

TINJAUAN ETIS DAN HUKUM TERHADAP PERLINDUNGAN DATA PRIBADI DI
TENGAH MARAKNYA KONTEN DEEPPAKE DI MEDIA SOSIAL

Anita Firdausi¹, Fauzan Nur Abadi², Tiara Yogi Dwi Amelia³, Triana⁴

Email: 240413004@mhs.udb.ac.id, 240413012@mhs.udb.ac.id,
240413026@mhs.udb.ac.id, triana@udb.ac.id

Universitas Duta Bangsa Surakarta

Abstrack

This research examines the ethical and legal implications of personal data protection amid the rise of deepfake content on social media platforms. Using a normative juridical method and qualitative descriptive approach, the study analyzes Indonesia’s legal framework, particularly the Personal Data Protection Law (UU PDP) and its alignment with international regulations such as the GDPR. The findings reveal significant regulatory gaps, ethical challenges related to autonomy and justice, and a lack of proactive platform accountability. This paper recommends legal reform, public digital literacy enhancement, and ethical audits for AI systems to ensure comprehensive data protection in the digital era.

Keywords: Deepfake, Personal Data Protection, Ethics, Artificial Intelligence, Legal Framework Abstrak

Abstrak

Article History

Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025

Copyright : Author
Publish by : CAUSA



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

¹ 240413004, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta
² 240413012, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta
³ 240413026, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta

Penelitian ini mengkaji implikasi etis dan hukum terkait perlindungan data pribadi di tengah maraknya konten deepfake di media sosial. Menggunakan metode yuridis normatif dengan pendekatan deskriptif kualitatif, studi ini menganalisis kerangka hukum Indonesia, khususnya Undang-Undang Perlindungan Data Pribadi (UU PDP), serta kesesuaiannya dengan regulasi internasional seperti GDPR. Hasil penelitian menunjukkan adanya kekosongan regulasi, tantangan etika terkait otonomi dan keadilan, serta minimnya akuntabilitas proaktif dari platform digital. Artikel ini merekomendasikan reformasi hukum, peningkatan literasi digital publik, dan audit etis terhadap sistem AI untuk memastikan perlindungan data yang komprehensif di era digital. Kata kunci: Deepfake, Perlindungan Data Pribadi, Etika, Kecerdasan Buatan, Kerangka Hukum	
---	--

PENDAHULUAN

Perkembangan teknologi digital yang pesat telah membawa dampak signifikan dalam berbagai aspek kehidupan, mulai dari sektor ekonomi, sosial, hingga ranah hukum. Salah satu kemajuan teknologi yang paling mencolok dalam dekade terakhir adalah kemunculan kecerdasan buatan (Artificial Intelligence/AI) yang tidak hanya mengubah cara manusia berinteraksi dengan teknologi, tetapi juga menghadirkan tantangan baru terhadap nilai-nilai dasar seperti privasi, otonomi, dan keadilan. Di antara inovasi AI yang paling kontroversial adalah deepfake, yakni teknologi yang memanipulasi visual dan suara manusia secara realistis menggunakan teknik *deep learning*. Teknologi ini memungkinkan seseorang menciptakan video atau audio yang seolah-olah berasal dari individu lain, padahal sepenuhnya rekayasa digital (Kietzmann et al., 2020). Meskipun pada awalnya deepfake dikembangkan untuk kepentingan hiburan dan sinema, dalam praktiknya teknologi ini telah digunakan secara luas dalam bentuk yang merugikan. Penyebaran konten deepfake mencakup pencemaran nama baik, pornografi non-konsensual, penipuan identitas, manipulasi politik, hingga disinformasi massal (Chesney, 2020). Fakta menunjukkan bahwa mayoritas korban konten deepfake adalah perempuan, terutama tokoh publik, selebritas, dan aktivis (Paris, 2019). Hal ini menimbulkan kekhawatiran yang semakin besar terhadap lemahnya regulasi perlindungan data pribadi, terutama data biometrik seperti wajah dan suara, yang menjadi bahan utama dalam pembuatan deepfake.

Di Indonesia, isu ini semakin relevan pasca disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini merupakan upaya legislasi pertama yang secara komprehensif mengatur perlindungan data pribadi warga negara. Meskipun demikian, masih terdapat sejumlah tantangan dalam implementasinya. Salah satu di antaranya adalah belum adanya peraturan pelaksana yang secara khusus mengatur penyalahgunaan data biometrik dalam konteks teknologi deepfake. Di sisi lain, pendekatan hukum pidana melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) juga belum mampu menjangkau kompleksitas pelanggaran yang terjadi karena sifat teknologi deepfake yang sangat teknis dan bersifat lintas yurisdiksi (Effendy, 2022);(Maulana, 2023)

Masalah ini tidak hanya berhenti pada aspek hukum positif, tetapi juga menyentuh wilayah etika teknologi. Penggunaan citra dan suara seseorang tanpa izin menimbulkan persoalan moral yang serius. Hal ini melanggar prinsip autonomy, yakni hak individu untuk mengontrol representasi diri mereka di ruang publik digital (Floridi, 2013). Dalam konteks keadilan, deepfake memperdalam ketimpangan informasi (epistemic asymmetry) antara pembuat konten dan konsumen informasi, sebagaimana diuraikan oleh (Campolo et al., 2017). Ketimpangan ini menciptakan situasi di mana publik kesulitan membedakan kebenaran dan rekayasa, sehingga menurunkan kualitas demokrasi digital dan kepercayaan sosial. Tanggung

jawab besar juga berada di tangan platform digital seperti TikTok, YouTube, Meta, dan Instagram. Sayangnya, hingga saat ini belum terdapat sistem deteksi otomatis yang efektif untuk menangani konten deepfake secara preventif. Mayoritas platform masih mengandalkan pelaporan manual dari pengguna, yang tentu saja tidak cukup responsif (Gillespie, 2018) Berbeda dengan Digital Services Act (DSA) dari Uni Eropa yang mewajibkan platform untuk melakukan penilaian risiko dan audit algoritmik secara berkala, Indonesia belum memiliki ketentuan serupa. Hal ini menunjukkan perlunya tata kelola digital yang lebih ketat dan kolaboratif antara negara, masyarakat, dan perusahaan teknologi (Jong & O'Neill, 2023).

Tujuan dari penelitian ini adalah untuk menganalisis sistem hukum nasional Indonesia dalam menanggapi penyebaran deepfake yang melibatkan penggunaan dan penyalahgunaan data pribadi orang lain tanpa persetujuan, dengan kemungkinan potensi pelanggaran hak atas privasi dan integritas digital. Selain itu, penelitian ini juga menjelaskan secara panjang lebar etika yang perlu diperhatikan yang timbul dari penyalahgunaan teknologi deepfake yang mengerikan, khususnya tantangan pelanggaran privasi, distribusi informasi yang tidak merata, dan penyalahgunaan otonomi individu di dunia maya. Selain itu, penelitian terkini ini mengevaluasi tanggung jawab etika dan hukum yang harus dipikul oleh platform daring—seperti penyedia layanan berbagi video dan media sosial—dalam mencegah dan menanggapi penyebaran konten manipulatif yang didorong oleh kecerdasan buatan. Silakan temukan situs yang terkait dengan ini dengan situs web yang relevan

Dengan pendekatan multidisipliner yang menggabungkan aspek hukum, etika, dan teknologi, diharapkan penelitian ini mampu memberikan kontribusi teoritis dan praktis bagi pengembangan kebijakan perlindungan data pribadi di era digital yang semakin kompleks dan transnasional. Dalam tinjauan literaturnya, (Westerlund, 2021) menyimpulkan bahwa meskipun teknologi deepfake memiliki potensi positif di bidang pendidikan, seni, dan hiburan, namun penyalahgunaannya di ruang publik jauh lebih mendominasi. Oleh karena itu, dibutuhkan regulasi yang lebih spesifik dan proaktif untuk mencegah dampak negatifnya terhadap masyarakat.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang berfokus pada kajian pustaka terhadap norma-norma hukum positif, baik dalam bentuk peraturan perundang-undangan, doktrin hukum, maupun prinsip-prinsip hukum internasional. Pendekatan ini dipilih karena permasalahan yang diangkat menyangkut analisis terhadap kerangka hukum yang berlaku dalam merespons fenomena teknologi deepfake, khususnya dalam konteks perlindungan data pribadi. Dengan pendekatan yuridis normatif, penelitian ini berupaya menelaah sejauh mana norma hukum nasional saat ini mampu menjawab tantangan hukum yang ditimbulkan oleh kemajuan kecerdasan buatan serta menyusun rekomendasi reformasi regulasi berdasarkan asas-asas hukum yang berlaku secara universal.

Penelitian ini menggunakan tiga jenis bahan hukum, yaitu bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan nasional seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Nomor 11 Tahun 2008 juncto UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Selain itu, instrumen hukum internasional seperti General Data Protection Regulation (GDPR) dan Digital Services Act (DSA) juga dianalisis untuk dijadikan pembanding dalam melihat kesiapan sistem hukum Indonesia terhadap dinamika global. Bahan hukum sekunder mencakup berbagai literatur ilmiah seperti jurnal hukum, buku, dan artikel teknologi informasi yang relevan, termasuk karya (Floridi, 2013), (Mittelstadt et al., 2016), dan (Campolo et al., 2017) yang membahas aspek etika dalam tata kelola AI dan data pribadi. Sedangkan bahan hukum tersier, seperti kamus hukum dan ensiklopedia, digunakan untuk memperkuat pemahaman istilah teknis seperti “data biometrik”, “deep learning”, dan “algorithmic accountability”.

Teknik pendekatan yang digunakan dalam penelitian ini bersifat multidimensi. Pendekatan perundang-undangan dilakukan untuk menganalisis muatan norma dalam UU PDP, UU ITE, serta regulasi internasional terkait. Pendekatan konseptual digunakan dalam mengkaji prinsip-prinsip etika digital seperti otonomi, keadilan, dan hak privasi. Sementara itu, pendekatan perbandingan digunakan untuk mengidentifikasi perbedaan dan kesenjangan antara kebijakan nasional dengan instrumen global seperti GDPR, agar dapat ditemukan peluang harmonisasi atau adopsi kebijakan.

Analisis bahan hukum dilakukan secara kualitatif deskriptif dengan metode deduktif, yaitu menarik kesimpulan dari norma hukum yang bersifat umum untuk menjelaskan persoalan khusus yang terjadi, yakni penyalahgunaan teknologi deepfake terhadap data pribadi. Proses analisis dilakukan dengan cara menginventarisasi dan menginterpretasikan ketentuan hukum yang relevan, mengidentifikasi kekosongan atau kelemahan regulasi, serta mengevaluasi prinsip

etika dan tanggung jawab digital dari para aktor, termasuk platform media sosial. Selain itu, pendekatan interdisipliner juga diterapkan untuk mengintegrasikan perspektif hukum, teknologi, dan filsafat etika dalam menjawab kompleksitas persoalan hukum di era kecerdasan buatan.

Dengan pendekatan dan teknik analisis tersebut, diharapkan penelitian ini mampu memberikan gambaran utuh tentang kesiapan hukum nasional menghadapi fenomena deepfake, serta menawarkan rekomendasi normatif yang bersifat proaktif dan solutif dalam rangka penguatan perlindungan data pribadi di era digital yang semakin kompleks.

PEMBAHASAN

1. Kekosongan Regulasi dan Tantangan Penegakan Hukum di Indonesia

Kemajuan teknologi deepfake telah memperlihatkan bahwa sistem hukum di berbagai negara, termasuk Indonesia, belum sepenuhnya siap dalam menghadapi tantangan baru yang ditimbulkan oleh rekayasa digital terhadap data pribadi. Di Indonesia, regulasi utama yang mengatur perlindungan data pribadi adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang baru diberlakukan dan masih dalam tahap transisi implementatif. UU ini menyatakan bahwa setiap pemrosesan data pribadi, termasuk data biometrik seperti wajah dan suara, harus dilakukan atas dasar persetujuan eksplisit dari subjek data. Namun, dalam praktiknya, teknologi deepfake justru memanfaatkan data biometrik tanpa persetujuan, sehingga pelanggaran terhadap hak privasi kerap terjadi dalam ruang digital.

Masalah utama dalam konteks ini adalah belum adanya aturan teknis atau peraturan pelaksana (peraturan pemerintah/peraturan menteri) yang secara khusus mengatur penyalahgunaan data biometrik oleh sistem AI, termasuk deepfake. Akibatnya, aparat penegak hukum mengalami kesulitan dalam mengklasifikasikan dan menindak pelanggaran yang bersifat teknologis kompleks ini. Beberapa kasus deepfake di Indonesia bahkan hanya dikenakan pasal umum seperti pencemaran nama baik atau pelanggaran kesusilaan berdasarkan UU ITE, yang tidak sepenuhnya relevan dengan aspek pelanggaran privasi (Maulana, 2023). Hal ini menciptakan apa yang disebut sebagai *legal loophole*, yaitu kekosongan atau ketidakjelasan hukum yang menyulitkan dalam proses penegakan hukum secara substantif. Berbeda dengan Indonesia, Uni Eropa telah lebih

dahulu mengantisipasi hal ini melalui General Data Protection Regulation (GDPR), yang tidak hanya mengatur perlindungan data pribadi secara komprehensif, tetapi juga memberikan pengakuan khusus terhadap kategori data sensitif, termasuk data biometrik. Dalam Pasal 9 GDPR, diatur bahwa pemrosesan data biometrik untuk tujuan identifikasi seseorang secara unik dilarang, kecuali dengan syarat ketat, termasuk adanya dasar hukum, persetujuan, atau kepentingan vital. Tidak hanya itu, Uni Eropa melalui Digital Services Act (DSA) tahun 2022 bahkan menuntut transparansi algoritma dan audit berkala terhadap platform digital untuk mencegah penyebaran konten manipulatif. Indonesia dapat mengambil pelajaran penting dari model hukum tersebut, khususnya dalam memperkuat prinsip kehati-hatian (*precautionary principle*) dan tanggung jawab operator sistem digital. Sebagai negara yang masih dalam tahap awal implementasi UU PDP, Indonesia seharusnya tidak hanya berfokus pada perlindungan data dalam transaksi komersial, tetapi juga dalam konteks penyalahgunaan identitas digital oleh teknologi manipulatif seperti deepfake.

2. Persoalan Etis Otonomi, Kepercayaan, dan Keadilan Digital

Permasalahan yang ditimbulkan oleh teknologi deepfake tidak hanya bersifat legal formal, tetapi juga menyentuh ranah etika digital. Salah satu prinsip fundamental yang dilanggar oleh deepfake adalah prinsip *respect for autonomy*, yaitu hak setiap individu untuk menentukan bagaimana dirinya direpresentasikan di ruang publik, termasuk representasi visual dan suara. Ketika wajah atau suara seseorang digunakan tanpa persetujuan untuk menciptakan konten palsu—terutama dalam konteks pornografi non-konsensual atau manipulasi politik—maka hak otonomi dan integritas moral individu tersebut dilanggar secara serius (Floridi, 2013). Menurut data dari (Paris, 2019), lebih dari 90% konten deepfake di internet bersifat pornografis, dan mayoritas korban adalah perempuan. Hal ini menunjukkan bahwa teknologi deepfake memperbesar ketimpangan gender dan memperparah bentuk-bentuk kekerasan berbasis gender secara digital. Dari sisi psikologis, korban deepfake mengalami berbagai bentuk trauma, termasuk rasa malu publik, tekanan sosial, kehilangan pekerjaan, dan bahkan bunuh diri dalam kasus-kasus ekstrem. Sistem hukum konvensional belum mampu menyediakan mekanisme pemulihan yang cepat dan menyeluruh bagi para korban, sehingga menambah penderitaan mereka.

Selain pelanggaran terhadap otonomi, deepfake juga mengganggu tatanan epistemik masyarakat. (Campolo et al., 2017) menyebut kondisi ini sebagai *epistemic asymmetry*, yaitu ketimpangan informasi antara pembuat konten dan publik yang mengonsumsinya. Dalam lingkungan digital yang dibanjiri informasi palsu, masyarakat kesulitan membedakan antara kebenaran dan rekayasa. Hal ini menurunkan kualitas

demokrasi, memperlemah kepercayaan publik terhadap institusi, dan mendorong munculnya *information disorder* dalam berbagai bentuk seperti misinformasi, disinformasi, dan malinformasi (Wardle, 2017)

Fenomena ini membuktikan bahwa regulasi hukum saja tidak cukup. Diperlukan pula pendekatan etika teknologi yang mendorong akuntabilitas para aktor, termasuk platform digital, desainer sistem AI, dan penyedia layanan internet. Prinsip *algorithmic accountability* sebagaimana dikembangkan dalam literatur AI ethics (Pasquale, 2015); (Schick, 2024), harus diadopsi dalam desain sistem agar teknologi tidak hanya efisien, tetapi juga adil dan manusiawi.

3. Tanggung Jawab Platform dan Standar Internasional

Platform digital memainkan peran kunci dalam penyebaran maupun pencegahan konten deepfake. Namun hingga saat ini, sebagian besar platform besar seperti YouTube, TikTok, Instagram, dan Facebook belum memiliki sistem pendeteksian otomatis yang cukup andal. Mereka masih mengandalkan pelaporan manual oleh pengguna, yang sangat bergantung pada partisipasi aktif masyarakat dan sering kali terlambat dalam menghentikan penyebaran konten bermasalah (Gillespie, 2018). Kondisi ini memperlihatkan perlunya penguatan mekanisme tanggung jawab platform, baik dalam bentuk hukum keras (*hard law*) maupun kebijakan kolaboratif (*co-regulation*). Di Uni Eropa, Digital Services Act menetapkan bahwa platform yang masuk kategori *very large online platforms* harus melakukan penilaian risiko, audit eksternal, dan membuka sistem algoritma mereka untuk evaluasi publik. DSA bahkan mewajibkan sistem moderasi konten secara *ex ante*—yakni sebelum konten beredar—bukan sekadar *reactive moderation* setelah pelaporan. Meskipun Uni Eropa telah mengesahkan Digital Services Act (DSA) sebagai regulasi yang menuntut tanggung jawab platform, (Jong & O'Neill, 2023) mencatat bahwa masih terdapat celah hukum, khususnya dalam efektivitas pelaksanaan audit algoritma dan perlindungan terhadap penyalahgunaan konten berbasis AI.

Regulasi di Indonesia belum sampai pada tahap ini. Tidak ada kewajiban hukum bagi platform untuk menjalankan audit etis terhadap sistem mereka, atau untuk membuka algoritma rekomendasi yang dapat memicu penyebaran konten manipulatif secara viral. Hal ini membuat posisi korban semakin lemah karena mereka menghadapi

sistem yang tidak transparan dan sulit diakses. Maka, ke depan, regulasi Indonesia perlu diarahkan pada pembentukan kebijakan yang mendorong prinsip *transparency*, *accountability*, dan *human dignity* dalam desain teknologi digital. Platform digital harus diposisikan bukan sebagai pihak netral, melainkan sebagai aktor yang memiliki tanggung jawab normatif dan sosial terhadap ekosistem digital yang mereka ciptakan. Konsep *algorithmic accountability* menjadi semakin penting dalam menghadapi dominasi sistem digital yang tidak transparan. (Schick, 2024) menyarankan bahwa platform digital besar harus membuka sistem algoritma mereka terhadap audit eksternal dan pengawasan publik agar tidak menjadi “kotak hitam” (*black box*) yang kebal terhadap tanggung jawab hukum dan etika. Selain itu, dibutuhkan kerja sama internasional untuk menciptakan standar etik dan hukum yang lintas batas, karena teknologi seperti deepfake bersifat global dan tidak mengenal yurisdiksi nasional.

4. Kebijakan Global dan Harmonisasi Hukum Internasional

Fenomena deepfake bukanlah isu yang terbatas pada satu negara, melainkan persoalan transnasional yang berdampak lintas yurisdiksi. Oleh karena itu, banyak negara mulai menerapkan pendekatan regulatif yang lebih progresif guna mengantisipasi penyalahgunaan teknologi manipulatif ini. Tiongkok, misalnya, melalui Provisions on the Administration of Deep Synthesis Internet Information Services (2023), telah mewajibkan bahwa semua konten digital yang dihasilkan melalui teknologi deepfake harus disertai label yang jelas, termasuk informasi tentang metode sintesis dan identitas pembuatnya. Kebijakan ini menempatkan kewajiban tinggi pada pengendali sistem agar bertanggung jawab terhadap transparansi algoritma.

Di Korea Selatan, langkah yang lebih ketat tengah dipertimbangkan dengan menyusun kerangka hukum pidana baru yang khusus menjerat pelaku pembuatan konten deepfake eksplisit, terutama yang bermuatan pornografi non-konsensual. Negara ini bahkan telah mulai mendorong kerja sama antara badan pengawas internet dan perusahaan teknologi untuk membentuk unit deteksi konten berbasis AI secara real-time. Di Amerika Serikat, meskipun belum terdapat regulasi federal yang komprehensif, beberapa negara bagian seperti California dan Texas telah mengesahkan undang-undang yang melarang penggunaan deepfake untuk tujuan politik menjelang pemilu, serta melindungi individu dari pemalsuan citra berbasis AI. Selain itu, berbagai lembaga seperti Electronic Frontier Foundation (EFF) dan AI Now Institute turut mendorong terbentuknya kerangka regulasi etik terhadap sistem AI yang dapat digunakan secara manipulatif (Campolo et al., 2017); EFF, 2020). Uni Eropa sendiri telah menjadi pionir

dalam pembentukan regulasi digital yang tanggap terhadap (Campolo et al., 2017) fenomena baru. Selain GDPR, Uni Eropa juga mengesahkan Digital Services Act (DSA) yang memberikan dasar hukum terhadap tanggung jawab platform dalam menangani konten berbahaya, termasuk konten deepfake. DSA menekankan prinsip transparansi algoritma, audit sistem AI secara rutin, serta penilaian dampak sosial (social risk assessment) sebagai bagian dari kewajiban hukum platform besar.

Indonesia dapat mengambil pelajaran penting dalam mengembangkan sistem hukum yang lebih antisipatif dan adaptif. Salah satu langkah yang dapat dilakukan adalah mengembangkan mekanisme pelabelan dan penandaan konten berbasis AI, serta mewajibkan platform digital untuk menyediakan informasi asal-usul konten (content provenance). Di samping itu, Indonesia dapat memperkuat partisipasinya dalam forum-forum internasional seperti Internet Governance Forum (IGF), Global Privacy Assembly, dan ASEAN Digital Ministers Meeting (ADGMIN) sebagai ruang untuk mendorong pembentukan standar internasional terkait perlindungan data dan etika teknologi. Penting pula untuk mengintegrasikan prinsip-prinsip dari International Covenant on Civil and Political Rights (ICCPR)—yang telah diratifikasi Indonesia melalui UU No. 12 Tahun 2005—sebagai dasar dalam mengembangkan norma hukum terhadap deepfake. ICCPR menjamin hak atas privasi, perlindungan dari perlakuan tidak manusiawi, serta hak atas reputasi dan integritas moral. Prinsip ini harus menjadi landasan moral dan yuridis dalam setiap langkah legislasi teknologi digital di Indonesia.

Dengan demikian, harmonisasi hukum digital lintas negara bukan hanya menjadi keharusan normatif, tetapi juga menjadi strategi strategis bagi Indonesia dalam menghadapi risiko globalisasi teknologi digital. Kolaborasi, interoperabilitas hukum, dan pengakuan terhadap standar internasional akan memperkuat posisi Indonesia sebagai negara yang tidak hanya reaktif terhadap teknologi, tetapi juga proaktif dalam membentuk masa depan etika dan hukum digital.

5. Rekomendasi Etis dan Regulatif

Analisis terhadap tantangan hukum dan etika yang diuraikan sebelumnya, respon terhadap maraknya konten deepfake di media sosial memerlukan pendekatan lintas sektor yang menyeluruh, dengan berlandaskan pada prinsip keadilan digital dan perlindungan hak asasi manusia. Pertama, penguatan hukum positif menjadi urgensi utama. Revisi terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta penyusunan peraturan pelaksana dari UU Perlindungan Data Pribadi (UU PDP) harus secara eksplisit mengatur isu-isu yang berkaitan dengan kecerdasan buatan, data

biometrik, dan konten manipulatif. Tanpa kerangka hukum yang jelas dan teknis, pelanggaran kompleks seperti penyebaran deepfake akan terus berada di wilayah abu-abu hukum (Effendy, 2022)

Edukasi publik melalui peningkatan literasi digital perlu diperkuat guna membangun kapasitas kritis masyarakat dalam mengenali dan menolak konten palsu. (Wardle, 2017) menekankan bahwa upaya melawan information disorder tidak dapat bergantung semata pada regulasi, tetapi juga memerlukan pemberdayaan pengguna sebagai aktor literat digital. Ketiga, penerapan audit etis pada sistem algoritmik yang digunakan oleh platform digital menjadi krusial untuk memastikan prinsip algorithmic accountability. Hal ini sejalan dengan gagasan (Pasquale, 2015) mengenai black box society, di mana transparansi dan akuntabilitas sistem digital menjadi kunci dalam mencegah bias dan ketimpangan informasi.

Penyediaan layanan pemulihan yang komprehensif penting bagi korban konten deepfake, mencakup bantuan hukum, dukungan psikologis, dan mekanisme cepat untuk penghapusan konten yang merusak reputasi serta privasi individu. Menurut laporan dari (Electronic Frontier Foundation., 2020), korban sering menghadapi hambatan prosedural dan psikologis dalam mengakses keadilan, sehingga diperlukan mekanisme yang lebih empatik dan responsif. Terakhir, kolaborasi internasional menjadi pilar penting dalam menghadapi fenomena transnasional seperti deepfake. Indonesia perlu mengambil peran aktif dalam forum global seperti Internet Governance Forum (IGF) dan ASEAN Digital Ministers Meeting (ADGMIN) untuk mendorong pembentukan standar regional dalam menghadapi teknologi manipulatif. Upaya harmonisasi ini sejalan dengan prinsip shared responsibility dan pentingnya interoperability dalam tata kelola internet global (DeNardis, 2014). Pendekatan integratif tersebut tidak hanya memperkuat sistem hukum nasional, tetapi juga memosisikan Indonesia sebagai aktor aktif dalam wacana etika dan hukum digital internasional.

KESIMPULAN DAN SARAN

Fenomena deepfake merupakan tantangan serius terhadap perlindungan data pribadi, hak privasi, dan integritas digital individu. Meskipun Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), regulasi tersebut belum sepenuhnya menjawab kompleksitas penyalahgunaan data biometrik melalui teknologi manipulatif. Tidak adanya aturan teknis yang spesifik, lemahnya moderasi konten oleh platform digital, serta pendekatan hukum pidana yang

belum adaptif membuat korban konten deepfake berada dalam posisi rentan. Dari sudut etika, praktik penyebaran konten palsu tanpa persetujuan individu merupakan bentuk pelanggaran terhadap prinsip otonomi, keadilan informasi, dan tanggung jawab sosial. Ketimpangan informasi dan absennya transparansi algoritmik memperparah krisis kepercayaan digital di tengah masyarakat. Sementara itu, sistem hukum Indonesia masih berfokus pada pendekatan reaktif, dan belum membangun infrastruktur hukum yang antisipatif dan kolaboratif.

Melalui studi perbandingan, tampak bahwa negara-negara seperti Tiongkok, Korea Selatan, dan Uni Eropa telah merespons fenomena ini dengan kebijakan yang lebih ketat dan progresif, termasuk pelabelan konten AI, audit sistem algoritma, serta pengenaan sanksi terhadap pelaku deepfake. Indonesia dapat mengambil pelajaran penting dari model tersebut melalui penguatan regulasi berbasis prinsip transparansi, akuntabilitas, dan penghormatan terhadap martabat manusia. Oleh karena itu, penelitian ini merekomendasikan perlunya peraturan pelaksana UU PDP yang mencakup isu AI dan data biometrik, revisi UU ITE yang relevan, kewajiban audit etis bagi platform digital, serta penguatan literasi digital publik. Kolaborasi internasional juga perlu diperluas agar Indonesia dapat terlibat aktif dalam penyusunan standar global tata kelola teknologi manipulatif seperti deepfake. Dengan pendekatan hukum yang integratif dan adaptif, perlindungan data pribadi dapat ditegakkan secara lebih efektif dan bermartabat di tengah kemajuan teknologi digital.

UCAPAN TERIMA KASIH

penulis mengucapkan terima kasih yang sebesar-besarnya kepada Dosen Pembimbing yang telah dengan sabar membimbing, mengarahkan, dan memberikan masukan yang sangat berharga selama proses penyusunan jurnal ini. Bimbingan akademik dan motivasi yang diberikan telah menjadi pijakan penting dalam penyelesaian tulisan ini secara ilmiah dan sistematis. Penulis juga menyampaikan terima kasih kepada seluruh rekan dan sahabat seperjuangan yang telah memberikan semangat, masukan, serta diskusi yang membangun selama proses penelitian ini berlangsung. Dukungan moral dan kerja sama yang hangat telah menjadi kekuatan tersendiri dalam menghadapi setiap tantangan yang muncul. Semoga tulisan ini dapat memberikan kontribusi positif bagi pengembangan keilmuan, khususnya dalam bidang hukum dan etika digital.

DAFTAR PUSTAKA

- Campolo, A., Sanfilippo, M., Whittaker, M., & Crawford, K. (2017). *AI Now 2017 report*. AI Now Institute. [https://ainowinstitute.org/AI Now 2017 Report.pdf](https://ainowinstitute.org/AI_Now_2017_Report.pdf)
- Chesney, R., & Citron, D. K. (2020). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 99(1), 147–155.
- Custers, B., & Keymolen, E. (2022). Artificial intelligence and the right to explanation: Three legal bases under the GDPR. *Computer Law & Security Review*, 44, Article 105634. <https://doi.org/10.1016/j.clsr.2022.105634>
- Dechesne, F. (2020). Ethics of AI and robotics. In *The Stanford Encyclopedia of Philosophy* (Fall 2020 Edition). <https://plato.stanford.edu/entries/ethics-ai/>
- Effendy, M. (2022). Tantangan penegakan hukum terhadap kejahatan siber. *Jurnal Hukum & Teknologi*, 7(1), 45–60.
- Electronic Frontier Foundation. (2020). *Deepfakes and synthetic media*. <https://www.eff.org>
- European Union. (2022). *Digital Services Act (DSA)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065>
- Floridi, L. (2013). *The ethics of information*. Oxford University Press.
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Jong, M., & O'Neill, B. (2023). Deepfake regulation in Europe: Assessing the gaps in the Digital Services Act. *Journal of Cyber Policy*, 8(1), 67–82. <https://doi.org/10.1080/23738871.2023.2184123>
- Kementerian Komunikasi dan Informatika. (2022). *Panduan perlindungan data pribadi*. <https://kominfo.go.id>
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Mansour, R., & Mahfouz, A. (2023). Ethics and deepfake technology: Mitigating risks through AI governance. *AI & Society*. <https://doi.org/10.1007/s00146-023-01653-w>
- Maulana, R. (2023). Kesenjangan hukum terhadap deepfake di Indonesia. *Jurnal Informasi Digital*, 4(2), 89–102.

- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>
- Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society. <https://datasociety.net/library/deepfakes-and-cheap-fakes/>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Schick, W., & Slotwinski, M. (2024). Algorithmic accountability and fairness in digital platforms: A legal perspective. *AI and Ethics*, 4(1), 23–38. <https://doi.org/10.1007/s43681-023-00256-1>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe. <https://www.coe.int/en/web/freedom-expression/information-disorder>
- West, D. M. (2020). *The rise of deepfakes: How disinformation threatens democracy and what can be done about it*. Brookings Institution. <https://www.brookings.edu>
- Westerlund, M. (2021). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 11(2), 39–52. <https://doi.org/10.22215/timreview/1412>