

Urgensi Pengaturan Deepfake dalam Perlindungan Data Pribadi dan Reputasi Digital di Indonesia

Raysa Diva Zalianti¹ Monica Tiur Simamora² Marco Vito Naibaho³ Marcel Zefanta Tarigan⁴ Dewi Pika Lumban Batu⁵ Parlaungan Gabriel Siahaan⁶

Program Studi Hukum Bisnis, Fakultas Ilmu Sosial, Wilayah, Universitas Negeri Medan, Indonesia^{1,2,3,4,5,6}

Email: raysa.3253240005@mhs.unimed.ac.id¹

monicatiurism.3252540003@mhs.unimed.ac.id²

marconaibaho.3253540007@mhs.unimed.ac.id³

marselsamuel.3253540006@mhs.unimed.ac.id⁴ dewi_pika_lumban@unimed.ac.id⁵

parlaungansiahaan@unimed.ac.id⁶

Abstrak

Perkembangan teknologi kecerdasan buatan telah menghadirkan teknologi deepfake yang mampu menghasilkan manipulasi gambar, suara, dan video secara realistis sehingga menimbulkan permasalahan hukum baru, khususnya terhadap perlindungan data pribadi dan reputasi digital di Indonesia. Permasalahan penelitian ini berfokus pada belum adanya pengaturan khusus mengenai penyalahgunaan deepfake yang menyebabkan ketidakpastian perlindungan hukum terhadap individu sebagai pemilik data dan korban manipulasi digital. Penelitian ini bertujuan untuk menganalisis urgensi pengaturan deepfake dalam sistem hukum Indonesia serta mengkaji keterkaitannya dengan perlindungan data pribadi dan reputasi digital. Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif dengan pendekatan perundang-undangan dan konseptual karena penelitian ini berfokus pada analisis norma hukum, regulasi, serta konsep hukum yang berkaitan dengan perkembangan teknologi digital. Hasil penelitian menunjukkan bahwa pengaturan hukum Indonesia saat ini belum secara spesifik mengatur deepfake, sehingga perlindungan terhadap korban masih bergantung pada interpretasi terhadap regulasi yang telah ada. Penelitian ini menyimpulkan bahwa diperlukan pembentukan regulasi khusus yang mengintegrasikan perlindungan data pribadi dan reputasi digital dalam menghadapi penyalahgunaan deepfake. Penelitian selanjutnya disarankan menggunakan pendekatan empiris untuk mengkaji praktik penegakan hukum dan perlindungan korban deepfake.

Kata Kunci: Deepfake, Perlindungan Data Pribadi, Reputasi Digital

Abstract

The development of artificial intelligence technology has introduced deepfake technology, which is capable of producing realistic manipulations of images, voices, and videos, thereby creating new legal issues, particularly regarding the protection of personal data and digital reputation in Indonesia. This research problem focuses on the absence of specific regulations governing deepfake misuse, which creates legal uncertainty in providing protection for individuals as personal data owners and victims of digital manipulation. This study aims to analyze the urgency of regulating deepfake within the Indonesian legal system and to examine its relationship with personal data protection and digital reputation protection. The research method used is normative juridical research with statutory and conceptual approaches, as this study focuses on analyzing legal norms, regulations, and legal concepts related to digital technology development. The results indicate that the current Indonesian legal framework does not specifically regulate deepfake, causing victim protection to remain dependent on interpretations of existing regulations. This study concludes that specific regulations are needed to integrate personal data protection and digital reputation protection in addressing deepfake misuse. Further research is recommended to employ an empirical approach to examine law enforcement practices and victim protection mechanisms regarding deepfake cases.

Keywords: Deepfake, Personal Data Protection, Digital Reputation



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

PENDAHULUAN

Transformasi digital yang berlangsung secara masif dalam beberapa dekade terakhir telah mengubah cara masyarakat berinteraksi, berkomunikasi, dan memperoleh informasi. Perkembangan teknologi informasi tidak hanya menghadirkan kemudahan dalam berbagai aspek kehidupan, tetapi juga melahirkan tantangan hukum baru yang sebelumnya tidak pernah dibayangkan. Salah satu perkembangan teknologi yang saat ini menjadi perhatian global adalah kemunculan teknologi Artificial Intelligence (AI) yang mampu menghasilkan berbagai bentuk konten digital secara otomatis, termasuk gambar, suara, video, maupun teks yang menyerupai kondisi nyata. Salah satu produk perkembangan kecerdasan buatan yang paling banyak menimbulkan perdebatan hukum dan etika adalah teknologi deepfake. Secara sederhana, deepfake merupakan teknologi berbasis kecerdasan buatan yang memungkinkan manipulasi wajah, suara, maupun gerakan seseorang ke dalam suatu video atau rekaman digital sehingga menghasilkan tampilan yang sangat realistis dan sulit dibedakan dari kondisi yang sebenarnya. Kehadiran teknologi ini pada awalnya dikembangkan untuk kepentingan hiburan, industri perfilman, pendidikan, serta pengembangan teknologi digital. Namun dalam praktiknya, deepfake juga mulai digunakan untuk berbagai tujuan yang bersifat merugikan, seperti penyebaran informasi palsu, manipulasi politik, penipuan digital, pencurian identitas, hingga pembuatan konten yang menyerang kehormatan dan reputasi seseorang.¹ Fenomena penyalahgunaan deepfake bukan lagi sekadar isu teoritis, melainkan telah menjadi permasalahan nyata di berbagai negara. Penggunaan deepfake mengalami peningkatan yang sangat signifikan seiring dengan semakin mudahnya akses masyarakat terhadap teknologi kecerdasan buatan generatif. Saat ini seseorang tidak lagi memerlukan kemampuan teknis tingkat tinggi untuk membuat video atau audio palsu karena berbagai aplikasi berbasis AI telah tersedia secara luas dan dapat digunakan oleh siapa saja. Kondisi tersebut menyebabkan risiko penyalahgunaan identitas digital menjadi semakin besar, terutama terhadap tokoh publik, pejabat negara, pelaku usaha, maupun masyarakat umum.

Perkembangan tersebut secara langsung menimbulkan tantangan baru bagi sistem hukum. Jika sebelumnya tindakan pemalsuan identitas umumnya dilakukan melalui dokumen fisik atau manipulasi konvensional, maka saat ini pemalsuan dapat dilakukan melalui rekayasa digital yang jauh lebih kompleks dan sulit dideteksi. Dalam banyak kasus, korban deepfake tidak hanya mengalami kerugian materiil, tetapi juga mengalami kerugian immateriil berupa rusaknya nama baik, menurunnya kepercayaan publik, terganggunya kehidupan pribadi, bahkan munculnya tekanan psikologis akibat penyebaran konten palsu yang mengatasnamakan dirinya. Dalam konteks Indonesia, ancaman deepfake menjadi semakin relevan karena tingginya tingkat penggunaan internet dan media sosial oleh masyarakat. Kemudahan akses terhadap aplikasi berbasis AI membuat proses pembuatan konten manipulatif tidak lagi memerlukan kemampuan teknis yang kompleks. Seseorang dapat menggunakan foto, video, atau rekaman suara yang diperoleh dari media sosial untuk menghasilkan konten palsu yang menyerupai individu tertentu. Kondisi ini menimbulkan kekhawatiran karena sebagian besar data yang digunakan dalam proses pembuatan deepfake berasal dari data pribadi yang tersebar di ruang digital. Di sisi lain, penggunaan teknologi deepfake memiliki keterkaitan yang erat dengan perlindungan data pribadi. Pada dasarnya, proses pembuatan deepfake membutuhkan data berupa foto, video, suara, atau informasi

¹ Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1820, <https://doi.org/https://doi.org/10.15779/Z38RVOD15J>.

identitas seseorang yang kemudian diproses menggunakan teknologi kecerdasan buatan untuk menghasilkan konten baru yang menyerupai individu tersebut. Dengan kata lain, keberadaan deepfake tidak dapat dilepaskan dari penggunaan data pribadi sebagai bahan utama pembentuk konten sintetis. Ketika penggunaan data tersebut dilakukan tanpa persetujuan pemilik data, maka tindakan tersebut berpotensi melanggar hak privasi dan hak atas perlindungan data pribadi yang dimiliki setiap individu.²

Pengakuan terhadap pentingnya perlindungan data pribadi di Indonesia semakin diperkuat melalui berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kehadiran undang-undang ini merupakan langkah penting dalam memberikan kepastian hukum terhadap hak-hak subjek data pribadi di era digital. Namun demikian, meskipun telah terdapat pengaturan mengenai pelindungan data pribadi, undang-undang tersebut belum secara khusus mengatur penggunaan teknologi deepfake sebagai salah satu bentuk penyalahgunaan data pribadi berbasis kecerdasan buatan. Demikian pula dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik yang telah mengatur berbagai bentuk penyalahgunaan teknologi informasi, namun belum memberikan klasifikasi maupun pengaturan khusus mengenai tindak penyalahgunaan deepfake.³ Akibatnya, masih terdapat ruang interpretasi yang cukup luas dalam menentukan dasar hukum yang tepat untuk menjerat pelaku maupun memberikan perlindungan yang optimal kepada korban. Selain berkaitan dengan data pribadi, deepfake juga berpotensi menimbulkan pelanggaran terhadap reputasi digital seseorang. Dalam era masyarakat informasi, reputasi digital memiliki nilai yang sangat penting karena dapat memengaruhi kehidupan sosial, profesional, maupun ekonomi seseorang. Reputasi yang telah dibangun selama bertahun-tahun dapat rusak hanya dalam waktu singkat akibat penyebaran konten palsu yang dipercaya oleh masyarakat. Dalam beberapa kasus, video atau audio deepfake digunakan untuk menggambarkan seseorang melakukan tindakan yang sebenarnya tidak pernah dilakukan, sehingga menimbulkan persepsi negatif yang sulit dipulihkan meskipun kemudian terbukti bahwa konten tersebut merupakan hasil manipulasi. Perlindungan terhadap kehormatan dan nama baik memang telah diatur dalam berbagai ketentuan hukum Indonesia, namun pengaturan tersebut masih bersifat umum dan belum secara spesifik dirancang untuk menghadapi karakteristik deepfake yang memanfaatkan kecerdasan buatan sebagai sarana utama pembentukan konten.⁴

Kajian mengenai deepfake dalam perspektif hukum siber telah berkembang dalam beberapa tahun terakhir. Penelitian yang dilakukan oleh Rizky Karo Karo dan Zein Jiddan (2025) menunjukkan bahwa penyalahgunaan deepfake memiliki keterkaitan erat dengan pelanggaran hak atas perlindungan data pribadi sebagaimana diatur dalam UU ITE dan UU Pelindungan Data Pribadi. Penelitian tersebut menegaskan bahwa hukum positif Indonesia belum memiliki pengaturan khusus mengenai deepfake sehingga perlindungan hukum masih bergantung pada interpretasi terhadap ketentuan yang sudah ada. Penelitian Kartika Ardina Raesyah Putri dan Haris Djoko Saputro (2025) membahas pertanggungjawaban hukum atas penggunaan Artificial Intelligence untuk menghasilkan deepfake berdasarkan UU Pelindungan Data Pribadi. Sementara itu, penelitian Rendi Syaputra dan Eko Nuriyatman (2024) menitikberatkan pada perlindungan korban deepfake dari perspektif hukum pidana Indonesia.

² Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP (Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law)," *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia (JIHAM)* 4, no. 2 (2025): 78-82, <https://doi.org/https://doi.org/10.35912/jihham.v4i2.3937>.

³ Rizky Karo Karo, Zein Jiddan, and Hannan Atanto Buono, "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia," *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, Dan Hukum (SENPIHUM)* 1, no. 1 (2026).

⁴ Rendi Syaputra Nur Haida and Eko Nutriyatman, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (AI) Dari Perspektif Hukum Pidana Indonesia," *Jurnal Respublica* 24, no. 1 (2024), <https://doi.org/https://doi.org/10.31849/respublica.v24i01.23327>.

Berbagai penelitian tersebut menunjukkan bahwa isu deepfake telah memperoleh perhatian akademik, namun fokus kajiannya masih terpisah antara aspek perlindungan data pribadi, pertanggungjawaban hukum, dan perlindungan korban.

No.	Peneliti Terdahulu	Judul	Fokus Penelitian	Perbedaan dengan Penelitian Ini
1.	Rizky Karo Karo & Zein Jiddan (2026)	Analisis dalam Kasus Penyalahgunaan Deepfake dari Segi Perlindungan Data Pribadi dalam UU ITE dan UU PDP di Indonesia	Perlindungan data pribadi	Penelitian ini menambahkan analisis reputasi digital dan urgensi regulasi khusus.
2.	Kartika Ardina Raesyah Putri & Haris Djoko Saputro (2025)	Pertanggungjawaban Hukum atas Penggunaan Artificial Intelligence untuk Deepfake Menurut UU Pelindungan Data Pribadi	Pertanggungjawaban hukum	Penelitian ini berfokus pada kebutuhan pengaturan hukum yang lebih komprehensif.
3.	Rendi Syaputra & Eko Nuriyatman (2024)	Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence dari Perspektif Hukum Pidana Indonesia	Perlindungan korban dan hukum pidana	Penelitian ini mengkaji hubungan deepfake dengan data pribadi dan reputasi digital dalam perspektif hukum siber.

Berdasarkan penelitian terdahulu tersebut, belum ditemukan penelitian yang secara khusus mengkaji urgensi pengaturan deepfake dengan mengintegrasikan perlindungan data pribadi dan perlindungan reputasi digital dalam satu kerangka analisis yang komprehensif. Sebagian besar penelitian terdahulu berfokus pada perlindungan data pribadi, pertanggungjawaban hukum pelaku, atau perlindungan korban dari perspektif hukum pidana secara terpisah. Padahal, penyalahgunaan deepfake pada praktiknya dapat menimbulkan dua bentuk kerugian sekaligus, yaitu pelanggaran terhadap hak atas data pribadi dan kerusakan reputasi digital korban. Kebaruan penelitian ini terletak pada analisis mengenai kebutuhan pengaturan deepfake sebagai instrumen perlindungan terhadap dua kepentingan hukum tersebut secara bersamaan. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan hukum siber Indonesia yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan. Penelitian ini bertujuan untuk menganalisis urgensi pengaturan teknologi deepfake dalam sistem hukum Indonesia, mengkaji keterkaitan penyalahgunaan deepfake dengan pelanggaran data pribadi dan reputasi digital, serta menganalisis kebutuhan pembentukan pengaturan hukum yang lebih spesifik guna memberikan perlindungan yang efektif terhadap masyarakat di era perkembangan kecerdasan buatan.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif dengan jenis penelitian hukum yuridis normatif. Penelitian yuridis normatif dilakukan dengan mengkaji norma-norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin, asas hukum, serta berbagai literatur yang berkaitan dengan permasalahan penelitian. Metode ini dipilih karena penelitian berfokus pada analisis pengaturan hukum mengenai teknologi deepfake dalam perlindungan data pribadi dan reputasi digital di Indonesia. Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan objek penelitian, antara lain Undang-Undang Nomor

27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sementara itu, pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang berkaitan dengan deepfake, kecerdasan buatan (artificial intelligence), perlindungan data pribadi, reputasi digital, dan hukum siber.

Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh melalui studi kepustakaan (*library research*) dan studi dokumentasi. Teknik pengumpulan data dilakukan dengan menelusuri, mengidentifikasi, menginventarisasi, serta mengkaji berbagai sumber hukum yang relevan dengan permasalahan penelitian. Data yang digunakan dalam penelitian ini merupakan data sekunder yang terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi dan teknologi informasi, yaitu Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Adapun bahan hukum sekunder terdiri atas buku, jurnal ilmiah, hasil penelitian terdahulu, prosiding, dan berbagai literatur yang relevan dengan deepfake, kecerdasan buatan, perlindungan data pribadi, reputasi digital, dan hukum siber. Data yang telah terkumpul kemudian dianalisis menggunakan metode analisis kualitatif deskriptif. Analisis dilakukan melalui proses klasifikasi, interpretasi, dan penelaahan terhadap berbagai bahan hukum yang telah diperoleh untuk mengidentifikasi kecukupan pengaturan hukum yang berlaku dalam mengantisipasi penyalahgunaan teknologi deepfake. Hasil analisis selanjutnya disusun secara sistematis guna memperoleh pemahaman yang komprehensif mengenai urgensi pengaturan deepfake dalam perlindungan data pribadi dan reputasi digital di Indonesia.

HASIL PENELITIAN DAN PEMBAHASAN

Pengaturan Hukum Deepfake dalam Sistem Hukum Indonesia

Pada peraturan perundang-undangan yang berlaku di Indonesia belum ditemukan pengaturan yang secara khusus mengatur teknologi deepfake sebagai bentuk manipulasi konten digital berbasis kecerdasan buatan. Pengaturan yang berkaitan dengan penyalahgunaan deepfake saat ini masih tersebar dalam berbagai regulasi, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektron. Hasil pencatatan bahan hukum menunjukkan bahwa ketiga regulasi tersebut telah mengatur perlindungan terhadap data pribadi, penggunaan sistem elektronik, serta penyebaran informasi elektronik yang merugikan pihak lain. Namun, tidak ditemukan ketentuan yang memberikan definisi hukum mengenai deepfake, klasifikasi bentuk penyalahgunaan deepfake, maupun mekanisme penanganan khusus terhadap konten sintetis yang dihasilkan melalui teknologi kecerdasan buatan. Perlindungan terhadap korban penyalahgunaan deepfake juga masih bergantung pada interpretasi berbagai ketentuan hukum yang telah ada. Dengan demikian, belum terdapat instrumen hukum yang secara khusus dirancang untuk mengantisipasi perkembangan teknologi deepfake dalam ruang digital Indonesia.

Penggunaan Data Pribadi sebagai Dasar Pembentukan Deepfake

Proses pembentukan deepfake memerlukan data yang berkaitan langsung dengan identitas seseorang. Data tersebut meliputi foto, video, rekaman suara, data biometrik wajah,

ekspresi, serta karakteristik visual dan audio lainnya yang kemudian diproses menggunakan sistem kecerdasan buatan untuk menghasilkan konten sintetis yang menyerupai individu tertentu. Penggunaan data pribadi tanpa persetujuan pemilik data juga menjadi salah satu karakteristik utama dalam berbagai kasus penyalahgunaan deepfake. Data yang sebelumnya dipublikasikan melalui media sosial, platform digital, maupun sumber daring lainnya dapat digunakan kembali untuk menghasilkan video atau audio manipulatif tanpa sepengetahuan subjek data. Kondisi tersebut menunjukkan adanya hubungan yang erat antara teknologi deepfake dan perlindungan data pribadi.⁵ Perkembangan teknologi artificial intelligence generatif ini telah meningkatkan kemampuan sistem dalam mereplikasi wajah dan suara seseorang secara lebih realistis. Sehingga kemudahan akses terhadap berbagai aplikasi berbasis AI menyebabkan proses pembuatan deepfake tidak lagi memerlukan kemampuan teknis yang tinggi sehingga potensi penyalahgunaan data pribadi menjadi semakin luas.

Data Empiris Insiden dan Modus Penyalahgunaan Deepfake Berdampak Ganda

Perkembangan teknologi deepfake dalam beberapa tahun terakhir menunjukkan bahwa pemanfaatan kecerdasan buatan tidak lagi terbatas pada kebutuhan hiburan, pendidikan, maupun industri kreatif. Kemudahan akses terhadap berbagai aplikasi berbasis artificial intelligence memungkinkan pembuatan konten sintetis berupa gambar, video, dan audio yang memiliki tingkat kemiripan tinggi dengan individu asli. Kondisi tersebut turut meningkatkan potensi penyalahgunaan teknologi untuk berbagai tujuan yang merugikan, terutama yang berkaitan dengan data pribadi dan reputasi digital. Salah satu bentuk penyalahgunaan yang banyak ditemukan adalah penggunaan foto, video, dan rekaman suara seseorang untuk menghasilkan konten sintetis yang menyerupai individu tersebut tanpa persetujuan pemilik data. Materi yang digunakan umumnya diperoleh dari media sosial, platform berbagi video, maupun berbagai sumber digital lain yang dapat diakses secara terbuka. Data tersebut kemudian diproses menggunakan teknologi kecerdasan buatan untuk menghasilkan representasi visual maupun audio yang tampak autentik sehingga sulit dibedakan dari konten asli. Fenomena ini mulai terlihat dalam berbagai peristiwa politik di Indonesia. Kajian mengenai penggunaan deepfake pada Pemilu Indonesia Tahun 2024 menunjukkan adanya pemanfaatan teknologi kecerdasan buatan untuk menghasilkan konten audio dan video yang menyerupai tokoh politik tertentu. Manipulasi tersebut dilakukan melalui teknik rekayasa suara (*voice cloning*) dan visual sehingga menciptakan kesan bahwa individu yang bersangkutan benar-benar menyampaikan pernyataan tertentu kepada publik.⁶ Selain itu, penelitian lain mengenai penyebaran hoaks pada masa kampanye Pemilu 2024 menemukan bahwa perkembangan teknologi deepfake berpotensi memperkuat penyebaran informasi yang menyesatkan karena konten yang dihasilkan memiliki tingkat realisme yang semakin tinggi.⁷

Selain digunakan dalam konteks politik, teknologi deepfake juga dimanfaatkan dalam berbagai bentuk penyalahgunaan identitas digital. Pemanfaatan foto, video, dan rekaman suara yang tersedia di ruang digital memungkinkan pelaku menghasilkan konten sintetis yang menyerupai individu tertentu tanpa persetujuan pemilik data. Teknologi tersebut dapat digunakan untuk menciptakan pernyataan, tindakan, maupun representasi visual yang sebenarnya tidak pernah dilakukan oleh individu yang bersangkutan. Kondisi ini menunjukkan bahwa perkembangan kecerdasan buatan telah memperluas risiko penggunaan data pribadi secara tidak sah sekaligus meningkatkan potensi kerugian yang dialami oleh korban di ruang

⁵ Karishma Verma, "Digital Deception: The Impact of Deepfakes on Privacy Rights," *LEX SCIENTIA LAW REVIEW* 8, no. 2 (2024): 856–96.

⁶ Burhanuddin Muhtadi and Maria Monica Wihardja, "Deepfakes and Selective Belief: How Partisanship Affects Voters' Exposure and Susceptibility to Deepfake Content," 2024.

⁷ Wilma Silalahi, Meily Natassya, and Shane Evelina, "Penggunaan Deepfake Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024," *Jurnal Bawaslau Provinsi Kepulauan Riau* 6, no. 1 (2024).

digital. Selain itu perkembangan teknologi voice cloning pada deepfake juga memperluas bentuk penyalahgunaan identitas digital. Dengan memanfaatkan sampel suara dalam durasi yang relatif singkat, sistem kecerdasan buatan mampu menghasilkan tiruan suara yang menyerupai individu tertentu. Kemampuan tersebut meningkatkan risiko penyebaran informasi palsu, penipuan digital, serta penciptaan pernyataan fiktif yang dapat memengaruhi persepsi publik terhadap seseorang. Berbagai modus tersebut menunjukkan bahwa satu tindakan deepfake dapat menimbulkan dua konsekuensi sekaligus. Pada tahap awal terjadi penggunaan data pribadi tanpa izin melalui pengambilan foto, video, atau rekaman suara milik seseorang. Selanjutnya, ketika konten sintesis tersebut disebarluaskan kepada publik, muncul potensi kerusakan terhadap reputasi digital, kehormatan, dan kredibilitas individu yang menjadi objek manipulasi. Perkembangan generative artificial intelligence yang semakin mudah diakses memperlihatkan bahwa bentuk penyalahgunaan identitas digital telah mengalami transformasi yang signifikan. Jika sebelumnya manipulasi dilakukan melalui teknik penyuntingan konvensional yang relatif mudah dikenali, saat ini konten sintesis dapat dibuat dengan tingkat realisme yang jauh lebih tinggi. Kondisi tersebut mendorong sejumlah negara untuk mulai mengembangkan regulasi khusus mengenai transparansi penggunaan kecerdasan buatan dan kewajiban pelabelan terhadap konten yang dihasilkan oleh sistem AI.⁸

Dampak Deepfake terhadap Reputasi Digital

Reputasi digital merupakan salah satu aspek yang paling rentan terdampak akibat penyalahgunaan teknologi deepfake. Konten deepfake memungkinkan seseorang ditampilkan melakukan tindakan, mengucapkan pernyataan, atau terlibat dalam suatu peristiwa yang sebenarnya tidak pernah terjadi. Penyebaran konten deepfake dapat membentuk persepsi publik yang keliru terhadap individu yang menjadi objek manipulasi. Dalam berbagai kasus yang dikaji, dampak yang muncul meliputi menurunnya tingkat kepercayaan publik, terganggunya hubungan profesional, kerusakan citra pribadi, serta munculnya stigma sosial yang berkelanjutan.⁹ Selain itu, ditemukan bahwa reputasi digital yang telah dibangun dalam jangka waktu panjang dapat mengalami penurunan dalam waktu yang relatif singkat akibat penyebaran konten sintesis yang dipercaya sebagai informasi autentik. Karakteristik media digital yang memungkinkan reproduksi dan distribusi informasi secara cepat turut memperbesar dampak yang ditimbulkan oleh penyalahgunaan deepfake.

Kekosongan Norma Pengaturan Deepfake di Indonesia

Perkembangan teknologi deepfake berlangsung lebih cepat dibandingkan perkembangan regulasi yang mengaturnya. Belum ditemukan ketentuan hukum yang secara khusus mengatur definisi deepfake, batasan penggunaan yang diperbolehkan, mekanisme pelabelan konten sintesis, tanggung jawab pengembang teknologi, maupun mekanisme pemulihan hak korban. Pencatatan terhadap berbagai bahan hukum primer dan sekunder menunjukkan bahwa pendekatan yang digunakan saat ini masih bersifat umum melalui regulasi perlindungan data pribadi dan informasi elektronik. Akibatnya, terdapat ruang interpretasi yang cukup luas dalam menentukan dasar hukum yang digunakan untuk menjerat pelaku maupun memberikan perlindungan yang optimal kepada korban penyalahgunaan deepfake.¹⁰

⁸ European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)" (2024).

⁹ Doni Noviantama, "Deepfake: A Review from The Victimology Perspective," *CONTEMPORARY ISSUES IN CRIMINAL LAW* 1, no. 2 (2025): 107–28, <https://doi.org/https://doi.org/10.20885/CICL>.

¹⁰ Verma, "Digital Deception: The Impact of Deepfakes on Privacy Rights."

Pembahasan

Perkembangan teknologi deepfake menunjukkan adanya perubahan mendasar dalam pola pelanggaran hukum di ruang digital. Apabila sebelumnya pelanggaran terhadap identitas seseorang lebih banyak dilakukan melalui pemalsuan dokumen atau penyalahgunaan informasi secara konvensional, maka keberadaan teknologi kecerdasan buatan telah menghadirkan bentuk manipulasi yang jauh lebih kompleks. Deepfake tidak hanya menciptakan informasi palsu, tetapi juga mampu membentuk suatu realitas digital yang tampak meyakinkan sehingga masyarakat mengalami kesulitan dalam membedakan antara informasi asli dan hasil rekayasa. Kondisi tersebut menyebabkan pendekatan hukum yang hanya berorientasi pada tindakan penyebaran informasi palsu menjadi tidak lagi memadai karena akar permasalahannya telah dimulai sejak tahap pengumpulan dan pemrosesan data pribadi seseorang tanpa persetujuan. Dalam perspektif hukum perlindungan data pribadi, penggunaan foto, suara, video, maupun karakteristik biometrik seseorang sebagai bahan pembentukan deepfake menunjukkan bahwa teknologi tersebut memiliki hubungan langsung dengan konsep pengendalian data oleh pemilik data pribadi. Data pribadi pada dasarnya bukan hanya sekadar informasi administratif mengenai seseorang, tetapi merupakan bagian dari identitas yang melekat pada individu dan memiliki nilai hukum. Oleh karena itu, ketika data tersebut digunakan untuk membangun representasi digital baru tanpa persetujuan pemiliknya, tindakan tersebut tidak hanya berkaitan dengan penyalahgunaan teknologi, tetapi juga merupakan bentuk penghilangan kontrol individu terhadap identitas digitalnya sendiri.¹¹

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar normatif mengenai hak subjek data pribadi untuk memperoleh perlindungan terhadap penggunaan data yang tidak sah. Undang-undang tersebut mengatur bahwa pemrosesan data pribadi harus dilakukan berdasarkan prinsip kehati-hatian, tujuan yang jelas, serta persetujuan dari pemilik data. Namun, apabila dikaitkan dengan karakteristik deepfake, regulasi tersebut masih memiliki keterbatasan karena belum memberikan pengaturan khusus mengenai penggunaan data biometrik atau identitas digital sebagai bahan pembuatan konten sintesis berbasis kecerdasan buatan. Dengan demikian, meskipun UU PDP dapat digunakan sebagai dasar perlindungan terhadap korban, regulasi tersebut belum sepenuhnya menjawab kompleksitas permasalahan deepfake yang memiliki karakteristik berbeda dengan bentuk pelanggaran data pribadi pada umumnya. Permasalahan tersebut menunjukkan adanya kesenjangan antara perkembangan teknologi dengan kemampuan hukum dalam memberikan perlindungan. Hukum pada dasarnya bersifat responsif terhadap perubahan sosial, tetapi perkembangan artificial intelligence generatif berlangsung jauh lebih cepat dibandingkan proses pembentukan regulasi. Akibatnya, hukum positif Indonesia saat ini masih menggunakan pendekatan interpretatif terhadap kasus deepfake, yaitu dengan menghubungkan perbuatan tersebut dengan ketentuan mengenai penyalahgunaan data pribadi, distribusi informasi elektronik yang merugikan, maupun pencemaran nama baik. Pendekatan demikian memang memberikan ruang penegakan hukum, tetapi belum memberikan kepastian hukum yang optimal karena belum terdapat batasan yang jelas mengenai definisi deepfake, bentuk pelanggaran, tanggung jawab penyedia teknologi, serta mekanisme pemulihan korban.

Apabila dibandingkan dengan penelitian sebelumnya, penelitian Rizky Karo Karo dan Zein Jiddan menegaskan bahwa penyalahgunaan deepfake memiliki keterkaitan dengan pelanggaran terhadap perlindungan data pribadi berdasarkan UU ITE dan UU PDP. Namun, penelitian tersebut lebih menitikberatkan pada aspek penyalahgunaan data pribadi sebagai

¹¹ Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP (Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law)."

bentuk pelanggaran hukum. Berbeda dengan penelitian ini, analisis tidak hanya melihat deepfake sebagai persoalan privasi data, tetapi juga menghubungkannya dengan kerusakan reputasi digital sebagai akibat lanjutan dari penggunaan data pribadi secara tidak sah.¹² Hal tersebut menjadi penting karena dalam praktiknya, kerugian korban deepfake tidak berhenti pada hilangnya kendali terhadap data pribadi, tetapi berkembang menjadi kerugian sosial, profesional, bahkan ekonomi akibat persepsi publik yang terbentuk dari konten manipulatif tersebut. Reputasi digital dalam konteks masyarakat modern memiliki kedudukan yang semakin penting karena identitas seseorang saat ini tidak hanya dibangun melalui interaksi langsung, tetapi juga melalui keberadaan dan aktivitasnya dalam ruang digital. Penyebaran konten deepfake menyebabkan seseorang dapat dikaitkan dengan tindakan, pernyataan, atau perilaku yang tidak pernah dilakukan sebelumnya. Permasalahan utamanya bukan hanya terletak pada keberadaan informasi palsu tersebut, tetapi pada kemampuan teknologi digital dalam memperluas jangkauan dan mempercepat penyebarannya. Sekalipun suatu konten kemudian dinyatakan palsu, dampak terhadap reputasi korban sering kali telah terjadi karena masyarakat telah membentuk persepsi berdasarkan informasi awal yang diterima.¹³

Temuan tersebut sejalan dengan pandangan Chesney dan Citron yang menjelaskan bahwa deepfake merupakan ancaman serius terhadap privasi, demokrasi, dan keamanan nasional karena teknologi ini mampu menciptakan manipulasi yang sulit dibedakan dari kenyataan.¹⁴ Ancaman deepfake tidak hanya berkaitan dengan penciptaan informasi palsu, tetapi juga berkaitan dengan kemampuan teknologi tersebut dalam merusak kepercayaan publik terhadap suatu informasi digital. Dalam konteks Indonesia, kondisi ini menjadi semakin relevan karena tingginya penggunaan media sosial menyebabkan suatu konten dapat menyebar secara cepat sebelum proses verifikasi dilakukan. Selain berdampak terhadap individu, penyalahgunaan deepfake juga memiliki implikasi terhadap kepentingan publik. Penggunaan deepfake dalam konteks politik, misalnya, menunjukkan bahwa teknologi ini dapat digunakan untuk memengaruhi opini masyarakat melalui manipulasi suara maupun visual tokoh tertentu. Fenomena tersebut menunjukkan bahwa deepfake bukan hanya persoalan privat antara pelaku dan korban, tetapi juga dapat mengganggu kepercayaan masyarakat terhadap informasi digital secara keseluruhan. Oleh karena itu, kebutuhan terhadap pengaturan khusus mengenai deepfake tidak hanya didasarkan pada perlindungan individu, tetapi juga sebagai upaya menjaga integritas ruang digital.

Jika dibandingkan dengan perkembangan regulasi internasional, beberapa negara mulai membangun pendekatan hukum yang lebih adaptif terhadap penggunaan kecerdasan buatan. Uni Eropa melalui Artificial Intelligence Act telah memperkenalkan pendekatan berbasis risiko dengan memberikan kewajiban transparansi terhadap penggunaan sistem AI tertentu, termasuk kewajiban pemberian informasi terhadap konten yang dihasilkan atau dimodifikasi menggunakan teknologi kecerdasan buatan. Pendekatan tersebut menunjukkan bahwa regulasi terhadap AI tidak hanya berfokus pada larangan penggunaan teknologi, tetapi juga menciptakan mekanisme akuntabilitas agar masyarakat dapat mengetahui ketika berhadapan dengan konten sintesis.¹⁵ Berdasarkan perbandingan tersebut, Indonesia memiliki kebutuhan untuk mengembangkan regulasi yang lebih spesifik mengenai deepfake. Regulasi tersebut tidak harus dipahami sebagai pembatasan terhadap perkembangan teknologi kecerdasan buatan, melainkan sebagai mekanisme pengendalian agar teknologi digunakan secara bertanggung jawab. Pengaturan khusus deepfake idealnya mencakup beberapa aspek, yaitu pemberian

¹² Karo Karo, Jiddan, and Buono, "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia."

¹³ Noviantama, "Deepfake: A Review from The Victimology Perspective."

¹⁴ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

¹⁵ European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).

definisi hukum mengenai deepfake, klasifikasi penggunaan yang diperbolehkan dan dilarang, kewajiban transparansi terhadap konten hasil AI, tanggung jawab pihak yang membuat maupun menyebarkan konten manipulatif, serta mekanisme pemulihan bagi korban yang mengalami kerugian. Dengan demikian, hasil penelitian ini menunjukkan bahwa urgensi pengaturan deepfake di Indonesia tidak hanya muncul karena adanya kekosongan norma hukum, tetapi juga karena adanya perubahan karakteristik pelanggaran hukum di era kecerdasan buatan. Deepfake telah mempertemukan dua kepentingan hukum yang saling berkaitan, yaitu perlindungan terhadap data pribadi sebagai dasar pembentukan identitas digital dan perlindungan terhadap reputasi digital sebagai bentuk perlindungan terhadap kehormatan individu dalam ruang siber. Kebaruan penelitian ini terletak pada pendekatan yang mengintegrasikan kedua aspek tersebut dalam satu analisis hukum, sehingga pengaturan deepfake tidak hanya dipandang sebagai persoalan teknologi, tetapi sebagai persoalan perlindungan hak individu dalam perkembangan masyarakat digital.

KESIMPULAN

Berdasarkan hasil penelitian mengenai urgensi pengaturan deepfake dalam perlindungan data pribadi dan reputasi digital di Indonesia, dapat disimpulkan bahwa perkembangan teknologi kecerdasan buatan telah menciptakan bentuk baru permasalahan hukum yang belum sepenuhnya mampu dijangkau oleh regulasi yang berlaku. Teknologi deepfake tidak hanya menjadi persoalan manipulasi informasi digital, tetapi juga berkaitan erat dengan penggunaan data pribadi seseorang sebagai dasar pembentukan konten sintetis serta potensi kerusakan terhadap reputasi digital korban. Kondisi tersebut menunjukkan bahwa pengaturan hukum yang saat ini tersedia melalui Undang-Undang Pelindungan Data Pribadi dan regulasi informasi elektronik masih memiliki keterbatasan karena belum mengatur secara khusus mengenai karakteristik, mekanisme penyalahgunaan, serta tanggung jawab hukum terhadap penggunaan teknologi deepfake. Temuan utama dalam penelitian ini menunjukkan bahwa deepfake memiliki karakter pelanggaran hukum yang bersifat ganda, yaitu pelanggaran terhadap hak individu atas kendali data pribadi sekaligus ancaman terhadap kehormatan dan reputasi seseorang dalam ruang digital. Oleh karena itu, pendekatan hukum terhadap deepfake tidak dapat hanya ditempatkan dalam perspektif perlindungan data pribadi maupun penegakan hukum terhadap konten elektronik secara terpisah, melainkan membutuhkan suatu konsep pengaturan yang mengintegrasikan perlindungan identitas digital dan perlindungan reputasi digital secara bersamaan. Konsep tersebut menjadi kebaruan penelitian ini, yaitu menempatkan deepfake sebagai bentuk perkembangan teknologi yang membutuhkan kerangka hukum khusus berbasis perlindungan hak digital manusia, bukan sekadar sebagai bentuk penyalahgunaan teknologi informasi.

Penelitian ini memiliki keterbatasan karena menggunakan pendekatan yuridis normatif yang berfokus pada kajian terhadap regulasi, doktrin hukum, serta literatur yang relevan, sehingga belum mengkaji secara mendalam aspek empiris mengenai pengalaman korban, pola penegakan hukum, maupun kesiapan institusi terkait dalam menangani kasus deepfake di Indonesia. Oleh karena itu, penelitian selanjutnya diharapkan dapat memperluas kajian melalui pendekatan empiris dengan melihat praktik penanganan kasus, perspektif aparat penegak hukum, penyelenggara platform digital, serta masyarakat sebagai pengguna teknologi agar diperoleh gambaran yang lebih komprehensif mengenai kebutuhan regulasi deepfake di Indonesia. Penulis menyampaikan ucapan terima kasih kepada pihak-pihak yang telah memberikan dukungan dalam pelaksanaan penelitian ini, khususnya dosen pengampu mata kuliah hukum siber Ibu Dewi Pika Lumban Batu, Program Studi Hukum Bisnis Fakultas Ilmu Sosial Universitas Negeri Medan, serta seluruh pihak yang telah membantu dalam proses penyusunan artikel ilmiah ini.

DAFTAR PUSTAKA

- Arvitto, Rafi Satrya. "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP (Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law)." *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia (JIHAM)* 4, no. 2 (2025): 78–82. <https://doi.org/https://doi.org/10.35912/jihham.v4i2.3937>.
- Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753–1820. <https://doi.org/https://doi.org/10.15779/Z38RVOD15J>.
- European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (2024).
- Haida, Rendi Syaputra Nur, and Eko Nutriyatman. "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (AI) Dari Perspektif Hukum Pidana Indonesia." *Jurnal Respublica* 24, no. 1 (2024). <https://doi.org/https://doi.org/10.31849/respublica.v24i01.23327>.
- Karo Karo, Rizky, Zein Jiddan, and Hannan Atanto Bueno. "Analisis Dalam Kasus Penyalahgunaan Deepfake Dari Segi Perlindungan Data Pribadi Dalam UU ITE Dan UU PDP Di Indonesia." *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, Dan Hukum (SENPISHUM)* 1, no. 1 (2026).
- Muhtadi, Burhanuddin, and Maria Monica Wihardja. "Deepfakes and Selective Belief: How Partisanship Affects Voters' Exposure and Susceptibility to Deepfake Content," 2024.
- Noviantama, Doni. "Deepfake: A Review from The Victimology Perspective." *CONTEMPORARY ISSUES IN CRIMINAL LAW* 1, no. 2 (2025): 107–28. <https://doi.org/https://doi.org/10.20885/CICL>.
- Silalahi, Wilma, Meily Natassya, and Shane Evelina. "Penggunaan Deepfake Terkait Penyebaran Isu Hoaks Pada Masa Kampanye Pemilu 2024." *Jurnal Bawaslu Provinsi Kepulauan Riau* 6, no. 1 (2024).
- Verma, Karishma. "Digital Deception: The Impact of Deepfakes on Privacy Rights." *LEX SCIENTIA LAW REVIEW* 8, no. 2 (2024): 856–96.