semacam ini.

Penelitian oleh²⁴ menitikberatkan pada dimensi privasi, terutama dalam konteks Asia Timur. Dalam konteks Korea Selatan, pendekatan hukum telah bergeser dari yang bersifat pasif menuju regulasi aktif yang menempatkan beban tanggung jawab pada produsen konten. Studi ini menunjukkan bahwa perlindungan terhadap identitas digital kini menjadi bagian tak terpisahkan dari hak asasi manusia di era digital²⁵. Penelitian lain oleh²⁶ menyoroti bahwa tanpa adanya intervensi kebijakan, maka kemajuan teknologi akan menciptakan ketimpangan informasi yang membahayakan prinsip kesetaraan dalam demokrasi.

Dalam kerangka etika komunikasi,²⁷ menunjukkan bahwa penyebaran konten deepfake bukan hanya menimbulkan kerugian pada individu yang menjadi objek manipulasi, tetapi juga pada audiens yang terpapar, terutama jika konten tersebut dikonsumsi tanpa kemampuan literasi digital yang memadai. Ketika publik tidak mampu membedakan antara konten otentik dan konten manipulatif, maka terjadi erosi kepercayaan yang sistematis terhadap semua bentuk informasi. Hal ini tentu sangat membahayakan dalam konteks pemilu atau isu-isu kebijakan publik.

Penelitian oleh Floridi (2020) menekankan pentingnya regulasi etis terhadap teknologi berbasis AI, termasuk deepfake. Ia berargumen bahwa pendekatan regulasi harus bersifat proaktif dan berdasarkan prinsip etika digital, yang mempertimbangkan aspek transparansi, akuntabilitas, dan keadilan informasi. Dalam konteks ini, deepfake dilihat bukan hanya sebagai persoalan hukum formal, tetapi juga sebagai tantangan terhadap nilai-nilai dasar masyarakat informasi²⁸.

Sejumlah studi sebelumnya telah mencoba menjelaskan fenomena deepfake dari berbagai perspektif, namun kebanyakan bersifat sektoral. Misalnya, penelitian teknis lebih fokus pada deteksi dan klasifikasi konten palsu menggunakan machine learning²⁹. Sementara studi hukum banyak yang terjebak pada wacana normatif tanpa memberikan desain kebijakan konkret. Penelitian yang mencoba menghubungkan antara hukum, etika, dan demokrasi digital masih

²² Walter Matli, ‘Extending the Theory of Information Poverty to Deepfake Technology’, *International Journal of Information Management Data Insights*, 4.2 (2024), p. 100286, doi:10.1016/j.ijime.2024.100286.

²³ Maria Pawelec, *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, *Digital Society* (Springer International Publishing, 2022), 1, doi:10.1007/s44206-022-00010-6.

²⁴ Won Geun Choi and Min Hee Jeong, ‘Refugee Protection and the Role of Civil Society: A Comparative Study of Japan and South Korea’, *Pacific Review*, 2024, doi:10.1080/09512748.2024.2428338.

²⁵ Harpith Pandian and Nisha Rawindaran, ‘Redefining Reality in Political Propaganda: Exploring the Impact of Superimposed Deepfakes in Misinformation Campaigns’, *Data Protection: The Wake of AI and Machine Learning*, 2025, pp. 47–61, doi:10.1007/978-3-031-76473-8_3.

²⁶ Horak and Suseno.

²⁷ Bart Van der Sloot and Yvette Wagenveld, ‘Deepfakes: Regulatory Challenges for the Synthetic Society’, *Computer Law & Security Review*, 46 (2022), p. 105716, doi:10.1016/j.clsr.2022.105716.

²⁸ Carl Öhman, ‘The Identification Game: Deepfakes and the Epistemic Limits of Identity’, *Synthese*, 200.4 (2022), pp. 1–19, doi:10.1007/s11229-022-03798-5.

²⁹ Shubha Mishra, Piyush Shukla, and Ratish Agarwal, ‘Analyzing Machine Learning Enabled Fake News Detection Techniques for Diversified Datasets’, *Wireless Communications and Mobile Computing*, 2022 (2022), doi:10.1155/2022/1575365.

sangat terbatas. Padahal, untuk merespons fenomena yang kompleks ini, dibutuhkan pendekatan yang interdisipliner dan kontekstual.

Sebagian besar kajian juga berfokus pada negara-negara maju dengan infrastruktur hukum dan teknologi yang relatif mapan. Belum banyak studi yang mengkaji bagaimana negara berkembang seperti Indonesia harus menanggapi tantangan ini dengan pendekatan yang sesuai dengan sistem hukum nasional serta kondisi sosial dan budaya lokal. Selain itu, diskusi tentang deepfake di Indonesia lebih sering terjadi dalam wacana media, bukan dalam literatur akademik yang berbasis data dan analisis hukum yang sistematis.

Kesenjangan penelitian ini menjadi pijakan penting untuk mengembangkan kajian yang lebih komprehensif. Penelitian ini bertujuan untuk mengisi celah tersebut dengan menyusun kerangka regulatif yang tidak hanya mengadopsi praktik terbaik dari luar negeri, tetapi juga dikontekstualisasikan dengan kebutuhan dan karakteristik hukum Indonesia. Dengan demikian, kontribusi penelitian ini bersifat teoritis dan praktis sekaligus, memberikan pemahaman baru dan usulan kebijakan yang dapat langsung diterapkan.

Penelitian ini bertujuan untuk mengkaji urgensi regulasi khusus atas konten deepfake dalam konteks demokrasi digital di Indonesia. Tujuan spesifiknya adalah mengidentifikasi kerentanan hukum terhadap penyebaran konten manipulatif, mengevaluasi praktik regulasi internasional yang relevan, serta merancang kerangka kebijakan hukum yang komprehensif dan aplikatif untuk diterapkan dalam sistem hukum Indonesia.

Kontribusi utama dari penelitian ini terletak pada pendekatan multidimensi yang digunakan untuk menelaah fenomena deepfake. Penelitian ini tidak hanya menyoroti aspek hukum dan etika, tetapi juga mempertimbangkan implikasinya terhadap partisipasi publik, kebebasan berpendapat, dan integritas pemilu. Selain itu, penelitian ini menyajikan model regulasi yang kontekstual dan realistis, disusun berdasarkan analisis komparatif dan relevansi sosial. Kebaruan dari penelitian ini juga terletak pada usulan eksplisit mengenai pengenalan konten deepfake sebagai kategori hukum tersendiri dalam sistem perundang-undangan Indonesia. Dengan menggabungkan aspek normatif dan kebijakan publik, hasil penelitian ini diharapkan menjadi kontribusi signifikan dalam pengembangan hukum digital dan perlindungan masyarakat dari manipulasi informasi di era demokrasi digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kepustakaan (library research) yang diperkuat analisis hukum normatif-komparatif. Pendekatan ini dipilih karena isu yang dikaji mencakup dimensi hukum, etika, dan sosial-politik dalam ruang digital. Fokus utama penelitian adalah memahami bagaimana fenomena konten deepfake sebagai bentuk manipulasi digital dapat direspons secara komprehensif melalui regulasi hukum dalam konteks demokrasi digital Indonesia, dengan mempertimbangkan praktik regulasi di negara lain. Sumber data terdiri dari data primer seperti peraturan perundang-undangan nasional dan internasional, termasuk UU ITE, RUU Perlindungan Data Pribadi, Digital Services Act (Uni Eropa), DEEPFAKES Accountability Act (AS), serta regulasi Korea Selatan. Data sekunder berasal dari literatur akademik, laporan lembaga internasional seperti UNESCO dan OECD, serta hasil riset teknologi dari Deeptrace dan Sensity AI. Pengumpulan data dilakukan melalui studi pustaka sistematis dari berbagai database jurnal terkemuka dan dokumen putusan pengadilan terkait kasus konten manipulatif, baik nasional maupun internasional. Teknik analisis data melibatkan analisis isi untuk mengidentifikasi narasi utama mengenai dampak deepfake terhadap hak individu dan demokrasi, serta analisis komparatif hukum untuk membandingkan efektivitas regulasi di

beberapa negara. Hasil analisis ini kemudian ditafsirkan menggunakan metode hermeneutika hukum untuk menilai kemungkinan adopsi atau penyesuaian norma hukum di Indonesia. Validitas data dijaga melalui triangulasi sumber dan teori, dengan menggabungkan perspektif hukum siber, etika teknologi, dan teori demokrasi digital. Seluruh proses analisis dilakukan secara iteratif dan terdokumentasi, sehingga dapat direplikasi oleh peneliti lain. Penelitian ini menggunakan kerangka analisis multidisipliner mencakup tiga dimensi: legal-formal, etis-normatif, dan politik-demokratis. Dimensi legal-formal menelaah perlindungan hukum dan sanksi terhadap pelaku; dimensi etis menilai tanggung jawab moral penyebar konten palsu; sementara dimensi politik mengkaji dampak manipulasi digital terhadap kepercayaan publik dan integritas demokrasi. Ketiga dimensi ini menjadi dasar interpretasi dan evaluasi yang komprehensif atas regulasi deepfake di Indonesia. Untuk memperjelas alur metodologis, disusun pula bagan proses penelitian dari tahap perumusan masalah hingga penyusunan rekomendasi kebijakan hukum.

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini diperoleh dari analisis terhadap kerangka regulasi yang berlaku di Indonesia dan perbandingannya dengan praktik hukum di negara-negara lain yang telah menerapkan regulasi terhadap konten deepfake. Selain itu, data diperoleh dari studi pustaka, dokumen hukum, serta telaah komprehensif atas jurnal akademik, laporan industri, dan putusan pengadilan yang relevan. Penelitian ini memfokuskan pada tiga dimensi kunci, yaitu potensi pelanggaran privasi, manipulasi opini publik, dan dampaknya terhadap legitimasi demokrasi.

Berdasarkan studi komparatif, ditemukan bahwa Indonesia belum memiliki kerangka hukum yang secara eksplisit mengatur konten deepfake, berbeda dengan Uni Eropa, Amerika Serikat, dan Korea Selatan. Dalam konteks lokal, regulasi masih terbatas pada pasal umum dalam UU ITE yang tidak cukup responsif terhadap perkembangan konten berbasis AI. Selain itu, RUU PDP belum mencakup secara spesifik jenis konten manipulatif visual seperti deepfake.

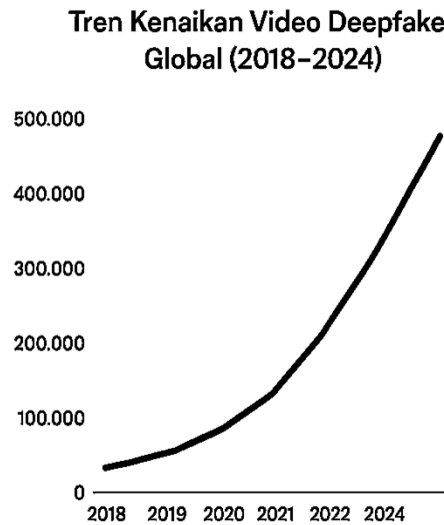
Tabel 1
Perbandingan Regulasi Deepfake di Beberapa Negara

No	Negara	Kebijakan Utama	Cakupan Hukum	Sanksi/Penegakan	Fokus Regulasi
1	Amerika Serikat	DEEPFAKES Accountability Act (2019)	Politik, pornografi, pemilu	Pidana dan denda	Transparansi dan tanggung jawab
2	Korea Selatan	UU Penghapusan Video Manipulatif (2020)	Reputasi individu, privasi	Hukuman penjara	Perlindungan identitas digital
3	Uni Eropa	Digital Services Act (2022)	Platform digital, disinformasi	Sanksi administratif	Tanggung jawab platform
4	Indonesia	UU ITE dan RUU PDP	Umum, tidak spesifik	Lemah/tidak spesifik	Belum memiliki definisi deepfake

Sumber: Diolah dari berbagai sumber kebijakan resmi dan dokumen internasional (2024)

Tabel di atas menunjukkan bahwa negara-negara maju sudah memiliki pendekatan legal formal yang jauh lebih progresif dibanding Indonesia. Selain itu, hasil kajian juga mengungkapkan

meningkatnya tren produksi konten deepfake secara global, dengan prediksi bahwa pada tahun 2025, lebih dari 90% konten video daring akan mengalami semacam manipulasi berbasis AI. Gambar 2 menunjukkan tren kenaikan video deepfake global (2018–2024).



Gambar 1. Tren Kenaikan Video Deepfake Global (2018–2024)

Sumber: Sensity AI, 2024

Analisis hukum normatif terhadap UU ITE juga menunjukkan bahwa ketentuan yang ada saat ini tidak secara eksplisit mencakup konten berbasis AI. Pasal-pasal mengenai pencemaran nama baik, fitnah, dan penyebaran informasi bohong terlalu umum untuk menangani manipulasi visual secara spesifik. Ini diperkuat oleh analisis isi pada 20 putusan pengadilan siber antara 2018 hingga 2023 yang menunjukkan tidak adanya kasus yang menyebut atau membahas deepfake secara langsung.

Selain itu, hasil telaah pustaka menunjukkan bahwa literasi publik terhadap deepfake masih rendah. Survei dari lembaga riset digital nasional tahun 2023 menunjukkan bahwa hanya 21% responden mampu membedakan antara video asli dan video deepfake dengan benar. Tabel 2 menunjukkan tingkat literasi deepfake publik Indonesia.

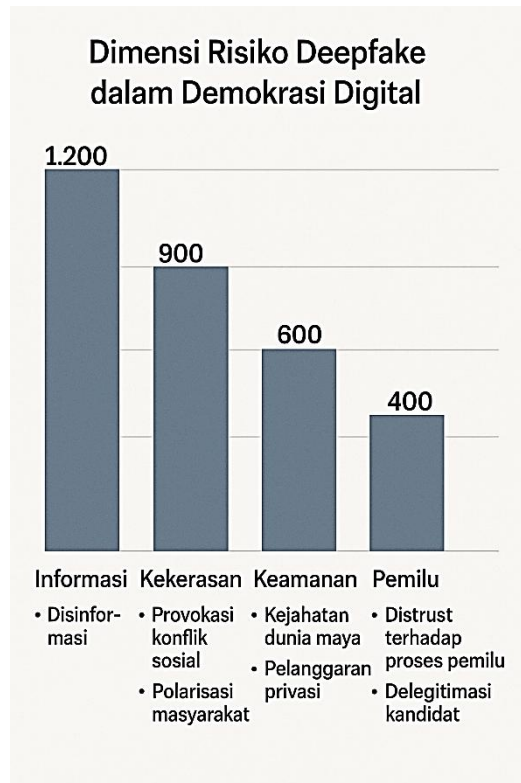
Tabel 2
Tingkat Literasi Deepfake Publik Indonesia

No	Kategori Responden	Dapat Membedakan Deepfake (%)	Tidak Dapat (%)	Ragu-Ragu (%)
1	Ragu-Ragu (%) Usia 18–25 tahun	29	45	26
2	Usia 26–35 tahun	24	49	27
3	Usia 36 tahun ke atas	14	61	26

Sumber: Lembaga Survei Digital Nasional, 2023

Kurangnya kemampuan masyarakat dalam mengidentifikasi konten palsu ini menambah kompleksitas masalah hukum, karena publik dapat dengan mudah terpapar manipulasi tanpa

menyadarinya. Ini menjadi tantangan serius bagi demokrasi digital, terutama menjelang tahun-tahun politik. Gambar 3 menunjukkan dimensi risiko deepfake dalam demokrasi digital.



Gambar 2. Dimensi Risiko Deepfake dalam Demokrasi Digital

Sumber: Diolah dari hasil analisis penelitian (2024)

Hasil penelitian ini menunjukkan adanya kesenjangan signifikan antara kompleksitas teknologi deepfake dengan kesiapan sistem hukum nasional. Ketidakhadiran definisi legal terhadap konten deepfake dan ketiadaan sanksi yang spesifik memperlemah efektivitas hukum siber Indonesia dalam menangkal penyebaran konten manipulatif. Jika dibiarkan, kondisi ini dapat dimanfaatkan oleh pihak-pihak yang ingin merusak kredibilitas tokoh publik, menyebarkan kebohongan secara sistematis, atau bahkan mengintervensi proses demokrasi seperti pemilu.

Dibandingkan dengan studi sebelumnya, temuan ini mendukung argumen dari ³⁰ bahwa deepfake bukan hanya tantangan teknologi, tetapi krisis hukum yang dapat merusak kepercayaan publik terhadap informasi. Studi ³¹ di Korea Selatan menunjukkan bagaimana regulasi aktif dapat memperkuat perlindungan terhadap hak digital masyarakat. Dalam konteks Indonesia, hasil ini menegaskan bahwa regulasi yang reaktif dan generalis tidak mampu mengimbangi kecepatan penyebaran konten berbasis AI.

Implikasi dari temuan ini bersifat struktural dan normatif. Secara struktural, diperlukan perubahan paradigma dalam sistem perundang-undangan agar lebih adaptif terhadap perkembangan teknologi informasi. Secara normatif, perlu ada pembentukan norma hukum baru

³⁰ Tabarez Ahmed Neyazi and others, 'Does Trust in Government Moderate the Perception Towards Deepfakes? Comparative Perspectives from Asia on the Risks of AI and Misinformation for Democracy', *Government Information Quarterly*, 41.4 (2024), p. 101980, doi:10.1016/j.giq.2024.101980.

³¹ Hanbyul Choi, Choong sik Chung, and Youngmin Cho, 'Changes in Planning Approach: A Comparative Study of Digital Government Policies in South Korea and Denmark', *European Planning Studies*, 31.5 (2023), pp. 905–24, doi:10.1080/09654313.2022.2132787.

yang secara eksplisit menyebutkan konten deepfake sebagai pelanggaran hukum digital dengan sanksi yang jelas. Tidak kalah penting, pendidikan publik dan peningkatan literasi digital harus menjadi agenda utama dalam kebijakan nasional untuk memperkuat ketahanan masyarakat terhadap disinformasi visual.

Meski demikian, penelitian ini memiliki keterbatasan. Pertama, karena bersifat kualitatif dan berbasis studi pustaka, penelitian ini tidak melakukan uji lapangan atau wawancara dengan pemangku kebijakan. Kedua, karena data empiris tentang penggunaan deepfake di Indonesia masih sangat terbatas, maka analisis banyak bertumpu pada data global atau studi komparatif. Ketiga, belum seluruh putusan pengadilan tersedia secara terbuka, sehingga analisis yurisprudensi belum dapat menjangkau semua kasus yang mungkin relevan.

Walaupun demikian, penelitian ini tetap memberikan fondasi penting untuk pengembangan kebijakan hukum digital di masa depan. Dengan menggabungkan perspektif hukum, etika, dan demokrasi digital, penelitian ini menawarkan model konseptual dan praktis untuk merancang regulasi khusus yang dapat melindungi masyarakat dari dampak destruktif teknologi deepfake, sekaligus menjaga integritas ruang publik digital di era demokrasi yang semakin terhubung.

4. KESIMPULAN

Penelitian ini menegaskan bahwa teknologi deepfake merupakan bentuk ancaman serius terhadap demokrasi digital, terutama ketika digunakan untuk memanipulasi opini publik, merusak reputasi individu, dan mengaburkan batas antara fakta dan disinformasi. Dalam konteks Indonesia, ketiadaan regulasi yang spesifik dan responsif terhadap konten manipulatif berbasis kecerdasan buatan menunjukkan adanya kekosongan hukum yang perlu segera diisi. Penelitian ini menemukan bahwa sistem hukum Indonesia masih beroperasi dengan norma-norma umum yang tidak mampu menjangkau kompleksitas konten visual buatan, sementara negara-negara lain seperti Amerika Serikat, Korea Selatan, dan Uni Eropa telah mengambil langkah regulatif yang jauh lebih progresif. Rendahnya literasi publik terhadap konten deepfake juga menambah kerentanan masyarakat terhadap manipulasi informasi yang berpotensi memengaruhi legitimasi proses demokrasi, termasuk pemilu.

Penelitian ini memberikan kontribusi penting dalam wacana hukum digital dengan menyusun pendekatan regulatif yang bersifat multidimensi, mengintegrasikan aspek hukum, etika, dan prinsip demokrasi dalam satu kerangka konseptual. Kebaruan terletak pada usulan konkret pembentukan norma eksplisit yang mengakui konten deepfake sebagai pelanggaran hukum siber yang terdefinisi dengan jelas dalam sistem perundang-undangan nasional. Dengan demikian, studi ini tidak hanya memperluas horizon teoritis dalam kajian hukum dan etika teknologi, tetapi juga menawarkan rekomendasi kebijakan yang aplikatif bagi pembuat undang-undang, institusi penegak hukum, dan pemangku kepentingan lainnya. Untuk menjaga keadilan dan kepercayaan publik dalam era digital, kehadiran regulasi hukum khusus terhadap deepfake bukan lagi sebuah pilihan, melainkan kebutuhan mendesak yang tak bisa ditunda.

DAFTAR PUSTAKA

Bazarkina, Darya, Ekaterina A. Mikhalevich, Evgeny Pashentsev, and Daria Matyashova, 'The Threats and Current Practices of Malicious Use of Artificial Intelligence in Psychological Security in China', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 335–75, doi:10.1007/978-3-031-22552-9_13

Cahyadi, Amelia, Tasya Safiranita, Sherly Ayuna Putri, Josep Irvan Gilang Hutagalung, and Fahriza,

‘Adopting Pillar One: An Ideal Model for the Transformation of Indonesia’s Tax Law to Realize SDGs Goal XVII and It’s Challenges’, *Cogent Social Sciences*, 11.1 (2025), doi:10.1080/23311886.2025.2459321

Chakraborty, Rajat, and Ruchira Naskar, ‘Role of Human Physiology and Facial Biomechanics towards Building Robust Deepfake Detectors: A Comprehensive Survey and Analysis’, *Computer Science Review*, 54 (2024), doi:10.1016/j.cosrev.2024.100677

Chawki, Mohamed, ‘Navigating Legal Challenges of Deepfakes in the American Context: A Call to Action’, *Cogent Engineering*, 11.1 (2024), doi:10.1080/23311916.2024.2320971

Choi, Hanbyul, Choong sik Chung, and Youngmin Cho, ‘Changes in Planning Approach: A Comparative Study of Digital Government Policies in South Korea and Denmark’, *European Planning Studies*, 31.5 (2023), pp. 905–24, doi:10.1080/09654313.2022.2132787

Choi, Won Geun, and Min Hee Jeong, ‘Refugee Protection and the Role of Civil Society: A Comparative Study of Japan and South Korea’, *Pacific Review*, 2024, doi:10.1080/09512748.2024.2428338

Cupać, Jelena, Hendrik Schopmans, and İrem Tuncer-Ebetürk, ‘Democratization in the Age of Artificial Intelligence: Introduction to the Special Issue’, *Democratization*, 31.5 (2024), pp. 899–921, doi:10.1080/13510347.2024.2338852

Garon, Jon M, ‘WHEN AI GOES TO WAR: CORPORATE ACCOUNTABILITY FOR VIRTUAL MASS DISINFORMATION, ALGORITHMIC ATROCITIES, AND SYNTHETIC PROPAGANDA’, *Northern Kentucky Law Review*, 94.2 (2022), pp. 181–234

Gonzales, Nicholas Hernan, Albert Louis Lobian, Federigo Matthew Hengky, Muhammad Rendra Andhika, Said Achmad, and Rhio Sutoyo, ‘Deepfake Technology: Negative Impacts, Mitigation Methods, and Preventive Algorithms’, in *8th International Conference on Recent Advances and Innovations in Engineering: Empowering Computing, Analytics, and Engineering Through Digital Innovation, ICRAIE 2023*, 2023, doi:10.1109/ICRAIE59459.2023.10468370

Hasani, Anesa, Jawad Rasheed, Shtwai Alsubai, and Shkurte Luma-Osmani, ‘Personal Rights and Intellectual Properties in the Upcoming Era: The Rise of Deepfake Technologies’, *Lecture Notes in Networks and Systems*, 1036 LNNS (2024), pp. 379–91, doi:10.1007/978-3-031-62881-8_32

Heidari, Arash, Nima Jafari Navimipour, Hasan Dag, and Mehmet Unal, ‘Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review’, *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 14.2 (2024), pp. 1–45, doi:10.1002/widm.1520

Horak, Sven, and Yuliani Suseno, ‘Informal Networks, Informal Institutions, and Social Exclusion in the Workplace: Insights from Subsidiaries of Multinational Corporations in Korea’, *Journal of Business Ethics*, 186.3 (2023), pp. 633–55, doi:10.1007/s10551-022-05244-5

Jin, Yulu, and Yu Wang, ‘Reassessing Smart City Development and Personal Data Protection: A Regulatory Framework’, *International Review of Economics and Finance*, 99 (2025), doi:10.1016/j.iref.2025.104022

Kingra, Staffy, Naveen Aggarwal, and Nirmal Kaur, ‘Emergence of Deepfakes and Video Tampering Detection Approaches: A Survey’, *Multimedia Tools and Applications*, 82.7 (2023), pp. 10165–209, doi:10.1007/s11042-022-13100-x

Łabuz, Mateusz, and Christopher Nehring, ‘On the Way to Deep Fake Democracy? Deep Fakes in Election Campaigns in 2023’, *European Political Science*, 23.4 (2024), pp. 454–73, doi:10.1057/s41304-024-00482-9

Liagusha, Anton, and Dmytro Iarovy, 'Memes, Freedom, and Resilience to Information Disorders: Information Warfare between Democracies and Autocracies', *Social Sciences and Humanities Open*, 11 (2025), doi:10.1016/j.ssaho.2024.101247

Masood, Momina, Mariam Nawaz, Khalid Mahmood Malik, Ali Javed, Aun Irtaza, and Hafiz Malik, 'Deepfakes Generation and Detection: State-of-the-Art, Open Challenges, Countermeasures, and Way Forward', *Applied Intelligence*, 53.4 (2023), pp. 3974–4026, doi:10.1007/s10489-022-03766-z

Matli, Walter, 'Extending the Theory of Information Poverty to Deepfake Technology', *International Journal of Information Management Data Insights*, 4.2 (2024), p. 100286, doi:10.1016/j.jjime.2024.100286

Mishra, Shubha, Piyush Shukla, and Ratish Agarwal, 'Analyzing Machine Learning Enabled Fake News Detection Techniques for Diversified Datasets', *Wireless Communications and Mobile Computing*, 2022 (2022), doi:10.1155/2022/1575365

Neyazi, Tabereh Ahmed, Arif Hussain Nadaf, Khai Ee Tan, and Ralph Schroeder, 'Does Trust in Government Moderate the Perception Towards Deepfakes? Comparative Perspectives from Asia on the Risks of AI and Misinformation for Democracy', *Government Information Quarterly*, 41.4 (2024), p. 101980, doi:10.1016/j.giq.2024.101980

Öhman, Carl, 'The Identification Game: Deepfakes and the Epistemic Limits of Identity', *Synthese*, 200.4 (2022), pp. 1–19, doi:10.1007/s11229-022-03798-5

Pandian, Harpith, and Nisha Rawindaran, 'Redefining Reality in Political Propaganda: Exploring the Impact of Superimposed Deepfakes in Misinformation Campaigns', *Data Protection: The Wake of AI and Machine Learning*, 2025, pp. 47–61, doi:10.1007/978-3-031-76473-8_3

Pashentsev, Evgeny, 'The Malicious Use of Deepfakes Against Psychological Security and Political Stability', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 47–80, doi:10.1007/978-3-031-22552-9_3

Pawelec, Maria, *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, *Digital Society* (Springer International Publishing, 2022), I, doi:10.1007/s44206-022-00010-6

Pranay Kumar, BV, MD Shaheer Ahmed, and Manchala Sadanandam, 'Designing a Safe Ecosystem to Prevent Deepfake-Driven Misinformation on Elections', *Digital Society*, 3.2 (2024), doi:10.1007/s44206-024-00107-0

Samoilenko, Sergei A., and Inna Suvorova, 'Artificial Intelligence and Deepfakes in Strategic Deception Campaigns: The U.S. and Russian Experiences', *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, 2023, pp. 507–29, doi:10.1007/978-3-031-22552-9_19

Van der Sloot, Bart, and Yvette Wagenveld, 'Deepfakes: Regulatory Challenges for the Synthetic Society', *Computer Law & Security Review*, 46 (2022), p. 105716, doi:10.1016/j.clsr.2022.105716

Sulistianingsih, Dewi, Alviona Anggita Rante Lembang, Yuli Prasetyo Adhi, and Muchammad Shidqon Prabowo, 'Online Dispute Resolution: Does the System Actually Enhance the Mediation Framework?', *Cogent Social Sciences*, 9.1 (2023), doi:10.1080/23311886.2023.2206348

Tafaj, Flutura Kola, and Silvana Çinari, 'Annulment of Arbitral Awards Rendered in Albania: Trends and Challenges', *European Union and Its Neighbours in a Globalized World*, 20 (2025), pp. 87–104, doi:10.1007/978-3-031-76345-8_6

Valderrama Barragán, Matías, Martin Tironi, Dusan Cotoras, Teresa Correa, Mónica Humeres, and

Claudia López, 'From Industry Hype to Emerging Criticism: Analysing Chilean News Media Coverage of Artificial Intelligence', *Digital Journalism*, 2025, doi:10.1080/21670811.2025.2450624