Analisis dalam Kasus Penyalahgunaan Deepfake dari Segi Perlindungan Data Pribadi dalam UU ITE dan UU PDP di Indonesia

Rizky Karo Karo[1*], Zein Jiddan[1], Hanan Atanto Buono[1]

[1]Fakultas Hukum Universitas Dirgantara Marsekal Surydarma, Jakarta.
*Alamat email penulis koresponden: rizkykarokaro@unsurya.ac.id

Abstrak

Perkembangan teknologi digital, khususnya teknologi deepfake, menghadirkan tantangan serius terhadap perlindungan hak privasi di Indonesia. Teknologi ini memungkinkan manipulasi citra dan suara seseorang secara realistis sehingga berpotensi digunakan untuk kejahatan, pencemaran nama baik, dan pelanggaran privasi. Namun, dalam hukum positif Indonesia, belum terdapat aturan khusus yang secara tegas mengatur mengenai penyalahgunaan teknologi deepfake. Penelitian ini bertujuan untuk mengkaji hakikat perlindungan hak privasi di Indonesia dan menelaah bagaimana perlindungan hukum terhadap penyalahgunaan teknologi deepfake. Metode yang digunakan adalah metode yuridis normatif dengan pendekatan peraturan perundang-undangan, konseptual dan kasus. Hasil penelitian menunjukkan bahwa hak privasi merupakan hak konstitusional dan hak asasi manusia yang diakui dalam Pasal 28G ayat (1) UUD NRI 1945. Bahkan hak privasi merupakan salah Hak Asasi Manusia bersifat universal yang diakui dalam Deklarasi Universal Hak Asasi Manusia 1948 dan ICCPR. Saat ini, perlindungan hukum terhadap penyalahgunaan Deepfake masih bersifat terbatas dan bersandar pada interpretasi UU ITE dan KUHP. Oleh karena itu, perlu pembentukan norma hukum baru yang secara eksplisit mengatur penyalahgunaan. teknologi Deepfake guna memberikan perlindungan maksimal terhadap hak privasi warga negara.

Kata Kunci: Hak Privasi, Deepfake, Perlindungan Hukum, FH Unsurya,

Abstract

The rapid advancement of digital technology, particularly Deepfake technology, presents a serious challenge to the protection of privacy rights in Indonesia. This technology enables the realistic manipulation of an individual's image and voice, potentially leading to crimes, defamation, and gross privacy violations. However, Indonesian positive law currently lacks specific regulations explicitly addressing the misuse of Deepfake technology. This study aims to examine the nature of privacy rights protection in Indonesia and to analyze the existing legal protection against the misuse of Deepfake. The research employs a normative legal methodology, drawing on statutory, conceptual, and case approaches. The findings indicate that the right to privacy is a constitutional and human right recognized under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Furthermore, privacy is considered a universal human right, acknowledged in the 1948 Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Currently, legal protection against the misuse of Deepfake technology remains limited. It relies heavily on the interpretation of the Information and Electronic Transactions Law (UU ITE) and the Criminal Code (KUHP). Therefore, the study concludes that it is necessary to establish new legal norms that explicitly regulate the misuse of Deepfake technology to provide maximal protection for citizens' privacy rights.

Keywords: Privacy Rights, Deepfake, Legal Protection, Unsurya Law Faculty

1. PENDAHULUAN

Perkembangan teknologi dalam industri digital 4.0, dimana teknologi Artificial Intelligence (AI) yang berkembang pesat yang dapat memberikan kemudahan dalam melakukan apapun. Artificial Intelligence (AI) adalah cabang dari ilmu komputer yang bertujuan membuat sistem/mesin yang meniru atau melampaui kemampuan kognitif manusia — misalnya belajar, menalar, memecahkan masalah, memahami bahasa, mengenali gambar atau suara . Deepfake adalah bentuk media sintetis di mana seseorang dalam gambar atau video yang sudah ada digantikan dengan penampilan orang lain. Istilah ini juga merujuk pada teknologi itu sendiri, yang menggabungkan "deep learning", yaitu bentuk pembelajaran mesin yang menggunakan jaringan saraf untuk pemrosesan data dan kecerdasan buatan, dengan "fake", seperti dalam istilah "fake news" . Pada dasarnya, teknologi Deepfake bergantung pada algoritma yang menganalisis data gambar dan suara asli untuk menciptakan ilusi atau kloning, seringkali membuat penonton sulit membedakan antara asli dan palsu . Sehingga menggiring opini masyarakat untuk memercayai video atau gambar yang dibuat oleh pihak yang tidak bertanggung jawab, Perkembangan teknologi Deepfake menimbulkan ancaman serius dapat digunakan menyebarkan informasi palsu atau hoax secara global serta mempengaruhi opini publik . Seperti halnya ketika terdapat video palsu yang mengandung unsur Deepfake yang menayangkan Presiden Prabowo Subianto yang melunasi utang masyarakat yang terjerat hutang pribadi, disitulah mempengaruhi opini publik bahwa video tersebut benar dan tertipu oleh pihak yang tidak bertanggung jawab dengan meminta uang kepada korban dari ratusan ribu hingga puluhan juta.

Terdapat beberapa penelitian artificial intelligence mengenai Deepfake ai dengan tema penelitian ini, pertama penelitian di amerika serikat Deepfake ai adalah Manipulasi wajah melibatkan perubahan pada fitur-fitur wajah tertentu dalam gambar, seperti warna rambut atau mata, jenis kelamin, ukuran, penampilan kacamata, dan sebagainya. Deepfakes mulai muncul di mana-mana. Teknologi Deepfake adalah pisau bermata dua yang dapat digunakan secara positif maupun negatif. Kita akan memulai dengan beberapa penggunaan positif teknologi DeepFake. Di tengah pandemi COVID-19, ketika pembuatan video pelatihan korporat dengan aktor sungguhan menjadi semakin sulit dan mahal, Deepfake juga digunakan untuk membantu mengubah efek visual wajah dalam produksi film dan televisi, menghidupkan kembali penampilan selebriti yang telah meninggal, atau memodifikasi penampilan mereka dengan menghapus ciri wajah seperti kerutan atau menambahkan kilauan pada wajah. Deepfake juga memiliki kemampuan untuk menggabungkan selebriti melintasi batas geografis dan generasional dalam lanskap kreatif . Misalnya, menggunakan teknologi Deepfake untuk menayangkan selebriti Belanda di televisi langsung, termasuk Perdana Menteri Mark Rutte dan Ratu Maxima dari Belanda. Saat ini, sebagian besar aplikasi media sosial (Instagram, Snapchat, dll.) mengubah penampilan pengguna atau untuk hiburan. Dari pertukaran wajah selebriti yang viral hingga peniruan pemimpin politik, sulit untuk membedakan antara yang asli dan palsu. Era evolusi teknologi, dan kecerdasan buatan, yang membuat Deepfake begitu mudah bagi siapa pun untuk diakses kapan pun . Berita palsu, hoaks, dan pencurian keuangan adalah beberapa aplikasi paling berbahaya dari konten deepfake. Penggunaan kecerdasan buatan dalam Deepfake membuatnya sulit untuk menentukan keaslian foto atau video, sehingga mempengaruhi kepercayaan publik terhadap sumber informasi dan keyakinan mereka terhadap apa yang mereka lihat .

Hukum diciptakan untuk mengejar ketertinggalan kemajuan teknologi. Teknolgi digunakan untuk kemakmuran rakyat, kebebasan berpendapat, kebebasan berekspresi dilindungi oleh

Undang-undang, hak kebebasan berpendapat merupakan hak asasi manusia yang dilindungi oleh Undang-undang Dasar 1945[1].

Perkembangan motif kejahatan siber yang baru ini tidak diiringi dengan perkembangan hukum positif yang dapat menjadi upaya pencegahan terjadinya kejahatan siber tersebut. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah beberapa kali melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 merupakan dasar hukum utama dalam menanggulangi berbagai bentuk kejahatan siber di Indonesia. UU ini mengatur berbagai aspek dalam pemanfaatan teknologi informasi, termasuk perlindungan data pribadi, larangan penyebaran informasi yang bersifat merugikan, serta ketentuan pidana terhadap pelanggaran dalam ruang digital . Namun, meskipun memiliki cakupan yang luas, UU ITE belum mengatur secara jelas mengenai deepfake. Sulitnya melacak pelaku yang sering menggunakan identitas palsu atau anonim, serta tidak adanya pedoman teknis khusus untuk menangani konten berbasis AI, semakin menghambat penyidik untuk memproses hukum pelaku. Oleh karena itu, diperlukan pembaruan atau revisi terhadap UU ITE yang relevan dengan perkembangan teknologi informasi terkini.

2. METODE

Metode penelitian yang digunakan adalah metode yuridis normatif menggunakan pendekatan peraturan perudang-undangan, pendekatan konseptual[2]. Pendekatan peraturan perundang-undangan yang digunakan berupa bahan hukum primer terdiri dari: 1. UU ITE; 2. UU PDP. Data yang digunakan adalah data sekunder, berupa bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Kesimpulan yang didapatkan menggunakan metode deduktif.

3. HASIL DAN PEMBAHASAN

3.1. HASIL

3.1.1. HAKIKAT HAK PRIVASI MENURUT HUKUM NASIONAL, UNDANG-UNDANG ITE DAN UNDANG-UNDANG PDP (PERLINDUNGAN DATA PRIBADI). DALAM HAK PRIVASI PENYALAHGUNAAN TEKNOLOGI *DEEPFAKE*

Fenomena penyebaran *Deepfake* non-pornografi, seperti video palsu yang menampilkan tokoh publik sedang mengatakan sesuatu yang sebenarnya tidak pernah diucapkan, atau manipulasi berita politik menjelang pemilu, menjadi bukti nyata bahwa kemajuan teknologi telah melampaui cakupan hukum yang ada[3]. Penggunaan *Deepfake* umumnya disalah-gunakan untuk penyebarluasan isu hoax, termasuk di bidang politik seperti yang dijabarkan pada kasus Presiden Joko Widodo yang seolah fasih berbahasa Mandarin. Fenomena ini bisa dimengerti

[1] Rizky Pratama Putra Karo Karo, "Hate Speech: Penyimpangan Terhadap UU ITE, Kebebasan Berpendapat Dan Nilai-Nilai Keadilan Bermartabat," *Jurnal Lemhannas RI :* 10, no. 4 (2022): 52–65, https://jurnal.lemhannas.go.id/index.php/jkl/article/view/370/242; Rizky Karo Karo, *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana*, 1st ed. (Tangerang: Penerbit Fakultas Hukum, Universitas Pelita Harapan, 2019); Teguh Prasetyo, Yuni Ginting, and Rizky Karo Karo, *Hukum Pidana - Edisi Revisi*, 1st ed. (Depok: RajaGrafindo Persada, 2023), https://www.rajagrafindo.co.id/produk/hukum-pidana-prof-dr-teguh-prasetyo-s-h-m-si-dr-yuni-priskila-ginting-s-h-m-h-rizky-karo-karo-s-h-m-h/; Susi Susantijo, "A Human Rights Perspective on Granting Privileges to Descendants of PKI in Indonesia," *Fiat Justisia: Jurnal Ilmu Hukum* 19, no. 1 (2025): 1–20.

[2] Rizky Karo Karo, *PENGANTAR METODOLOGI PENELITIAN HUKUM DI ERA DIGITAL*, 1st ed. (Depok: Raja Grafindo Persada, 2025); Bambang Widarto, Faisal Santiago, and Hj. Darwati, *Kebijakan Hukum Ideal Pengaturan Ruang Udara Indonesia Untuk Pertahanan Negara Dan Kesejahteraan Bangsa*, 1st ed. (Depok: Raja Grafindo Persada, 2025); Rizky Karo Karo and Teguh Prasetyo, "The Provision of Licensed Financial Technology Lending From The Perspective of Cyber Law and Criminal Law in Indonesia," *Pena Justisia Media Komunikasi dan Kajian Hukum* 24, no. 2 (2025): 7263–7280, https://jurnal.unikal.ac.id/index.php/hk/article/view/6559?__cf_chl_tk=i2MoqKyoZVP_9RqM49DetHTpFw33sBasZW903XevVu4-1761709716-1.0.1.1-zv92QUdHaDxMj7tWA42vZnmSSJfCKQDGeyBXIIbEPN4.

[3] Nurfaizah Ayu, "Waspadai Politik Identitas Lewat Manipulasi Opini Jelang Pemilu 2024 ", https://www.kompas.id/baca/polhuk/2023/03/02/waspadai-politik-identitas-menjelang-pemilu-2024./ diakses pada tanggal 29 oktober 2025.

dengan menelusuri asal-usul teknologi *Deepfake* yang pertama kali dikenal publik melalui Reddit pada 2017. Kala itu, seorang pengguna tanpa identitas jelas membuat forum bernama R *Deepfake* dan memposting konten pornografi yang memadukan wajah seorang artis dengan tubuh pemeran film dewasa. Sejak momen itu, video hasil manipulasi wajah menggunakan algoritma *Deepfake* mulai beredar luas[4].

Pada konteks perlindungan hukum, secara umum konstitusi mengamanatkan kepada negara untuk memberikan jaminan perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya yang merupakan bagian dari Hak Asasi Manusia sebagaimana yang disebutkan dalam Pasal 28J ayat (1) UUD NRI 1945. Sebagai implementasi dari amanat tersebut, maka diatur larangan terkait menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal dengan maksud supaya hal tersebut diketahui umum dalam bentuk informasi elektronik dan/atau dokumen elektronik yang dilakukan melalui sistem elektronik sebagaimana yang disebutkan dalam Pasal 27A UU Nomor 1 Tahun 2024. Pasal 27A tersebut memiliki implikasi pidana yang diatur dalam Pasal 45 ayat (4), di mana ancamannya pidana kurungan penjara 2 (dua) tahun dan/atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah). Di samping itu, UU PDP juga menyebutkan dalam Pasal, 66 bahwa setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Ancaman pidana terhadap pelanggaran Pasal 66 ini ialah pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah).

Namun, pengaturan dalam Pasal 27A UU ITE maupun dalam UU PDP menjadi tidak cukup kuat untuk melindungi korban dari manipulasi visual yang merusak citra dan integritasnya, karena elemen ”penghinaan” atau ”pencemaran” yang didefinisikan secara konvensional belum tentu dapat diterapkan pada teknologi manipulatif seperti deepfake. Bahkan definisi AI serta *Deepfake* sampai saat ini belum dijelaskan dalam peraturan perundang-undangan. Oleh karena itu, diperlukan pendekatan hukum baru yang tidak hanya berfokus pada bentuk konten (tulisan atau ucapan), tetapi juga pada substansi manipulasi visual dan dampaknya terhadap persepsi publik. Ini menunjukkan pentingnya pembaruan hukum yang lebih adaptif terhadap bentuk-bentuk kejahatan digital masa kini, agar perlindungan hukum tetap relevan dan efektif di tengah perkembangan teknologi yang semakin kompleks[5], dengan cara diskusi publik mengkaji lebih dalam mengenai teknologi AI oleh pihak yang berpengalaman agar publik bahaya nya AI dalam konteks deepfake.

Diartikan oleh akademi ahli hukum sebagai bentuk invasi privasi seksual. Para ahli juga memasukkan *Deepfake* pornografi ke dalam pornografi tanpa consent dan kekerasan seksual melalui gambar. Pelaku pornografi mencuri otoritas tubuh korban dengan merekayasa korban melakukan sesuatu yang pelaku inginkan tanpa izin dan bahkan sepengetahuan korban. Pelaku bertindak seolah ia mempunyai kuasa sepenuhnya akan tubuh perempuan yang berada dalam dunia maya. Hal ini termasuk dalam perbuatan kriminal, dimana pelakunya melakukan beberapa kejahatan sekaligus ketika membuat *Deepfake* pornografi, yaitu kekerasan seksual, mencuri data pribadi, menyebarkan informasi palsu, dan juga manipulasi[6].

3.2. PEMBAHASAN

[4] Laura Payne, “Deepfake: History & Facts”, Britannica, https://www.britannica.com/technology/deepfake./ diakses pada 29 Oktober 2025.
[5] Putu Bagus Dananjaya, Khairina, dkk, Dasar-Dasar Hukum : Pedoman Hukum Di Indonesia, (Jambi: PT. Sonpedia Publishing Indonesia, 2024), hal, 160.
[6]Ibid hlm 2

3.2.1. Cara pencegahan *Deepfake* AI

Dalam penelitian di turki menggunakan berbagai algoritma dan metode yang dirancang oleh para ahli desainer untuk mengekstrak informasi dan karakteristik spesifik dari gambar wajah. Misalnya, mendeteksi status mata (terbuka/tertutup) dapat dilakukan dengan mengekstrak fitur buatan tangan (tepi dan sudut) dari gambar wajah. Ini adalah metode buatan tangan yang terkenal untuk sistem pengenalan wajah: filter Gabor, pola biner lokal (LBP), pola terner lokal (L.T.P.), dan histogram gradien terarah (H.O.G)[7].

Para peneliti di turki menghipotesiskan bahwa "setiap orang memiliki ekspresi wajah dan gerakan khusus saat berbicara". Oleh karena itu, para penulis mengusulkan model deteksi keunikan untuk membedakan orang yang menjadi fokus dari orang lain berdasarkan metode SVM kelas. Para penulis meneliti satu klip video selama 10 detik. Klip ini digunakan sebagai input untuk melacak gerakan kepala, mengekstrak ekspresi, dan membedakan fitur dari wajah. Mereka menggunakan toolkit OpenFace2 untuk mengekstrak gerakan kepala, pengangkat alis, bagian bibir yang diturunkan, rahang yang turun, hidung, pipi, dan kedipan mata[8]. Mengusulkan metode Deep Vision untuk menganalisis pola kedipan mata seseorang dan mendeteksi Deep - fakes dalam video. mengekstrak wilayah wajah orang target dan melacak kedipan matanya berdasarkan perhitungan E.A.R. (eye-aspect-ratio) untuk setiap frame.

Mereka menggunakan nilai E.A.R untuk mendeteksi peristiwa kedipan mata (tertutup/terbuka) dan menganalisis ambang batas kedipan mata seseorang untuk setiap formulasi kerangka dalam video. Mereka mencapai tingkat akurasi 87,5%. Akibatnya, fitur yang diekstraksi tidak mewakili karakteristik masalah atau aplikasi error, menyebabkan akurasi rendah dan akurasi yang berbeda-beda berdasarkan faktor gambar[9].

Dalam penelitian diatas bahwa perlu adanya penelitian bagi praktisi hukum dan kelembagaan pemerintahan yang mengurusi masalah isu cyber crime dan kerja sama internasional agar membenahi teknologi, peraturan dan hukum.

Pembentukan undang-undang terkait AI di Indonesia menghadapi berbagai tantangan dan hambatan yang kompleks. Sebagai perbandingan, Uni Eropa pada Maret 2024 telah menerbitkan peraturan yang bertujuan menganalisis dan mengklasifikasikan risiko dari berbagai aplikasi berbasis AI. Regulasi ini dirancang untuk memberlakukan pengaturan berdasarkan tingkat risiko, guna menciptakan lingkungan penggunaan AI yang lebih aman dan terkontrol. Dengan pendekatan ini, Uni Eropa berupaya memaksimalkan manfaat teknologi AI sembari mengelola potensi risikonya secara efektif. Regulasi tersebut mencakup klasifikasi risiko di mana aplikasi AI dengan risiko tinggi seperti yang digunakan di bidang medis atau keamanan akan dikenakan pengawasan dan persyaratan lebih ketat. Proses pembentukan regulasi AI membutuhkan pemahaman mendalam mengenai teknologi ini termasuk identifikasi risiko dan manfaatnya. Di Indonesia, isu-isu seperti privasi, keamanan data, dan etika dalam penggunaan AI juga harus menjadi perhatian utama. Selain itu, diperlukan peningkatan kesadaran dan pemahaman tentang AI di kalangan pembuat kebijakan dan masyarakat umum,

[7] Robinson JP. Automatic face understanding: recognizing families in photos. PhD thesis, ProQuest. 2020.https://doi.org/28314324./ https://www.proquest.com/openview/c7cc950b2e62621407f0278775665cf8/1?pqorigsite=gscholar&cbl=18750 &diss=y./ Diakses pada tanggal 29 Oktober 2025

[8] Agarwal P, Mukerji G, Desveaux L, Ivers NM, Bhattacharyya O, Hensel JM, Shaw J, Bouck Z, Jamieson T, Onabajo N, Cooper M, Marani H,
Jefs L, Bhatia RS. Mobile app for improved self-management of type 2 diabetes: multicenter pragmatic randomized controlled trial. JMIR Mhealth Uhealth. 2019;7(1):10321. https://doi.org/10.2196/10321./ diakses pada tanggal 29 Oktober 2025

[9] Jung T, Kim S, Kim K. Deepvision: deepfakes detection using human eye blinking pattern. IEEE Access. 2020;8:83144–54. https://doi.org/10.1109/access.2020.2988660./ diakses pada tanggal 29 Oktober 2025

agar regulasi yang dihasilkan relevan dan efektif dalam mengatur perkembangan teknologi ini[10].

4. KESIMPULAN

Penelitian ini telah mengidentifikasi tantangan hukum yang signifikan yang ditimbulkan oleh teknologi *Deepfake* AI, khususnya dalam konteks regulasi di Indonesia yang belum secara spesifik mengatur penyalahgunaannya. Ketiadaan aturan spesifik mengenai *Deepfake* berpotensi menyebabkan salah perspektif atau diskresi interpretasi dalam penegakan hukum pidana. Saat ini, penyalahgunaan *Deepfake* harus disandarkan pada interpretasi pasal-pasal dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam UU ITE, tindakan pembuatan dan penyebaran konten *Deepfake* yang merugikan dapat dikonstruksikan melalui Pasal 27 ayat (1) (tentang kesusilaan, jika konten pornografi), Pasal 27 ayat (3) (tentang pencemaran nama baik dan penghinaan), serta Pasal 28 ayat (2) (tentang penyebaran berita bohong yang menimbulkan permusuhan SARA). Sementara itu, aspek pelanggaran privasi dalam *Deepfake* dapat dijerat melalui Pasal 67 ayat (1) jo. Pasal 12 ayat (2) UU PDP, yang melarang penggunaan data pribadi (termasuk biometrik wajah dan suara) secara melawan hukum, serta potensi penggunaan Pasal 69 terkait pemalsuan data pribadi untuk keuntungan.

Meskipun pasal-pasal tersebut memberikan landasan hukuman pidana, konstruksi hukum ini masih bersifat terbatas dan tidak spesifik melarang penggunaan teknologi *Deepfake* AI untuk tujuan kejahatan di masa depan. Mengingat pesatnya perkembangan teknologi deepfake, yang kemampuannya melampaui regulasi yang ada, urgensi untuk pembentukan norma hukum baru sangat mendesak. Pembentukan regulasi spesifik mengenai *Deepfake* tidak hanya akan memberikan kepastian hukum, tetapi juga akan mewujudkan perlindungan maksimal terhadap hak privasi dan integritas warga negara. Oleh karena itu, perlu segera dilakukan pembahasan rancangan undang-undang atau peraturan pemerintah yang secara eksplisit mengatur dan melarang penyalahgunaan *Deepfake* oleh lembaga yang berwenang dalam keamanan siber dan perlindungan data pribadi.

5. UCAPAN TERIMA KASIH

Ucapan terima kasih hanya disampaikan kepada Dekan Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma, Ketua Program Studi Ilmu Hukum Universitas Dirgantara Marsekal Suryadarma.

DAFTAR PUSTAKA

Agarwal, P., G. Mukerji, L. Desveaux, N. M. Ivers, O. Bhattacharyya, J. M. Hensel, J. Shaw, Z. Bouck, T. Jamieson, N. Onabajo, M. Cooper, H. Marani, L. Jefs, dan R. S. Bhatia. "Mobile App for Improved Self-Management of Type 2 Diabetes: Multicenter Pragmatic Randomized Controlled Trial." *JMIR Mhealth Uhealth* 7, no. 1 (2019): 10321. https://doi.org/10.2196/10321.

Ayu, Nurfaizah. "Waspadai Politik Identitas Lewat Manipulasi Opini Jelang Pemilu 2024." *Kompas.id*, 2 Maret 2023. https://www.kompas.id/baca/polhuk/2023/03/02/waspadai-politik-identitas-menjelang-pemilu-2024.

[10] Mufti dkk., "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence," 139–40.

Dananjaya, Putu Bagus, Khairina, dkk. *Dasar-Dasar Hukum: Pedoman Hukum Di Indonesia*. Jambi: PT. Sonpedia Publishing Indonesia, 2024.

Juefei-Xu, F., R. Wang, Y. Huang, Q. Guo, L. Ma, dan Y. Liu. "Countering Malicious Deepfakes: Survey, Battleground, and Horizon." *Int J Comput Vis* 130, no. 7 (2022): 1678–734. https://doi.org/10.1007/s11263-022-01606-8.

Jung, T., S. Kim, dan K. Kim. "Deepvision: Deepfakes Detection Using Human Eye Blinking Pattern." *IEEE Access* 8 (2020): 83144–54. https://doi.org/10.1109/access.2020.2988660.

Karo, R. K. (2025). *PENGANTAR METODOLOGI PENELITIAN HUKUM DI ERA DIGITAL* (1st ed.). Raja Grafindo Persada.

Karo Karo, Rizky. *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana*. 1st ed. Tangerang: Penerbit Fakultas Hukum, Universitas Pelita Harapan, 2019.

Karo, Rizky Pratama Putra Karo. "Hate Speech: Penyimpangan Terhadap UU ITE, Kebebasan Berpendapat Dan Nilai-Nilai Keadilan Bermartabat." *Jurnal Lemhannas RI :* 10, no. 4 (2022): 52–65. https://jurnal.lemhannas.go.id/index.php/jkl/article/view/370/242.

Karo, R. K., & Prasetyo, T. (2025). The Provision of Licensed Financial Technology Lending From The Perspective of Cyber Law and Criminal Law in Indonesia. *Pena Justisia Media Komunikasi Dan Kajian Hukum*, *24*(2), 7263–7280.

Mufti, dkk. "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence." *Jurnal Tidak Diketahui* [Nomor Halaman Tidak Diketahui].

Prasetyo, Teguh, Yuni Ginting, and Rizky Karo Karo. *Hukum Pidana - Edisi Revisi*. 1st ed. Depok: RajaGrafindo Persada, 2023. https://www.rajagrafindo.co.id/produk/hukum-pidana-prof-dr-teguh-prasetyo-s-h-m-si-dr-yuni-priskila-ginting-s-h-m-h-rizky-karo-karo-s-h-m-h/.

Payne, Laura. "Deepfake: History & Facts." *Britannica*. https://www.britannica.com/technology/deepfake.

Rahmad, Noor. "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online." *Jurnal Hukum Ekonomi Syariah* 3, no. 2 (2019): 103-117. https://doi.org/10.26618/j-hes.v3i2.2419.

Robinson, J. P. "Automatic Face Understanding: Recognizing Families in Photos." PhD thesis, ProQuest, 2020. https://www.proquest.com/openview/c7cc950b2e62621407f0278775665cf8/1?pqorigsite=gscholar&cbl=18750&diss=y.

Susantijo, Susi. "A Human Rights Perspective on Granting Privileges to Descendants of PKI in Indonesia." *Fiat Justisia: Jurnal Ilmu Hukum* 19, no. 1 (2025): 1–20.

Tan, M., dan Q. Le. "Efcientnet: Rethinking Model Scaling for Convolutional Neural Networks." Dalam *Proceedings of the International Conference on Machine Learning*, 2019. http://proceedings.mlr.press/v97/tan19a.html.

Taylor, Matthews. "Deepfakes, Intellectual Cynics, and the Cultivation of Digital Sensibility." *Royal Institute of Philosophy Supplement* 92 (2022): 67–85.

Vera, Nick. "Between Realities: Information Sharing Practices of *Deepfake* Creators." *Proceedings of the Association for Information Science and Technology* 60, no. 1 (2023):

1161–1163.

VOA Indonesia. "Banyak Warga Jadi Korban Penipuan *Deepfake* yang Catut Nama Prabowo." *VOA Indonesia*, 2 November 2023. https://www.voaindonesia.com/a/banyak-warga-jadi-korban-penipuan-deepfake-yang-catut-nama-prabowo/7994103.html.