

**IMPLIKASI HUKUM TENTANG PENYALAHGUNAAN TEKNOLOGI DEEFAKE
TERHADAP KEJAHATAN IDENTITAS DIGITAL****Nabila Aprillia, Dian Ratu Ayu Uswatun Khasanah, Ronald Jolly Pongantung**

Prodi Ilmu Hukum, Administrasi Publik, FHSIP, Universitas Terbuka

e-mail : nabilaaprillia025@gmail.com**ABSTRAK**

Perkembangan teknologi kecerdasan buatan telah melahirkan teknologi deepfake yang berpotensi disalahgunakan untuk merusak identitas digital seseorang. Penelitian ini bertujuan untuk menganalisis modus penyalahgunaan teknologi deepfake di Indonesia, menelaah implikasi hukumnya berdasarkan peraturan perundang-undangan yang berlaku, serta mengkaji urgensi pengaturan khusus terhadap deepfake dalam sistem hukum Indonesia. Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif dengan pendekatan perundang-undangan dan konseptual, serta pengumpulan data dilakukan melalui studi pustaka terhadap bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa penyalahgunaan deepfake dapat berupa penyebaran video palsu, pemalsuan wajah, dan penipuan berbasis identitas digital yang merugikan korban baik secara sosial, hukum, maupun psikologis. Meskipun beberapa pasal dalam UU ITE, UU Perlindungan Data Pribadi, dan KUHP dapat digunakan untuk menjerat pelaku, regulasi tersebut belum secara khusus dan eksplisit mengatur karakteristik serta aspek teknis dari kejahatan berbasis deepfake. Hal ini menimbulkan hambatan dalam penegakan hukum dan perlindungan korban. Maka dari itu, diperlukan pembentukan regulasi khusus atau amandemen undang-undang yang ada agar sistem hukum di Indonesia mampu merespons tantangan teknologi deepfake secara tepat, adil, dan efektif.

Kata Kunci : Deepfake, Identitas Digital, Implikasi Hukum.**ABSTRACT**

The development of artificial intelligence technology has given birth to deepfake technology which has the potential to be misused to damage a person's digital identity. This research aims to analyze the mode of misuse of deepfake technology in Indonesia, examine its legal implications based on applicable laws and regulations, and examine the urgency of special regulation of deepfake in the Indonesian legal system. Applicable, as well as examining the urgency of special arrangements against deepfake in the Indonesian legal system. The research method used is normative juridical legal research with statutory and conceptual approaches, and data collection is carried out through literature study of primary, secondary, and tertiary legal materials tertiary. The results show that deepfake abuse can take the form of spreading fake videos, face forgery and digital identity-based fraud that

harms victims socially, legally and psychologically. Although several articles in the ITE Law, Personal Data Protection Law, and Criminal Code can be used to charge perpetrators, these regulations have not specifically and explicitly regulated the characteristics and technical aspects of deepfake-based crimes. This creates obstacles in law enforcement and victim protection. Therefore, it is necessary to establish special regulations or amend existing laws so that the legal system in Indonesia is able to answer the challenges of deepfake technology appropriately, fairly, and effectively.

Keywords : Deepfake, Digital Identity, Legal Implications.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa berbagai inovasi yang mempengaruhi hampir seluruh aspek kehidupan manusia. Salah satu inovasi yang kini menjadi sorotan adalah teknologi *deepfake*, yaitu suatu teknik manipulasi media visual dan audio yang menggunakan kecerdasan buatan (*artificial intelligence*) untuk menciptakan konten yang menyerupai individu nyata secara sangat meyakinkan. Teknologi ini memungkinkan seseorang untuk membuat video atau rekaman suara yang seolah-olah diucapkan oleh orang lain, padahal tidak pernah terjadi di dunia nyata.¹ Meski memiliki potensi positif dalam dunia hiburan dan industri kreatif, penggunaannya yang tidak etis dan tanpa izin telah memunculkan banyak persoalan, terutama dari aspek hukum dan perlindungan identitas.

Identitas digital kini menjadi bagian tak terpisahkan dari kehidupan masyarakat modern. Identitas ini mencakup berbagai elemen seperti nama, foto, video, suara, tanda tangan elektronik, hingga jejak aktivitas daring. Dalam konteks ini,

identitas digital dapat dikatakan sebagai representasi diri seseorang dalam dunia maya.² Namun, perkembangan teknologi deepfake telah membuka celah bagi penyalahgunaan identitas digital yang berujung pada berbagai kejahatan siber, seperti pencemaran nama baik, penipuan, pemerasan, dan pelanggaran privasi.

Fenomena penyalahgunaan teknologi *deepfake* telah menimbulkan kekhawatiran global, termasuk di Indonesia. Banyak kasus yang menunjukkan bagaimana teknologi ini digunakan untuk memalsukan pernyataan publik tokoh masyarakat, membuat video porno palsu yang merusak reputasi seseorang, atau menyebarkan hoaks yang merugikan pihak-pihak tertentu.³ Di sinilah letak urgensinya, ketika identitas digital seseorang bisa dimanipulasi dengan mudah, maka perlindungan hukum terhadap individu pun menjadi tantangan besar. Permasalahan ini menjadi semakin kompleks karena teknologi *deepfake* dapat dibuat dan disebar oleh siapa saja, bahkan tanpa keterampilan teknis yang tinggi. Berbagai aplikasi dan perangkat lunak berbasis AI kini tersedia secara luas

¹ (Faqih & Soerjati Priowirjanto, 2022, p.2)

² (Husna et al., 2024, p.45)

³ (Amanda et al., 2024, p.181)

dan mudah diakses, sehingga potensi penyalahgunaannya pun meningkat.

Hal ini sejalan dengan pendapat⁴ yang menyatakan bahwa *deepfake* membuat kehidupan kedepan menjadi serba tidak pasti. Kita sudah tidak bisa lagi memercayai apa yang kita lihat dan apa yang kita dengar. Teknologi akan membawa kita ke arah yang tidak pernah kita bayangkan sebelumnya. Situasi ini menuntut adanya langkah-langkah preventif dan kuratif dari sisi regulasi dan penegakan hukum agar ruang digital tidak menjadi medan yang bebas dari tanggung jawab hukum.

Dengan latar belakang tersebut, penelitian ini menjadi penting untuk mengkaji bagaimana implikasi hukum dari penggunaan teknologi *deepfake* terhadap penyalahgunaan identitas digital di Indonesia. Fokus kajian diarahkan pada perlindungan hukum terhadap individu yang identitasnya disalahgunakan, efektivitas regulasi yang ada, serta kebutuhan akan pembentukan norma hukum baru yang lebih spesifik. Kajian ini diharapkan mampu memberikan kontribusi terhadap pengembangan hukum siber di Indonesia yang adaptif terhadap kemajuan teknologi.

Melalui penelitian ini, diharapkan pula dapat meningkatkan kesadaran masyarakat terhadap bahaya penyalahgunaan teknologi *deepfake*, sekaligus mendorong pemerintah dan pemangku kepentingan untuk memperkuat perlindungan hukum dalam ranah digital. Tanpa perlindungan yang memadai, ruang siber akan semakin rentan terhadap kejahatan berbasis manipulasi identitas, dan hal ini bisa berdampak serius terhadap

kehidupan sosial, ekonomi, dan hukum di masa mendatang.

METODE PENELITIAN

Jenis penelitian ini adalah penelitian hukum normatif atau yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) yaitu penelitian yang dilakukan dengan menelaah bahan-bahan hukum seperti peraturan perundang-undangan, putusan pengadilan, doktrin, serta literatur hukum yang relevan. Penelitian ini bersifat kualitatif deskriptif, karena bertujuan untuk memberikan gambaran secara sistematis mengenai konsep identitas digital, bentuk penyalahgunaan teknologi *deepfake*, dan perlindungan hukum yang berlaku di Indonesia.

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis kualitatif, yaitu dengan mendeskripsikan, menafsirkan, dan mengkaji permasalahan berdasarkan data yang diperoleh dari bahan hukum. Analisis ini dilakukan secara sistematis untuk menemukan jawaban atas rumusan masalah, mengaitkan teori dengan norma hukum positif, serta memberikan argumentasi hukum yang logis dan kritis terhadap isu yang dibahas.

HASIL DAN PEMBAHASAN

Konsep Teknologi *Deepfake* dan Identitas Digital

Teknologi *deepfake* merupakan bentuk kemajuan dari kecerdasan buatan (*Artificial Intelligence/AI*), khususnya dalam bidang *deep learning*, yang digunakan untuk memanipulasi konten visual dan audio secara sangat realistis. Istilah “*deepfake*” berasal dari gabungan

⁴ (Khusna & Pangestuti Sri, 2019, p.18)

kata *deep learning* dan *fake* (palsu), yang mencerminkan teknik manipulasi data digital dengan memanfaatkan algoritma *neural networks*. Teknologi ini bekerja dengan mempelajari pola wajah, ekspresi, dan suara seseorang dari berbagai sumber data (misalnya foto atau video), kemudian menirukannya secara meyakinkan dalam sebuah video yang tampak seolah-olah asli.⁵

Teknologi ini mulai dikenal luas di kalangan akademisi pada tahun 2016, ketika Justus Thies dan timnya mempresentasikan hasil penelitian mereka dalam sebuah konferensi tentang visi komputer dan pengenalan pola. Dalam penelitian tersebut, mereka menunjukkan bagaimana wajah seseorang (disebut sebagai sumber) dapat digunakan untuk mengendalikan ekspresi wajah orang lain (disebut sebagai target) dalam sebuah video.

Hasilnya, video tersebut tampak sangat nyata, seolah-olah wajah target benar-benar meniru ekspresi dan gerakan wajah sumber.⁶ Meskipun pada awalnya digunakan untuk keperluan hiburan, film, dan kreativitas digital, teknologi ini dengan cepat berkembang dan kini rentan disalahgunakan untuk kejahatan, termasuk penipuan, pemerasan, pencemaran nama baik atau peretasan akun pribadi. Oleh karena itu, penting untuk memahami konsep identitas digital secara utuh.

Identitas digital merupakan bentuk identifikasi elektronik seseorang yang terdiri dari dua elemen penting, yaitu kunci publik yang dapat diakses secara terbuka dan kunci privat yang bersifat rahasia. Dalam praktiknya, identitas digital dapat berbentuk QR Code yang menyimpan data

pribadi dan dapat digunakan di berbagai perangkat digital. Identitas ini mencakup seluruh informasi pribadi seperti nama, foto, tanda tangan digital, alamat email, hingga rekam jejak aktivitas online, dan memiliki kedudukan yang sangat penting dalam ruang siber karena menjadi dasar autentikasi, akses layanan, dan interaksi daring.⁷

Secara sederhana, identitas digital dapat dipahami sebagai sekumpulan data mengenai individu atau entitas yang tersedia dan dapat diakses secara daring. Tidak seperti identitas fisik seperti KTP atau paspor yang terbatas pada bentuk fisik dan wilayah tertentu, identitas digital memungkinkan proses autentikasi dari mana saja melalui platform digital yang terkoneksi. Oleh karena itu, identitas digital memiliki kedudukan yang sangat penting dalam dunia maya karena menjadi dasar bagi eksistensi dan perlindungan hak-hak individu dalam berbagai layanan berbasis teknologi.

Modus Penyalahgunaan Deepfake di Indonesia

Penyalahgunaan teknologi *deepfake* di Indonesia menunjukkan tren yang mengkhawatirkan karena kemampuannya yang canggih dalam memanipulasi konten digital. Bentuk-bentuk penyalahgunaan yang umum terjadi meliputi penyebaran video palsu yang menyerupai tokoh publik, pemalsuan wajah untuk konten pornografi non-konsensual, penipuan berbasis identitas palsu, hingga penggiringan opini publik dengan konten manipulatif. Dalam kasus tertentu, wajah atau suara seseorang dapat ditempelkan ke video yang mengandung ujaran kebencian, konten

⁵ (Latifatunnisa & Yudha, 2025, p.2)

⁶ (Mutmainnah et al., 2024, p.69)

⁷ (Zahra et al., 2024, p.87)

asusila, atau pernyataan yang sebenarnya tidak pernah diucapkan oleh orang tersebut. Konten semacam ini sangat merugikan, karena selain merusak reputasi korban, juga dapat memicu keresahan sosial.

Salah satu kasus nyata yang sempat menjadi perhatian publik di Indonesia adalah dugaan video asusila yang menyeret nama seorang selebritas ternama. Menanggapi keramaian tersebut, pihak kepolisian telah melakukan pemeriksaan pada video tersebut dan telah memastikan bahwa video mirip selebritas tersebut merupakan hasil rekayasa. Dengan kata lain, wajah pemeran yang terdapat dalam video asusila tersebut merupakan hasil penyuntingan yang dilakukan oleh seseorang agar menyerupai sang selebritas. Pihak kepolisian telah menilai bahwa rekayasa itu memanfaatkan teknologi *deepfake*.⁸

Kabar terbaru juga terdapat dugaan pelecehan seksual secara daring yang melibatkan mahasiswa di sebuah Universitas, yang mana pelaku diduga mengambil foto dari media sosial lalu digabungkan secara realistis ke dalam video atau gambar pornografi. Pelaku diduga menggunakan perangkat lunak berbasis kecerdasan buatan yang kini mudah diakses publik. Teknologi *deepfake* memungkinkan pembuatan konten visual palsu yang sulit dibedakan dari aslinya. Aksi ini dilakukan secara diam-diam, dan kontennya disebarluaskan melalui jaringan tertutup hingga akhirnya bocor ke publik.⁹ Kasus ini menunjukkan betapa mudahnya

teknologi tersebut digunakan untuk menciptakan konten palsu yang merugikan korban.

Pada kasus terbaru¹⁰ memaparkan dalam artikel berita terbarunya bahwa pengadilan mulai menyidangkan kasus penyebaran video palsu bermuatan penipuan yang menyeret nama Presiden Republik Indonesia dan tokoh nasional lainnya. Modus yang digunakan terdakwa melibatkan video rekayasa digital dengan menampilkan wajah Presiden Prabowo Subianto yang tampak mengajak masyarakat untuk menghubungi nomor tertentu guna mendapatkan bantuan dana. Korban yang terpedaya kemudian diminta mentransfer uang sebagai syarat administrasi, seperti biaya pajak dan pendaftaran. Kerugian yang ditimbulkan dari penipuan ini ditaksir mencapai puluhan juta rupiah, dengan jumlah korban yang terus berkembang. (dikutip dalam *detikSumbagSel*, 2025)

Di tingkat global, teknologi *deepfake* juga telah digunakan dalam skema penipuan korporat, di mana suara eksekutif perusahaan dipalsukan untuk mengelabui pegawai agar mentransfer dana ke akun pelaku. Meskipun belum banyak dilaporkan secara terbuka di Indonesia, potensi kasus semacam ini bisa saja terjadi, mengingat akses terhadap teknologi *deepfake* kini semakin mudah melalui berbagai aplikasi berbasis *AI* yang tersedia secara gratis di internet.

Kerentanan terhadap penyalahgunaan *deepfake* sangat tinggi

⁸ Zulfikar Hardiansyah and Reska K Nistanto, 'Selebriti Dan Tokoh Publik Yang Jadi Korban Video Deepfake Selain Nagita Slavina', *Kompas.Com*, 2022 <<https://tekno.kompas.com/read/2022/01/19/13160047/selebriti-dan-tokoh-publik-yang-jadi-korban-video-deepfake-selain-nagita?page=all>>.

⁹ Rolandus Nampu, 'Universitas Udayana Investigasi Kasus Dugaan Pelecehan Seksual Daring', *Antaranews*, 2025 <<https://kalsel.antaranews.com/rilis-pers/4802537/universitas-udayana-investigasi-kasus-dugaan-pelecehan-seksual-daring>>.

¹⁰ Saputra (2025)

karena dua faktor utama yakni, kecanggihan teknologi dan rendahnya literasi digital masyarakat. Teknologi *deepfake* terus berkembang menjadi lebih halus dan sulit dibedakan dari konten asli, sehingga masyarakat awam sulit mengenali manipulasi yang terjadi. Selain itu, keterbukaan akses terhadap data pribadi melalui media sosial seperti foto dan video yang dibagikan secara bebas juga memperbesar peluang terjadinya penyalahgunaan. Kelompok yang paling rentan menjadi korban umumnya adalah publik figur, tokoh politik, pejabat publik, dan perempuan, terutama karena eksistensi mereka di ruang digital sering terekspos luas. Namun, masyarakat umum pun tidak luput dari ancaman ini, terutama jika data pribadi mereka tersebar dan digunakan tanpa izin.

Dengan tingkat kemudahan akses teknologi *deepfake* dan minimnya regulasi khusus yang mengaturnya, penyalahgunaan identitas digital melalui media manipulatif ini berpotensi menjadi bentuk kejahatan siber yang semakin marak. Oleh karena itu, pemahaman terhadap modus-modus penyalahgunaan *deepfake* perlu terus dikembangkan, tidak hanya dari sisi hukum, tetapi juga dari sisi teknologi dan edukasi digital.

Analisis Implikasi Hukum Penyalahgunaan Deepfake Menurut Peraturan Perundang-Undangan yang Berlaku

Penyalahgunaan teknologi *deepfake* dalam konteks pelanggaran identitas digital dapat dijerat dengan beberapa ketentuan hukum positif di Indonesia, meskipun hingga saat ini belum ada regulasi khusus yang secara eksplisit mengatur mengenai *deepfake*. Dalam praktiknya, penanganan hukum terhadap kejahatan ini masih

bergantung pada penyesuaian dengan peraturan perundang-undangan yang berlaku, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta Kitab Undang-Undang Hukum Pidana (KUHP).

UU ITE, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 dan perubahan melalui Undang-Undang Nomor 19 Tahun 2016, menjadi instrumen hukum utama yang digunakan dalam menindak kejahatan berbasis teknologi. Pasal 27 ayat (1) UU ITE melarang distribusi dan/atau transmisi konten yang melanggar kesusilaan, sehingga dapat digunakan untuk menjerat pelaku yang menyebarkan konten *deepfake* bernuansa asusila. Pasal 28 ayat (1) mengatur penyebaran informasi palsu yang merugikan pihak lain, relevan jika *deepfake* digunakan untuk menyebarkan hoaks atau merusak reputasi individu. Selain itu, Pasal 35 mengatur pemalsuan informasi elektronik, yang tepat digunakan untuk menangani konten *deepfake* yang memanipulasi identitas seseorang secara digital. Pasal-pasal ini diperkuat oleh Pasal 36 yang memberikan sanksi tambahan apabila perbuatan tersebut menimbulkan kerugian.

Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan dasar hukum terhadap penyalahgunaan data pribadi, termasuk data biometrik seperti wajah dan suara yang umumnya digunakan dalam teknologi *deepfake*. Penggunaan data pribadi tanpa persetujuan dapat dikategorikan sebagai pelanggaran hak subjek data dan dikenai sanksi pidana maupun administratif sebagaimana diatur dalam Pasal 65 sampai Pasal 70 UU PDP.

Selain kedua undang-undang tersebut, KUHP juga memiliki beberapa pasal yang dapat digunakan untuk menjerat pelaku penyalahgunaan *deepfake*, meskipun masih bersifat konvensional. Pasal 263 KUHP tentang pemalsuan dokumen dapat dikenakan apabila konten *deepfake* digunakan untuk meniru identitas orang lain demi keuntungan pribadi atau merugikan orang lain. Pasal 311 KUHP tentang pencemaran nama baik dapat berlaku apabila konten *deepfake* digunakan untuk menyebarkan fitnah atau merusak reputasi seseorang secara terbuka. Sementara itu, Pasal 378 KUHP tentang penipuan dapat diterapkan jika *deepfake* digunakan untuk mengelabui korban, misalnya dalam kasus penipuan digital berbasis video palsu.

Urgensi Pengaturan Hukum Khusus Terhadap Deepfake di Indonesia

Teknologi *deepfake*, yang memanfaatkan kecerdasan buatan untuk memanipulasi konten visual dan audio, telah berkembang begitu pesat dan menghadirkan tantangan hukum yang signifikan. Meskipun Indonesia telah memiliki beberapa peraturan perundang-undangan seperti UU ITE, UU PDP, dan KUHP yang dapat digunakan untuk menjerat pelaku kejahatan berbasis teknologi informasi, hukum yang ada saat ini masih belum cukup untuk memberikan perlindungan hukum yang komprehensif dan efektif terhadap penyalahgunaan teknologi *deepfake*.

Salah satu kelemahan utama adalah tidak adanya ketentuan hukum yang secara eksplisit menyebut atau mengatur istilah “*deepfake*” maupun karakteristik khususnya sebagai bentuk konten manipulatif digital. Akibatnya, penegakan hukum terhadap kasus *deepfake* cenderung

mengandalkan interpretasi terhadap pasal-pasal umum yang belum tentu sepenuhnya relevan atau memadai dalam menjerat pelaku maupun melindungi korban. Di samping itu, aspek teknis dalam pembuktian kasus *deepfake* juga belum secara jelas diatur, sehingga menyulitkan aparat penegak hukum dalam mengungkap pelaku atau menjamin keadilan bagi korban.

Sebagai perbandingan, beberapa negara telah mulai menyusun regulasi khusus yang secara eksplisit mengatur tentang *deepfake*. Misalnya, di Amerika Serikat, beberapa negara bagian seperti Texas dan California telah mengesahkan undang-undang yang melarang penyebaran konten *deepfake* untuk tujuan politik maupun pornografi tanpa persetujuan. Di Uni Eropa, *deepfake* juga menjadi perhatian dalam kerangka kerja *Digital Services Act* (DSA) yang mewajibkan platform digital untuk mengidentifikasi dan menghapus konten manipulatif. Negara-negara ini menyadari bahwa keterlambatan dalam merespons perkembangan teknologi seperti *deepfake* dapat menimbulkan kerugian sosial dan hukum yang besar.

Jika Indonesia tidak segera merumuskan pengaturan hukum khusus terkait *deepfake*, maka akan terjadi kekosongan hukum (*legal vacuum*) yang berisiko menimbulkan ketidakpastian hukum dan lemahnya perlindungan terhadap warga negara. Tanpa dasar hukum yang jelas, pelaku penyalahgunaan *deepfake* bisa saja lolos dari jeratan hukum, sementara korban tidak memiliki perlindungan dan pemulihan yang layak.

Kekosongan hukum ini juga membuka ruang abu-abu yang rentan disalahgunakan oleh pihak-pihak tidak bertanggung jawab, terutama dalam konteks politik, ekonomi, dan privasi

digital. Oleh karena itu, pemerintah perlu segera merumuskan regulasi baru yang secara khusus mengatur tentang teknologi *deepfake*, baik dalam bentuk undang-undang tersendiri maupun sebagai bagian dari revisi UU ITE atau UU PDP.

Regulasi tersebut setidaknya harus mencakup definisi dan klasifikasi *deepfake*, bentuk-bentuk pelanggaran dan sanksinya, perlindungan hak korban, serta ketentuan pembuktian yang berbasis forensik digital. Amendemen terhadap peraturan yang ada juga menjadi alternatif, agar pasal-pasal hukum dapat menyesuaikan dengan dinamika dan risiko kejahatan digital yang muncul akibat teknologi *deepfake*.

Lebih lanjut, kolaborasi antara pemerintah, pembuat kebijakan, aparat penegak hukum, perusahaan teknologi, dan masyarakat sipil sangat penting dalam merespons isu ini. Pemerintah tidak dapat bekerja sendiri, karena penyebaran konten *deepfake* terjadi melalui berbagai platform digital yang dikelola oleh entitas swasta, baik lokal maupun global. Oleh karena itu, dibutuhkan kerja sama dalam hal pelaporan konten, pengawasan algoritma, edukasi digital, dan pengembangan alat deteksi konten manipulatif. Dengan langkah-langkah ini, pengaturan hukum terhadap *deepfake* tidak hanya akan melindungi hak-hak individu, tetapi juga menjaga integritas ruang digital Indonesia di masa depan.

PENUTUP

Kesimpulan

Penyalahgunaan teknologi *deepfake* di Indonesia telah menimbulkan ancaman serius terhadap perlindungan identitas digital, karena memungkinkan manipulasi wajah, suara, dan data pribadi seseorang untuk tujuan yang merugikan, seperti penipuan, pencemaran nama baik, hingga pelanggaran privasi. Meskipun telah ada

sejumlah peraturan seperti UU ITE, UU PDP, dan KUHP yang dapat digunakan sebagai dasar hukum, regulasi tersebut belum cukup komprehensif dan eksplisit dalam menjawab tantangan hukum yang ditimbulkan oleh teknologi *deepfake*. Oleh karena itu, diperlukan pembaruan hukum yang lebih spesifik serta peningkatan kapasitas penegakan hukum agar dapat memberikan perlindungan hukum yang efektif dan relevan di tengah kemajuan teknologi informasi yang semakin pesat.

Saran

Penelitian selanjutnya disarankan untuk mengembangkan kajian *deepfake* tidak hanya dari aspek normatif, tetapi juga melalui pendekatan empiris, seperti studi kasus atau survei terhadap korban. Selain itu, penelitian dapat diarahkan pada perbandingan regulasi *deepfake* di negara lain sebagai bahan pertimbangan pembentukan regulasi di Indonesia. Kajian lanjutan juga diharapkan mampu merumuskan model hukum yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan dan perlindungan identitas digital.

REFERENSI

Perundang-undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kitab Undang-Undang Hukum Pidana (KUHP).

Jurnal

Amanda, Sarah, Uly Sijabat, and Diana

- Lukitasari, 'Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik', *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, 13.2 (2024), pp. 179–94
- Faqih, Muhammad, and Enni Soerjati Priowirjanto, 'Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia', *Jurnal Indonesia Sosial Teknologi*, 3.11 (2022), pp. 1156–68, doi:10.36418/jist.v3i11.528
- Hardiansyah, Zulfikar, and Reska K Nistanto, 'Selebriti Dan Tokoh Publik Yang Jadi Korban Video Deepfake Selain Nagita Slavina', *Kompas.Com*, 2022 <<https://tekno.kompas.com/read/2022/01/19/13160047/selebriti-dan-tokoh-publik-yang-jadi-korban-video-deepfake-selain-nagita?page=all>>
- Husna, Asmaul, Kamaruddin Hasan, and Awaluddin Arifin, 'Identitas Dan Penciptaan Diri Di Era Disrupsi Digital', *Jurnal Ilmu Sosial Dan Ilmu Politik Malikussaleh (JSPM)*, 5.1 (2024), p. 45, doi:10.29103/jspm.v5i1.11590
- Khusna, Itsna Hidayatul, and Pangestuti Sri, 'Deepfake, Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen', *Promedia*, 2, 2019, pp. 1–24
- Latifatunnisa, Raihani, and Made Wira Yudha, 'Urgensi Pembaruan Regulasi Dalam Menanggulangi Penyalahgunaan Teknologi', *Jurnal Hukum Dan Kewarganegaraan*, 11.1 (2025), doi:10.8734/CAUSA.v1i2.3
- Mutmainnah, Anti, Awalia Marwah Suhandi, and Yusuf Tri Herlambang, 'Problematika Teknologi Deepfake Sebagai Masa Depan Hoax Yang Semakin Meningkat: Solusi Strategis Ditinjau Dari Literasi Digital', *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, 1.2 (2024), pp. 67–72, doi:10.30812/upgrade.v1i2.3702
- Nampu, Rolandus, 'Universitas Udayana Investigasi Kasus Dugaan Pelecehan Seksual Daring', *Antaraneews*, 2025 <<https://kalsel.antaraneews.com/rilis-pers/4802537/universitas-udayana-investigasi-kasus-dugaan-pelecehan-seksual-daring>>
- Saputra, Tommy, 'Kasus Video Deepfake Libatkan Presiden, Tersangka Almandela Disidangkan', *DetikSumbagSel*, 2025 <<https://www.detik.com/sumbagsel/hukum-dan-kriminal/d-7907061/kasus-video-deepfake-libatkan-presiden-tersangka-almandela-disidangkan>>
- Zahra, Nabilla, Recca Ayu Hapsari, and Melisa Safitri, 'Perlindungan Hukum Teknologi Identitas Digital Melalui Sistem Verifikasi Identitas Berbasis Biometrik', *Supremasi: Jurnal Pemikiran Dan Penelitian Ilmu-Ilmu Sosial, Hukum, & Pengajarannya*, XIX.1 (2024), pp. 86–98

Website

- Hardiansyah, Z., & Nistanto, R. K. (2022). *Selebriti dan Tokoh Publik yang Jadi Korban Video Deepfake Selain Nagita Slavina*. Kompas.Com. <https://tekno.kompas.com/read/2022/01/19/13160047/selebriti-dan-tokoh-publik-yang-jadi-korban-video-deepfake-selain-nagita?page=all>
- Nampu, R. (2025). *Universitas Udayana investigasi kasus dugaan pelecehan*

seksual daring. Antaranews.
<https://kalsel.antaranews.com/rilis-pers/4802537/universitas-udayana-investigasi-kasus-dugaan-pelecehan-seksual-daring>

Saputra, T. (2025). *Kasus Video Deepfake Libatkan Presiden, Tersangka Almandela Disidangkan.* DetikSumbagSel.
<https://www.detik.com/sumbagsel/hukum-dan-kriminal/d-7907061/kasus-video-deepfake-libatkan-presiden-tersangka-almandela-disidangkan>